5th Edition

EnCase LEGAL JOURNAL

The practitioner's guide to legal issues related to digital investigations and electronic discovery

Guidance SOFTWARE

Guidance® SOFTWARE

EnCase® Legal Journal
5th Edition

Official Legal Citation: EnCase L.J. (2014)

Copyright © 2014 Guidance Software Inc.

All rights reserved. No part of this book may be reproduced, stored, or transmitted by any means—whether auditory, graphic, mechanical, or electronic—without written permission of both publisher and author, except in the case of brief excerpts used in critical articles and reviews. Unauthorized reproduction of any part of this work is illegal and is punishable by law.

ISBN: 978-1-4834-0915-3 (sc)
ISBN: 978-1-4834-0914-6 (e)

Because of the dynamic nature of the Internet, any web addresses or links contained in this book may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

The information provided herein is general information only and does not constitute legal or other professional advice or any opinion of Guidance Software, Inc. or its contributing authors. For this reason, it is recommended that you seek the advice of a lawyer who can advise you on the specific legal issues that may be applicable to your business concerns.

Any people depicted in stock imagery provided by Thinkstock are models, and such images are being used for illustrative purposes only.
Certain stock imagery © Thinkstock.

Lulu Publishing Services rev. date: 3/24/2014

Acknowledgements

Guidance Software Editorial Board

- *Victor T. Limongelli, Editor-in-Chief, President & CEO*
- *Chad McManamy, Managing Editor, Assistant General Counsel*

Guidance Software would like to thank the following authors for their generous contribution to this edition of the EnCase® Legal Journal:

- *Patrick J. Burke, Attorney, Reed Smith LLP*
- *Dominic Jaar, Associate Partner, Information Management and E-Discovery, KPMG*
- *Scott A. Carlson, Partner, Seyfarth Shaw*
- *Denise Backhouse, Associate, Morgan, Lewis & Bockius, LLP*
- *Chris Dale, E-Disclosure Information Project*
- *John Blumenschein, Counsel, Seyfarth Shaw LLP*
- *Daniel Lim, E-Discovery Attorney*
- *Siddartha Rao, E-Discovery Attorney*

Preface

Over the last twenty years, the field of computer forensics and electronic discovery (e-discovery) have expanded greatly, mirroring the explosion of digital data in society at large. What began as a practice of a select few technical experts has become a field in which thousands are involved. Computer evidence is now a mainstay not only in criminal matters, but also in civil discovery, internal corporate investigations, and computer security incident response. In each of these situations, the authentication and presentation of electronic evidence at trial is either a primary goal or, at a minimum, a consideration that the computer investigator must take into account. This EnCase® Legal Journal is provided with three goals in mind:

1. It reports on court decisions involving EnCase® software, as well as notable court decisions involving computer evidence in general.
2. It addresses how the EnCase process facilitates the authentication and admission of electronic evidence in light of evolving industry practices and the current status of the law, providing investigators and their counsel with an added resource when addressing questions involving computer forensics and the use of EnCase software.
3. It focuses on how the rules regarding e-discovery of Electronically Stored Information (ESI) have been interpreted by various courts and how EnCase software facilitates compliance with those rules.

The EnCase Legal Journal is provided for informational purposes and is not intended as legal advice, nor should it be construed or relied upon as such. Each set of circumstances may be different and all cited legal authorities should be confirmed and updated.

Just as Guidance Software is committed to ongoing product research and development, so must we also be on top of the latest legal developments impacting this field. As such, this journal should be considered as a work perpetually in progress.

A special thanks to the Guidance Software Associate General Counsel (AGC) team for updating this edition. If you have any questions, comments or suggestions for future revisions, please feel free to contact the editors at LegalJournal@EnCase.com

Contents

New in the Fifth Edition xi

Authentication of Computer Evidence 1

§ 1.0 Overview 1
§ 1.1 Authentication of Computer Data 1
§ 1.2 Authentication of the Recovery Process 4
§ 1.3 Authentication of the EnCase Recovery Process 7
§ 1.4 Challenges to Foundation Must Have Foundation 8
§ 1.5 Evidentiary Authentication Within the EnCase® Enterprise Process 8
§ 1.6 Cases Involving the Use of EnCase Enterprise and Other Relevant Authority 11

Validation of Computer Forensic Tools 17

§ 2.0 Overview 17
§ 2.1 Frye/Daubert Standard and Judicial Notice 17
§ 2.2 Computer Forensics as an Automated Process 22
§ 2.3 Commercial vs. Custom Forensics Software and Authentication Issues 25

Expert Witness Testimony 29

§ 3.0 Overview 29
§ 3.1 Threshold Under Rule 702 29
§ 3.2 Importance of Well-Established Certifications, such as the EnCE for Expert Testimony 32
§ 3.3 Illustrations of Testimony 32

The Best Evidence Rule 47

§ 4.0 Overview 47
§ 4.1 "Original" Electronic Evidence 47
§ 4.2 Presenting Electronic Evidence at Trial 49
§ 4.3 Compression and the Best Evidence Rule 51
§ 4.4 United States v. Naparst – The EnCase Evidence File Validated as Best Evidence 52

Legal Analysis of the EnCase Evidence File 55

§ 5.0 Overview 55
§ 5.1 Evidence File Format 55
§ 5.2 CRC and MD5 Hash Value Storage and Case Information Header 56
§ 5.3 Chain of Custody Documentation 57
§ 5.4 The Purpose of Sterile Media and The EnCase Process 57
§ 5.5 Analyzing the Evidence File Outside of the EnCase Process 58

Challenges to EnCase Software and Cases Involving EnCase Software 61

§ 6.0 Validation v. Reference 61
Cases Involving EnCase Software 63

Search and Seizure Issues and EnCase Software 101

§ 7.0 Overview 101
§ 7.1 EnCase-Specific Court Decisions Concerning Search and Seizure Issues 101
§ 7.2 Computer Files and the Plain View Doctrine 105
§ 7.3 United States v. Carey 108
§ 7.4 Post-*Carey* Case Law 110
§ 7.5 Post-*Carey* Practice 121
§ 7.6 Business Disruption Caused by the Seizure of Computers 122

Complying with Discovery Requirements in Criminal Cases When Utilizing the EnCase Process 125

§ 8.0 Overview 125
§ 8.1 Production of Entire EnCase Images 125
§ 8.2 Production of Restored Drives 126
§ 8.3 Production of Exported Files 126
§ 8.4 Supervised Examination 126
§ 8.5 Production of EnCase Evidence Files to Defense Experts 127
§ 8.6 Discovery Referee in Civil Litigation Matters 129
§ 8.7 Federal Rules of Civil Procedure's Electronically Stored Information Amendments in a Criminal Context 130

Civil E-Discovery 131

§ 9.0 Overview 131
§ 9.1 E-Discovery – A Mandated and Routine Process 131

§ 9.2 Sanctions....138
§ 9.3 The Defensibility of an In-House Process and the 30(b)(6) Witness....147
§ 9.3.1 Employing a Reasonable and Defensible Process....149
§ 9.4 The Sedona Conference® Cooperation Proclamation....157
§ 9.5 Preservation / Spoliation....159
§ 9.6 Litigation Hold....170
§ 9.7 Custodian Self-Collection....177
§ 9.8 Metadata....180
§ 9.9 Search....189
§ 9.9.1 Keyword Searches....193
§ 9.9.2 Technology Assisted Review....200
§ 9.10 Privilege....203
§ 9.11 Proportionality....206
§ 9.12 Social Networking....210
§ 9.13 Cloud Computing....213
§ 9.14 Discovery in United States Federal Agencies....215
§ 9.15 State Rules Update....217

Employee Data Privacy (US)....221

§ 10.0 Overview....221
§ 10.1 Preliminary Considerations for Employers....221
§ 10.2 The Electronic Communications Privacy Act of 1986....222
§ 10.3 Employee Monitoring in the Private Sector....224
§ 10.4 Monitoring of Government Employees....227
§ 10.5 Monitoring the Military....230

International E-Discovery....233

§ 11.0 Overview....233
§ 11.1 E-Discovery Outside the US and Cross-Border Litigation....233

Articles....265

Article Index....495

Case Index....497

New in the Fifth Edition

The following sections have been added or revised for this edition:

Section 1.6 Cases Involving the Use of EnCase Enterprise and other Relevant Authority
Section 3.2 Importance of Well-Established Certifications, such as the EnCE, for Expert Testimony
Chapter 7 Search and Seizure Issues and EnCase Software
Chapter 9 Civil E-Discovery
Chapter 10 Employee Data Privacy (US)
Chapter 11 International E-Discovery (New)

1. Authentication of Computer Evidence

§ 1.0 Overview

Documents and writings must be authenticated before they may be introduced into evidence. The United States Federal Rules of Evidence, as well as the laws of many other jurisdictions, define computer data as documents.[1] Electronic evidence presents particular challenges for authentication, as such data can be easily altered without proper handling. The proponent of evidence normally carries the burden of offering sufficient support to authenticate documents or writings, and electronic evidence is no exception.

What testimony is required to authenticate computer data? How does a witness establish that the data he or she recovered from a hard drive is not only genuine, but completely accurate? Are there guidelines or checklists that should be followed? How familiar with the software used in the investigation must the examiner be in order to establish a proper foundation for the recovered data? These are some of the questions that face computer investigators and counsel when seeking to introduce electronic evidence. This chapter will address these questions.

§ 1.1 Authentication of Computer Data

Oftentimes, the admission of computer evidence, typically in the form of active ("non-deleted") text or graphical image files, is accomplished without the use of specialized computer forensic software. Federal Rule of Evidence 901(a) provides that the authentication of a document is "satisfied by evidence sufficient to support a finding that the matter in question is what the proponent claims." The Canada Evidence Act specifically addresses the authentication of computer evidence, providing that an electronic document can be authenticated "by evidence capable of supporting a finding that the electronic document is that which it is purported to be."[2] Under these statutes, a printout of an e-mail message can often be authenticated simply through direct testimony from the recipient or the author.[3]

The United States (US) Federal Courts have thus far addressed the authentication of computer-generated evidence based upon Rule 901(a) in much the same manner as other types of evidence that

1 See Fed. R. Evid. 1001(1); Canada Evidence Act, R.S.C. 1985, c. C-5, s.30(12), 31.8(b).

2 Canada Evidence Act, R.S.C. 1985, c. C-5, s.31.1.

3 United States v. Siddiqui, 235 F.3d 1318 (11th Cir. 2000) (testimony of recipients sufficient to authenticate e-mails sent by defendant); Laughner v. State, 769 N.E.2d 1147 (Ind. Ct. App. 2002) (AOL instant messages authenticated by the recipient).

existed before computer usage became widespread.[4] *United States v. Tank*,[5] which involves evidence of Internet chat room conversation logs, is an important illustration.

In *Tank*, the defendant appealed from his convictions for conspiring to engage in the receipt and distribution of sexually explicit images of children and other offenses. Among the issues addressed on appeal was whether the government made an adequate foundational showing of the relevance and the authenticity of a co-conspirator's Internet chat room log printouts. A search of a computer belonging to one of defendant Tank's co-conspirators, Riva, revealed computer text files containing "recorded" online chat room discussions that took place among members of the Orchid Club, an Internet chat room group to which Tank and Riva belonged.[6] Riva's computer was programmed to save all of the conversations among Orchid Club members as text files whenever he was online.

At an evidentiary hearing, Tank argued that the district court should not admit the chat room logs into evidence because the government failed to establish a sufficient foundation. Tank contended that the chat room log printouts should not be entered into evidence because: (1) they were not complete documents, and (2) undetectable "material alterations," such as changes in either the substance or the names appearing in the chat room logs, could have been made by Riva prior to the government's seizure of his computer.[7] The district court ruled that Tank's objection went to the evidentiary weight of the logs rather than to their admissibility, and allowed the logs into evidence. Tank appealed, and the appellate court addressed the issue of whether the government established a sufficient foundation for the chat room logs.

The appellate court considered the issue in the context of Federal Rule of Evidence 901(a), noting that "[t]he rule requires only that the court admit evidence if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification… The government must also establish a connection between the proffered evidence and the defendant."[8]

In authenticating the chat room text files, the prosecution presented testimony from Tank's co-conspirator Riva, who explained how he created the logs with his computer and stated that the printouts appeared to be an accurate representation of the chat room conversations among members of the Orchid Club. The government also established a connection between Tank and the chat room log printouts. Tank admitted that he used the screen name "Cessna" when he participated in one of the conversations recorded in the chat room log printouts. Additionally, several co-conspirators testified that Tank used the chat room screen name "Cessna," which appeared throughout the printouts. They further testified that when they arranged a meeting with the person who used the screen name "Cessna," it was Tank who appeared at the meeting.[9]

Based upon these facts, the court found that the government made an adequate foundational showing of the authenticity of the chat room log printouts under Rule 901(a). Specifically, the

4 Stanley a. Kurzban, Authentication of Computer-Generated Evidence in the United States Federal Courts, 35 IDEA 437, 439 (1995).

5 200 F.3d 627 (9th Cir. 2000).

6 Id. at 629.

7 Id. at 630.

8 Id. (citing United States v. Black, 767 F.2d 1334, 1342 (9th Cir. 1985)).

9 Id. at 631.

government "presented evidence sufficient to allow a reasonable juror to find that the chat room log printouts were authenticated."[10]

The *Tank* decision is consistent with other cases that have addressed the issue of the authenticity of computer evidence in the general context of Fed.R.Evid. 901(a).[11] *Tank* illustrates that there are no specific requirements or set procedures for the authentication of digital evidence, but that the facts and circumstances of the creation and recovery of the evidence, as applied to Rule 901(a), is the approach generally favored by the courts. (See also *United States v. Scott Emuakpor,*[12] [Government properly authenticated documents recovered from a computer forensic examination under Rule 901(a)]).

In *State (Ohio) v. Cook*, an Ohio Appellate Court upheld the validity of EnCase® software under Ohio Rule of Evidence 901(a), which is nearly identical to the corresponding federal rule.

NOTE: Please see Chapter 6 for a detailed analysis of *State v. Cook*.

Lorraine v. Markel American Insurance Company[13] is an important decision that addresses in detail the issue of computer evidence authentication in the context of e-discovery. In this case, which involves a contract dispute and interpretation issues, Magistrate Judge Grimm rejected the submission of printouts of computer evidence into evidence to support dueling cross-motions. He found the printouts failed to meet any of the standards for admission under the Federal Rules of Evidence. The e-mails were not authenticated but simply attached to the parties' motions as exhibits, as has been a common practice in civil litigation motion practice.

Judge Grimm — in a long opinion — discusses, in particular, Federal Rule of Evidence 901(b), which includes an illustrative list of methods to authenticate evidence. Many of these authentication techniques are particularly well suited to electronically stored information (ESI).

Circumstantial Authentication through Metadata

Judge Grimm notes that Rule 901(b)(4) is the most common method for authenticating electronically stored information in the context of civil litigation. This rule allows for authentication by "appearance, contents, substance, internal patterns or other distinctive characteristics, taken in conjunction with circumstances." Under this rule, an electronic document can be authenticated by, for example, considering the file permissions, file ownership, when created and modified dates and other metadata that tie the document to the purported author and/or custodian. "Metadata certainly is a useful tool for authenticating electronic records by use of distinctive characteristics."

---

10 Id.

11 See also, United States v. Whitaker, 127 F.3d 595, 601(7th Cir. 1997).

12 U.S. v. Scott-Emuakpor, No. 1:99-CR-138 , 2000 WL 288443 (W.D. Mich. 2000).

13 Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007).

Circumstantial Authentication through Hash Values

Judge Grimm endorses the use of hash values to authenticate individual files, the generation of which is a common practice in computer forensics at the time of collection:

> "Hash values can be inserted into (read: attached to) original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4). Also, they can be used during discovery of electronic records to create a form of electronic "Bates stamp" that will help establish the document as electronic. This underscores a point that counsel often overlook. A party that seeks to introduce its own electronic records may have just as much difficulty authenticating them as one that attempts to introduce the electronic records of an adversary. Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the "final" or legally operative version. This can plague a party seeking to introduce a favorable version of its own electronic records, when the adverse party objects that it is not the legally operative version, given the production in discovery of multiple versions. Use of hash values when creating the "final" or "legally operative" version of an electronic record can insert distinctive characteristics into it that allow its authentication under Rule 901(b)(4)."

This ruling is very notable as it clearly validates the standard practice of using computer forensics software to generate, maintain and document the hash values of individual files from the time of collection through analysis, production, and ultimate presentation at trial.

Authentication through an Automated Process (Rule 901(b)(9)):

Judge Grimm recognizes Rule 901(b)(9) as an important method of authenticating electronic evidence stored in or generated by computers. It authorizes authentication by "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." Fed.R.Evid. 901(b)(9). "Rule 901(b)(9), which is designated as an example of a satisfactory authentication, describes the appropriate authentication for results of a process or system and contemplates evidence describing the process or system used to achieve a result and demonstration that the result is accurate. The advisory committee note makes plain that Rule 901(b)(9) was designed to encompass computer-generated evidence . . .)"

Rule 901(b)(9) is further discussed in detail in section 2.2.

§ 1.2 Authentication of the Recovery Process

Where direct testimony is not available, a document may be authenticated through circumstantial evidence. A computer forensic examination is often an effective means to authenticate electronic

evidence through circumstantial evidence. The examiner must be able to provide competent and sufficient testimony to connect the recovered data to the matter in question.

Courts have recognized the importance of computer forensic investigations to authenticate computer evidence. *Gates Rubber Co. v. Bando Chemical Indus., Ltd.,*[14] is a particularly important published decision involving competing computer forensics expert testimony, where the court essentially defines a mandatory legal duty on the part of litigants or potential litigants to perform proper computer forensic investigations. There, one party's examiner failed to make a mirror image copy of the target hard drive and instead performed a "file-by-file" copy in an invasive manner, resulting in lost information.[15] The opposing expert noted that the technology needed for a mirror image backup was available at the time (February 1992), even though not widely used. In its ruling issuing harsh evidentiary sanctions, the court criticized the errant examiner for failing to make an image copy of the target drive, finding that when processing evidence for judicial purposes a party has "a duty to utilize the method which would yield the most complete and accurate results."[16]

Some courts have required only minimal testimony concerning the recovery process, particularly where the defense fails to raise significant or adequate objections to the admission of the computer evidence. In *United States v. Whitaker,*[17] a Federal Bureau of Investigation (FBI) agent obtained a printout of business records from a suspect's computer by simply operating the computer, installing Microsoft Money, and printing the records.[18] The court affirmed the admission of the printouts, finding that testimony of the agent with personal knowledge of the process used to retrieve and print the data provided sufficient authentication of the records.[19] However, in an apparent admonition to the defense bar, the court noted that the defense conspicuously failed to question the FBI agent "about how the disks were formatted, what type of computer was used, or any other questions of a technical nature."[20]

In a similar decision, *Bone v. State*,[21] the defendant contended that the trial court erred when it admitted pictorial images recovered from a hard drive without proper authentication. The appellate court noted that the computer investigator testified about the process he used to recover the data — that he "remove[d] the hard drive" from Bone's computers and "made an image of it"; he "right [sic] protected" the various floppy diskettes before viewing them, and testified about the software program he used to recover deleted files.[22] The detective further testified as to how he exported images found on the image of Bone's computer media. He testified that he printed copies of images in Bone's computer files "exactly" as he found them, and further stated that the images "fairly and accurately" showed the

14 167 F.R.D. 90 (D.C. Colo. 1996).
15 Gates Rubber co. v. Bando Chem. Indus., 167 F.R.D. 90, 112 (D. Colo. 1996).
16 Id.
17 127 F.3d 595 (7th Cir. 1997).
18 Id. at 600-01.
19 Id. at 600.
20 Id.
21 771 N.E.2d 710 (Ind. Ct. App. 2002).
22 Id. at 716.

images that he had seen "on the computer that [he was] using to examine Mr. Bone's computer."[23] In reviewing Indiana Evidence Rule 901(a), which is identical to the federal rule, and citing *Whitaker*, the appellate court determined that the trial court testimony was sufficient to establish the authenticity of the images contained in Bone's computer.[24]

People v. Lugashi[25] is another particularly notable case involving a detailed analysis by the court on this subject. Although not involving a computer forensic investigation per se, the court addressed issues concerning the authentication of computer-based evidence challenged by the defense in a criminal prosecution. The prosecution successfully introduced computer evidence generated by a routine business process through the testimony of one of the bank's systems administrators. Although she conceded that she was not a computer expert, she did work with those who operated the systems, maintained the records, and was familiar with the system that generated the computer evidence. She personally produced the data in question from the microfiche records and knew how to interpret it.[26] The defense contended that as the systems administrator was not a computer expert, she was incompetent to authenticate the data in question and that, essentially, only the computer programmers involved in the design and operation of the bank's computer systems could adequately establish that the systems and programs in question were reliable and free from error. The defense also asserted that because the systems administrator's understanding of how the system worked came from her discussions with the bank's programmers and other technical staff, her testimony constituted hearsay and thus should not be allowed.[27]

The court rejected the defense's argument, noting that the defense's position incorrectly assumed that only a computer expert "who could personally perform the programming, inspect and maintain the software and hardware, and compare competing products, could supply the required testimony."[28] Instead, the court ruled that "a person who generally understands the system's operation and possesses sufficient knowledge and skill to properly use the system and explain the resultant data, even if unable to perform every task from initial design and programming to final printout, is a 'qualified witness'" for purposes of establishing a foundation for the computer evidence.[29] The court noted that if the defense's proposed test were applied to conventional hand-entered accounting records, for example, the proposal "would require not only the testimony of the bookkeeper records custodian, but that of an expert in accounting theory that the particular system employed, if properly applied, would yield accurate and relevant information."[30] Further, if the defense's position were correct, "only the original hardware and software designers could testify since everyone else necessarily could understand the system only through hearsay." The *Lugashi* court also commented that the defense's proposed test

23 Id.
24 Id. at 716-17.
25 252 Cal. Rptr. 434 (Ct. App. 1988).
26 Id. at 440.
27 Id.
28 Id. at 439.
29 Id.
30 Id.

would require production of "hordes" of technical witnesses that would unduly burden both the already crowded trial courts and the business employing such technical witnesses "to no real benefit."[31]

In the context of computer forensics investigations, the courts have applied the same standard. In *Ohio v. Huffman*,[32] the appellant sought to overturn his conviction by contending that the prosecution did not adequately authenticate computer disks that contained key evidence. The appellant challenged the supporting evidence offered to support his convictions for pandering sexually oriented matter involving a minor by arguing that the state failed to show he "reproduced" the sexually explicit material involving a minor. In response, the court held that "the disks were in the same condition that prevailed when they had been recovered from the appellant's office" and the "state offered evidence to show that each exhibit was what the state claimed it to be: images obtained from disks recovered from Huffman's office." The court determined that the prosecution sufficiently established the authenticity of the evidence because the state showed, through a detailed computer forensics investigation and authentication process, that the material was recovered from the defendant's office. The state's computer-forensics expert testified that the materials were from Huffman's computer and that his computer forensics analysis established that they were "backups of data that had at one time been stored on the hard drive." The court held the testimony to be sufficient and upheld the lower court's conviction.

§ 1.3 Authentication of the EnCase Recovery Process

Under the standard articulated under *Lugashi* and several other similar cases, the examiner need not be able to intricately explain how each and every function of EnCase software works in order to provide sufficient testimony regarding the EnCase process. There are no known authorities requiring otherwise for software that is both commercially available and generally accepted. A skilled and trained examiner with a strong familiarity with the EnCase process should be able to competently present EnCase-based evidence obtained through a forensic examination.[33]

NOTE: See Chapter 6 for a detailed analysis of reported cases involving EnCase software.

An examiner should have a strong working familiarity of how the program is used and what the EnCase process involves when seeking to introduce evidence recovered by the program. This means that the examiner should ideally have received training on EnCase software, although such training should not be strictly required, especially where the witness is an experienced computer forensics investigator and has received computer forensics training on similar computer systems in the past. Examiners should also conduct their own testing and validation of the software to confirm that the

31 Id.

32 847 N.E.2d 58 (Ohio Ct. App. 2006).

33 Additionally, Lugashi is clearly an important case when seeking to introduce computer-generated evidence created or maintained by third-party ISPs, businesses and other institutions.

program functions as advertised. However, a "strong working familiarity" does not mean that an examiner must obtain and be able to decipher all 600,000+ lines of the program source code or be able to essentially reverse-engineer the program on the witness stand.

§ 1.4 Challenges to Foundation Must Have Foundation

In the event the initial evidentiary foundation established by the computer forensics examiner's testimony is sufficiently rebutted, so as to challenge the admissibility or the weight of the evidence, expert testimony may be required to rebut such contentions. However, courts will normally disallow challenges to the authenticity of computer-based evidence absent a specific showing that the computer data in question may not be accurate or genuine—mere speculation and unsupported theories generally will not suffice.[34] There is ample precedent reflecting that unsupported claims of possible tampering or overlooked exculpatory data are both relatively common and met with considerable skepticism by the courts. One federal court refused to consider allegations of tampering that was "almost wild-eyed speculation… [without] evidence to support such a scenario."[35] Another court noted that the mere possibility that computer data could have been altered is "plainly insufficient to establish untrustworthiness."[36]

One court suggests that the defense should perform its own credible computer forensic examination to support any allegation of overlooked exculpatory evidence or tampering.[37] Another court noted that while some unidentified data may have been inadvertently altered during the course of an exam, the defendant failed to establish how such alteration, even if true, affected the data actually relevant to the case.[38] As such, in order for a court to even allow a challenge based upon alleged tampering or alteration of the computer data, the defense should be required to establish both specific evidence of alteration or tampering and that such alteration affected data actually relevant to the case. Further, even if there were some basis to allegations that relevant computer records have been altered, such evidence would go to the weight of the evidence, not its admissibility.[39]

§ 1.5 Evidentiary Authentication Within the EnCase® Enterprise Process

Computer data retrieved in a network environment in the regular course of business has been successfully admitted into evidence in many reported cases.[40] In the corporate enterprise environment,

34 United States v. Tank, 200 F.3d 627 (9th Cir. 2000); State v. Schroeder, 613 N.W.2d 911 (Wis. Ct. App. 2000).

35 United States v. Whitaker, 127 F.3d 595, 602 (7th Cir. 1997).

36 United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988); See also, United States v. Glasser, 773 F.2d 1553 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records.").

37 Tank, 200 F.3d at 631 fn. 5.

38 Schroeder, 613 N.W.2d at 911.

39 See Bonallo, 858 F.2d at 1436.

40 See, e.g., United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991); United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir. 1990); People v. Lugashi, 252 Cal. Rptr. 434 (Ct. App. 1988).

effective computer incident response examinations must occur in real-time and over the network, either because the targeted workstations or servers are in a remote location, or because the drives cannot be powered down without causing significant harm to the business.

In order to evaluate issues concerning chain of custody and data integrity through the EnCase Enterprise process, the disadvantages of other more limited procedures often used for remote analysis and file recovery over a network must first be understood. For example, using virus-checking utilities or system administrator tools to conduct remote analysis of active files presents several problems from an evidentiary standpoint.

First, such applications will materially alter the files being accessed or examined. In addition to changing critical file date stamps, including last-accessed and last-modified times, remotely opening files through Windows NT and other operating systems administration processes will likely result in a temporary file and other shadow data being generated on the target drive being examined.

EnCase Enterprise software is designed to address these challenges presented by real-time enterprise investigations. Importantly, EnCase Enterprise software operates at the disk level, allowing EnCase software to analyze the subject media in a read-only manner, without querying the resident operating system. This means that when the native files are read by EnCase software, the various metadata related to those files--such as time stamps, date stamps, and other information--are not altered. This also means that no backup files or shadow data are generated during this process.

Courts recognize the importance of employing best practices in the collection of computer evidence. "Best practices" is a shifting standard based upon both the circumstances of the investigation and the evolution of new technology. In incident response investigations, the analysis must be as rapid as possible to mitigate the loss and increase the likelihood of identifying the culprit. As the European Convention on Cybercrime has noted, "effective collection of evidence in electronic form requires very rapid response."[41]

For these reasons, many law enforcement agencies in the United States and throughout the world are employing EnCase Enterprise software in criminal investigations in situations in which (i) the circumstances do not allow for systems to be taken offline, (ii) the necessity of a rapid response requires utilization of a wide area network (WAN) to access the target media, or (iii) there is a need to investigate numerous volumes of computer media attached to a WAN. Under these situations, best practices support the use of EnCase Enterprise software.

Of course, because EnCase Enterprise software operates in a live environment, a "static" imaging process is simply not possible. Whenever a computer drive remains operating in its native environment, there will be changes made to that drive by virtue of its continued operation, such as writes to the swap file or other automatic functions of the resident operating system. However, despite operating in a live environment, EnCase Enterprise software does not itself write to the target drive during the exam, nor are files altered in any way when viewed or copied by EnCase software.

It is often more advantageous from both evidentiary and cost standpoints to remotely image or

41 Council of Europe's Convention on Cybercrime, Explanatory Report, ¶ 298.

forensically search a live computer system, rather than to shut down a system for stand-alone analysis, for reasons including the following:

- Critical systems often cannot be brought down without causing substantial damage to an enterprise's business operations. With the advent of EnCase Enterprise software, it is no longer absolutely necessary to shut down mission-critical servers in order to conduct a proper computer investigation.

- Critical evidence will often be lost between the time an investigation is deemed necessary and when the investigator can gain physical access to a computer. It is thus often more advantageous to conduct an immediate remote investigation, rather than waiting several hours or even days to either travel to a site or conduct a clandestine stand-alone computer investigation. With the advent of EnCase Enterprise technology, such a delay is no longer reasonable.

- When operating on a live system, a substantial amount of volatile data can be accessed that would otherwise disappear or not be available if a system were shut down. Running processes, open ports, data in RAM, connected devices, and current open documents are just a few examples of forensically important live data that is only available when a computer is running in its native environment.

Factors such as these are considered by the courts in determining the appropriateness of methodology to search computer systems for purposes of recovering evidence.[42]

Another question sometimes raised when a live system is remotely previewed or recovered over a network is whether the recovered data is genuine and can be associated with the specific computer in question. EnCase Enterprise software addresses this equation on three fronts:

1. EnCase Enterprise software, unlike typical system administrative tools, cannot write to the subject media at any time during the examination. This means that any relevant data found on the subject drive could not have been placed there through the use of EnCase Enterprise software, even if the investigator had wanted to do so.
2. The elaborate, role-based security apparatus of EnCase Enterprise software disallows unauthorized access and securely logs and identifies all users and activity throughout the course of the examination through a secure server, thus documenting important chain of custody and creating a detailed and secure record of the examination.
3. All transported data in the EnCase Enterprise software environment and the resulting evidence files are encrypted with 128-bit Advanced Encryption Standard (AES) encryption. In addition,

42 See United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (upholding seizure of "[a]ny and all computer software and hardware, . . . computer disks, disk drives" in a child pornography case because "[a]s a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the [sought after] images").

when creating evidence files, EnCase Enterprise software calculates cyclic redundancy check (CRC) and message digest 5 (MD5) checksums[43]in the same manner as the standalone forensic version.

§ 1.6 Cases Involving the Use of EnCase Enterprise and Other Relevant Authority

EnCase Enterprise software is based upon the same code and foundation as the EnCase stand-alone software (known as EnCase® Forensic software). EnCase Enterprise software is essentially the core EnCase stand-alone product, but network-enabled in a highly scalable manner, with the addition of internal role-based security and database support for increased functionality. As such, the above case law set forth below in Chapter 6 is highly relevant to EnCase Enterprise software and serves as an important foundation of credibility that is simply not present with any other tool used in corporate computer investigations.

EnCase Enterprise software has been used in thousands of investigations to date. The following are some key decisions:

Positive Software v. New Century Mortgage44

Positive Software Solutions Inc. v. New Century Mortgage,[45] is a U.S. federal court case in which EnCase Enterprise software was used by the defendant's expert to image 11 of the defendant's 250+ servers. The plaintiff raised objections and sought direct access to the defendant's network to conduct their own imaging. In denying the plaintiff's motion to conduct their own imaging of defendant's servers, the court ordered the defendant "to preserve all extant backups or images of all servers or personal computers that now or previously contained any [relevant evidence] . . . and to preserve all extant backups or images of all e-mail servers, pending further order of the Court or directive of the arbitrator." The court ignored the plaintiff's unspecified allegations questioning "the quality and accuracy of the imaging," and in no way faulted the use of EnCase Enterprise software or otherwise find that the forensic imaging that was conducted using EnCase Enterprise software was in any way deficient or unacceptable.

United States v. Greathouse[46]

The *Greathouse* case is a published decision that is highly relevant to EnCase Enterprise and Field Intelligence Model (EnCase Enterprise for Law Enforcement) because the court approves of the

43 Checksums are mathematically calculated values that are used, inter alia, to check data integrity. CRCs, or cyclic redundancy checks are common checksums that use codes of fixed length for error detection and as hash codes for data in digital systems and storage devices. MD5 or message digest 5 values are similarly used for error detections and as hash codes to track data integrity after a forensic acquisition.

44 259 F. Supp. 2d 561 (N.D. Tex. 2003).

45 Id.

46 297 F. Supp. 2d 1264 (D. Or. 2003).

network preview function of EnCase, which is the engine of EnCase Enterprise, as well as key functionality found in EnCase Enterprise, such as its data triage and "port scan" capabilities.

In *Greathouse*, federal agents executed a search warrant at a residence and discovered that five people lived in the house, and that six computers were networked together (five of which were in the den, and one of which was in defendant's bedroom).[47] Two other computers were located in the den but not connected to the network. The execution of the warrant and the interviewing of the residents took place over a three-to-four hour time period.[48] According to the court:

> [The investigating agent] explained that he decided to seize all of the computers and shut down the network because he could not tell which of the computers had the suspected child pornography and it would take several days to review and make this determination. [The investigating agent] further testified that he could see that the defendant's computer was hooked up to the network because of the presence of a network cable and a network card installed on the computer.
>
> At the hearing, defendant proffered testimony from a computer forensic consultant… [who] explained that there is a computer preview program known as ENCASE that has been available for many years that makes it possible to quickly scan computers for certain information. [The expert] testified that, with ENCASE, a computer could be scanned for the presence of child pornography within just a few minutes. [The expert] also testified that there is a "port scan" that can be used to learn more about the nature of computer equipment. [The investigating agent] testified that he was aware of the ENCASE program, that he has this program available, but that he did not bring the program with him for this particular search.[49]

The court ultimately granted the defendant's motion to suppress the evidence based on other grounds, but did address in dicta what constitutes best practices in conducting searches in locations where multiple computers may well be present:

> Defendant also claims that the seizure of all eight computers was overly broad and he challenges, under *Franks,* [the investigating agent's] statement in the search warrant affidavit that the computers would need to be searched off-site by a forensics expert. Defendant relies upon [his expert's] testimony regarding the ENCASE preview program.
>
> Numerous cases have upheld the wholesale seizure of computers and computer disks and records for later review for particular evidence as the only reasonable means of conducting a search. *See Hay,* 231 F.3d at 637 (agents justified in taking entire computer

47 Id. at 1268.
48 Id. at 1268-69.
49 Id. at 1269.

> system off-site for proper analysis); *Lacy,* 119 F.3d at 746; *United States v. Upham* 168 F.3d 532, 534 (1st Cir.1999).
>
> However, I recognize that this may not always be true due to technological developments. In this case, I find that [the investigating agent] acted in reasonable reliance upon well-settled and clear Ninth Circuit authority upholding the right of investigating authorities to seize computers for later forensic analysis given that he had no way of knowing, prior to entry, that he would encounter eight computers instead of one. **Had there been any evidence that a number of suspect computers would be found on site, there may well be an obligation to use a program like ENCASE to more narrowly tailor the search and seizure.**[50] [emphasis added]

Thus, the *Greathouse* case, although decided on other grounds, strongly suggests that best practices require up-to-date tools, and that when sophisticated programs like EnCase software and its network analysis version (EnCase Enterprise) are available for an investigation involving networked computers, investigators will be expected to use them.

Companies that use EnCase Enterprise can point to the important guidance from the *Greathouse* court as essentially endorsing the use of technologies such as EnCase Enterprise as "best practice" for pre-screening of searches to prevent overly broad seizures involving networked computers. Additionally, this guidance appears in the law enforcement context, which generally involves a higher degree of scrutiny than corporate investigations.

Zubulake v. UBS Warburg, LLC[51]

The landmark *Zubulake* line of cases are very important in the e-discovery field as they establish a procedural framework involving processes, policies, and general technology. In *Zubulake V*, the court laid out an important recommended technological procedure for use when a company seeks to preserve and collect computer evidence in a larger scale investigation:

> To the extent that it may not be feasible for counsel to speak with every key player, given the size of a company or the scope of the lawsuit, counsel must be more creative. It may be possible to run a system-wide keyword search; counsel could then preserve a copy of each "hit." Although this sounds burdensome, it need not be. Counsel does not have to review these documents; only see that they are retained. For example, counsel could create a broad list of search terms, run a search for a limited time frame, and then segregate responsive documents.[52]

---

50 Id. at 1275 (emphasis added).

51 Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004); see also Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC, 216 F.R.D. 280 (S.D.N.Y. 2003); Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003).

52 Zubulake, 229 F.R.D. at 422.

Whether the court intended it or not, this is a very important recognition of the need for technologies such as EnCase Enterprise technology, which, at its core, uniquely provides the ability to perform a "system-wide keyword search" and "then preserve a copy of each 'hit.'" Like *Greathouse*, *Zubulake V* is very important, as companies that use EnCase Enterprise can point to this important guidance from the *Zubulake* court that essentially endorses the functionality of EnCase Enterprise software as best practice when preserving and collecting computer evidence for corporate investigations.

Keesoondoyal Case

In this criminal case in Wales,[53] EnCase Enterprise software was successfully used to gather relevant electronic evidence. As described in the local press:

> Dheej Keesoondoyal, 34, was employed by the BP/Safeway partnership as an accountant at their head office.
>
> But he set up a fictional company to create a series of false invoices for building work, which had never been carried out, and planned to start a jet-set life abroad with the proceeds.
>
> The money was paid into an account set up by brother-in-law Eric James under the made-up Global Construction and Electrical Contractors.
>
> Prosecutor Martyn Kelly said, "The company had never traded. It was not real."
>
> "The scheme was hatched and 12 false invoices were created authorizing payment for more than £1.5m from the BP/Safeway Partnership." [54]

Keesoondoyal received a four-year prison sentence.

State (Ohio) v. Morris[55]

Also, see the discussion of the *State (Ohio) v. Morris* case in Chapter 6, below. Although the case does not directly involve EnCase Enterprise software, the court considers EnCase disk images to be exact copies and admissible when the "original" is no longer available, which is important for cases involving the collection of computer evidence using network-enabled computer forensic software, such as EnCase Enterprise software.

---

53 See Paul Carey, Accountant plotted to cheat employers of €1.5m, The Western Mail, June 26, 2004, http://icwales.icnetwork.co.uk/0100news/0200wales/tm_objectid=14367417&method=full&siteid=50082&headline=accountant-plotted-to-cheat-employers-of---pound-1-5m-name_page.html.

54 Id.

55 State v. Morris, 2005 WL 356801 (Ohio App. 9 Dist. Feb. 16, 2005).

Yelton v. PHI, Inc.[56]

Courts notes use of "EnCase Command Center" used to collect evidence from two local hard drives.

NOTE: Please See Chapter 7 for a discussion of *United States v. Maali,* another case in which the forensic images comprised the only computer evidence in existence, as the original drives had been returned to the defendants.

---

56 279 F.R.D. 377 (E.D. Pa. 2011)

2. Validation of Computer Forensic Tools

§ 2.0 Overview

Chapter 1 addressed authenticating computer evidence through direct or circumstantial evidence in order to establish that the recovered data is genuine and accurate. Another form of an objection to authenticity may involve questioning the reliability of the computer program that generated or processed the computer evidence in question. In such cases, the proponent of the evidence must testify to the validity of the program or programs utilized in the process. This chapter discusses which standards the courts are actually applying in such challenges, and what testimony the examiner may need to provide to validate computer forensics tools.

Computer forensics and electronic evidence are now a standard component of the judicial process. Effective December 1, 2006, the Federal Rules of Civil Procedure were amended specifically to account for the discovery of "Electronically Stored Information" (ESI). (See Section 9.1, *infra*) A search of online legal databases reveals several hundred published decisions that address computer forensics evidence. More than just a useful tool for advocacy, such technologies are now becoming an integral part of establishing basic attorney competence. By way of example, in *Upton v. Knowles*[57], the court determined that the failure of a defense attorney to retain a computer forensics expert may constitute ineffective assistance of counsel.

§ 2.1 Frye/Daubert Standard and Judicial Notice

Daubert v. Merrell Dow Pharmaceuticals, Inc.,[58] is a landmark U.S. Supreme Court decision that sets forth a legal test to determine the validity of scientific evidence and its relevance to the case at issue. Many state court jurisdictions in the US follow the *Frye*[59] test, which is very similar, but not identical to *Daubert*. The introduction of DNA evidence is a typical scenario where a court may require a *Daubert/Frye* analysis.

In the past, the most concerted challenges to EnCase software involved the *Daubert* or *Frye* standards. However, a corporate defendant advocating the EnCase-based evidence in *Mathew Dickey v. Steris Corporation*[60] (further discussed at §6.01) successfully asserted that EnCase constituted an automated process that produces accurate results, and thus evidence obtained from that process would be subject to a presumption of authenticity under Federal Rules of Evidence (FRE) 901(b)(9). Rule 901(b)(9) provides that evidence produced by an automated process, including computer-generated

57 No. C 06-07854 WHA, 2007 WL 3023062 (N.D. Cal. Oct. 15, 2007).

58 509 U.S. 579 (1993).

59 Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

60 No. 99-2362-KHV (D. Kan. 2001).

evidence, may be authenticated if such an automated process is shown to produce accurate results. However, the court also addressed the *Daubert* factors. Although it is clear that EnCase software meets the standards under both Rule 901 and *Daubert*,[61] the trend of the courts is to include "non-scientific" technical evidence within the purview of *Daubert/Frye*, in addition to the purely scientific forms of evidence, such as DNA analysis, that are more traditionally subject to *Daubert*. The judicial analysis applied in notable challenges to EnCase software is clearly consistent with this trend. As such, a computer forensics examiner should be very familiar with the basic elements of the *Daubert* analysis, which are as follows:

1. Whether a "theory or technique … can be (and has been) tested;"
2. Whether it "has been subjected to peer review and publication;"
3. Whether, in respect to a particular technique, there is a high "known or potential rate of error;" and
4. Whether the theory or technique enjoys "general acceptance" within the "relevant scientific community."[62]

Under the first prong of the test, courts have expressly noted that EnCase software is a commercially available program that can be easily tested and validated. This is in contrast to tools that are not commercially available to the general public or are custom tools with arcane command-line functionality that are not easily tested by third parties unfamiliar with those processes. The law is clear that in the context of computer-generated evidence, the courts favor commercially available and standard software.[63]

Further, many agencies have tested EnCase software in their labs before standardizing their agents on use of the software. Importantly, the widespread adoption of EnCase software by the computer forensics community serves as a crucial factor for authentication, as the community generally knows the capabilities and accuracy of the program through such extensive usage. Additionally, many publications have featured EnCase software as the highest-rated tool in testing and comparisons among other commercially available software tools.[64]

These reviews are among several industry publications featuring EnCase software, and are relevant to the second prong of the *Daubert* test. Peer review and publication in the relevant industry is an important factor looked to by the courts in considering the validity of a technical process under

61 526 U.S. 137 (1999).

62 Daubert, 509 U.S. at 592-94.

63 See, e.g., United States v. Liebert, 519 F.2d 542, 547 (3rd Cir. 1975) (holding that computer evidence was admissible in criminal trial provided that prosecution lays a sufficient foundation to warrant a finding that such information is trustworthy and the defense is given the same opportunity to inquire into the accuracy of the computer system involved in producing such evidence). See also, United States v. Weatherspoon, 581 F.2d 595, 598 (7th Cir. 1978).

64 Test Center- GETTING THE HARD FACTS, SC Magazine, April 2001 (Testing of Computer Forensics analysis tools reported in the leading publication in the IT Security industry. EnCase receives the highest rating over the other tested programs, noting: "If you work doing forensic analysis of media on a regular basis, you must have this tool.") See also Group Test 1: Data Forensics, SC Magazine, Oct. 2003, (EnCase received a 5-star rating -- "**VERDICT:** Sets the standard for other forensic products. Definitely the best option for professional forensics investigations.").

Daubert/Frye. Various published articles in the information security and high-tech crime investigation industries favorably review or mention EnCase software.[65]

It is important for computer forensic examiners to keep abreast of peer review of computer forensic tools in industry publications. Examiners should also be cognizant of whether developers decline invitations from respected industry publications to participate in testing and peer-review opportunities, as such refusals could raise questions regarding the validity of such tools.

An important peer-review article that appeared in *The Computer Paper*, Canada's leading information technology (IT) publication, illustrates how peer review is also an important source to establish general acceptance and industry trends:

> Because courts around the world have accepted EnCase as a standard, commercially available forensic software application, defense attorneys have switched from attacking the accuracy of the software to attacking the methodology of the operator, or forensic technician. This makes training important—and is also the reason why Guidance Software has an extensive and busy training facility in California.[66]

It is not uncommon for investigators to be asked to testify to specific examples of peer review and publication of technical or scientific processes. For instance, in *People v. Rodriguez*,[67] a case in Sonoma County, California, where EnCase software was subjected to a *Frye* analysis, the district attorney investigator referenced in his testimony the above-mentioned IEEE Computer Society article, as well as other published articles. Often, testifying experts will bring copies of relevant articles from industry publications to court for admission into evidence as part of the validation process.

The prosecution in *Rodriguez* also provided testimony that there were no known reports of a high potential rate of error regarding EnCase software. While all software programs contain bugs to varying degrees, the various tests and extensive usage of EnCase software reveal that the program does not have a high error rate, especially in contrast to other available tools. Additionally, it is important for an investigator to be able to point to either his/her own testing of EnCase software or that performed by his/her agency. In a detailed and documented published testing of computer forensic software, leading IT-security publication *SC Magazine* noted in 2001 that EnCase Forensic Edition "outperformed all the other tools" that were tested by the magazine, and in a report on its group test of data forensics in 2003, noted that EnCase software "sets the standard for other forensic products" and is "[d]efinitely the best option for professional forensics investigations."[68]

Courts have referred to the need for a body of data from "meaningful testing" efforts to guide them in their *Daubert* analysis. There is no requirement for a regimented and universal standard

---

65 In addition to the SC Magazine test reviews in 2001 and 2003 noted above, EnCase has received dozens of favorable reviews and mentions in industry publications, which are available for review and download at: http://www.encase.com/corporate/news/index.shtm

66 Dave Chappelle, Sherlock Holmes meets data, The Computer Paper, Dec. 5 2002.

67 No. SCR-28424 (Cal. Supr. Ct. Cty. Sonoma Jan. 11, 2001).

68 Test Center- GETTING THE HARD FACTS, SC Magazine, April 2001; Group Test 1: Data Forensics, SC Magazine, Oct. 2003.

for such testing agreed on by all the experts in the field. However, any testing should be meaningful and objective, subject to the same peer review as the tools and processes being analyzed. Further, professional testing ideally culminates in the preparation of a detailed report or white paper, allowing for proper analysis and comment. In *United States v. Saelee,*[69] the court noted that peer review should be conducted by "disinterested parties, such as academics." Needless to say, the more thoroughly a tool has been tested, and the wider its acceptance within the relevant community, the more likely it is to withstand a *Daubert* challenge.

At one time, there was only a limited amount of published testing concerning computer forensics tools. Although many large agencies had conducted successful tests with EnCase software, often they had not published their results. Additionally, tests that had been conducted were often problematic, because it is difficult to determine whether a particular tool has a high rate of error unless the testing process and methodologies are disclosed and documented in full. It is also difficult to define a "high rate of error" when many developers of popular forensic tools declined to allow testing of their tools, depriving the analysis of a wider field of comparison.

In 2003, however, the published testing landscape changed considerably when the National Institute of Standards and Technology (NIST) published the results of its extensive testing of computer forensics tools under its Computer Forensics Tools Testing Project. The rigorous and comprehensive testing revealed no flaws in the EnCase imaging engine, as reflected in the NIST report "Test Results for Disk Imaging Tools: EnCase 3.20."[70] (Note that there have been no substantial changes made to the imaging engine portion of the EnCase code since Version 3.20).

The NIST testing process for EnCase software was remarkably comprehensive, involving over fifty separate test scenarios of IDE and SCSI hard drives, including using the FastBloc® hardware write-blocking device. All performed NIST testing was disclosed in the report. In addition:

- EnCase software flawlessly imaged all sectors and achieved expected results on tests utilizing direct disk access mode. EnCase flawlessly imaged all sectors and achieved expected results on tests utilizing BIOS disk access with one exception. There was one reported anomaly when accessing IDE drives on an older computer using a legacy BIOS. This anomaly reflects a flaw in the legacy BIOS technology. As noted by the NIST Report, Guidance Software has previously addressed this limitation of legacy BIOS technology by easily enabling direct disk access through the ATAPI interface.

- EnCase software properly verified the imaged media in all such test scenarios.

- EnCase software properly reported and logged I/0 errors during the imaging process in all such test scenarios.

69 162 F. Supp. 2d 1097, 1103 (D. Alaska 2001).

70 The final report can be obtained from the National Institute of Justice web site at http://www.ojp.usdoj.gov/nij/pubs-sum/200031.htm.

- EnCase software properly detected and reported verification errors when the image files were intentionally altered by a disk editor.

- Two items were noted regarding the restore function, which is not related to the imaging process and were solely reflective of the limitations of the Windows operating systems.

- The three identified anomalies in the report reflected limitations of third-party technology, with proper workarounds documented. The results of this report establish that no changes or modifications to the code of the EnCase imaging engine is warranted.

In short, the NIST testing is an example of the sort of scientific, independent, thorough, and fully disclosed testing that had been lacking in the computer forensics industry. It should further aid the already widespread court acceptance of EnCase software under the *Daubert* standard.

The final prong—whether a process enjoys "general acceptance" within the "relevant scientific community"—is a particularly important factor strongly considered by the courts in validating scientific tools and processes. "`[A] known technique that has been able to attract only minimal support within the community,' . . . may properly be viewed with skepticism."[71] EnCase software is without question the most widely used computer forensics technology and process in the field. Thousands of law enforcement agencies and companies worldwide employ EnCase software for their computer investigations. In addition, EnCase software has over twenty thousand users, and Guidance Software trains more than five thousand students annually in the use of EnCase software, with over 50,000 digital investigators trained as of 2012.

The widespread general acceptance of a process is often considered to be the most important prong in a *Daubert/Frye* analysis. In addition, even outside the litigation context, there are practical considerations: if it should become necessary to replace an expert, his or her use of standard software will make the transition to a replacement expert much easier.

In the case of many other technical processes, counsel will often struggle to establish that all the *Daubert* factors are sufficiently met. However, it is difficult to imagine any other computer forensics process that could better qualify under the *Daubert/Frye* analysis. In fact, more than one court has taken judicial notice of the established reliability of EnCase software. Black's Law Dictionary defines judicial notice as the act by a court to "recognize the existence and truth of certain facts, having bearing on the controversy at bar, which, from their nature, are not properly the subject of testimony, or which are universally regarded as established by common notoriety." Importantly, more than one court has adopted this standard for EnCase software.

In *Sanders v. State*[72], the Texas Court of Appeals reaffirmed the reliability and accuracy of EnCase Forensic software after the defendant challenged the evidence on the *pro forma* assertion that the State failed to show that the software they used during their investigation was reliable and accurate.

At trial, the State's forensic expert explained that EnCase Forensic took an image of Sander's hard

71 Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993).

72 191 S.W.3d 272 (Tex. App. 2006), cert. denied, 549 U.S. 1167 (2007).

drive and used a MD5 hash to validate the image. The expert stated that using an MD5 hash ensures that there is no possibility an error could occur during the investigation process. The Sanders court utilized the three-prong test set forth in *Kelly v. State* (the Texas state court *Daubert/Frye* test) in determining the admissibility of evidence retrieved with EnCase. The *Kelly* test determines the reliability and, ultimately, admissibility of evidence obtained through scientific analysis. In *Williford v. State*, a case with a similar fact pattern, the court approved the use of EnCase software after detailing the software's compliance with each factor of the *Kelly* test. After performing a shallow *Kelly* analysis and citing *Williford*, the appellate court affirmed the trial court's admittance of the evidence retrieved with EnCase. EnCase software was held to be a reliable means of obtaining digital evidence from a defendant's computer system.

In a very important and notable development, the *Sanders* court took judicial notice of prior court cases which validated EnCase software: "once some courts have, through a *Daubert/Kelly* 'gate keeping' hearing, determined the scientific reliability and validity of a specific methodology to implement or test the particular scientific theory, other courts may take judicial notice of the reliability (or unreliability) of that particular methodology."

In another case, a trial court also took judicial notice that EnCase software is a commercially available tool with widespread general acceptance.[73] As such, counsel should seek judicial notice from the court under the authority of *Sanders v. State* as a means to respond to any pro forma challenge to EnCase software .[74]

The defendant ultimately appealed this case to the United States Supreme Court. One of the stated grounds of appeal was a challenge to the appellate court's judicial notice finding regarding the reliability of EnCase. In January 2007, the Supreme Court denied to hear this appeal (certiorari petition), thus allowing the Texas appellate court's decision to stand.[75] The Supreme Court's denial of the defendant's certiorari petition gives even stronger weight to this important decision regarding the established acceptance and reliability of EnCase software.

§ 2.2 Computer Forensics as an Automated Process

Federal Rule of Evidence 901(b)(9) provides a presumption of authenticity to evidence generated by or resulting from a largely automated process or system that is shown to produce an accurate result. This rule is often cited in the context of computer-processed evidence.[76]

---

73 State of Washington v. Leavell (Okanogan County, Washington Superior Ct. no. 00-1-0026-8).

74 Judicial Notice is the act of a court recognizing the existence and truth of certain facts relevant to the case at bar. Such notice excuses a party from having the burden of establishing fact from necessity of producing formal proof.

75 Sanders v. Texas, 191 S.W.3d 272 (Tex. App. 2006), cert. denied, 549 U.S. 1167 (2007).

76 "Thus, evidence describing, for example, the process of creating x-rays, photographs, tape recordings, computer generated records, radar records, or scientific surveys when coupled with evidence showing that a particular process or system produces an accurate result when correctly employed and properly operated and that the process or system was in fact so employed and operated constitutes sufficient evidence that the result is what it purports to be." Wright & Miller, Fed. Prac. & Proc. Evid. § 6830; Notes of the Advisory Committee regarding Rule 901(b)(9); see also, People v. Lugashi, 252 Cal. Rptr. 434 (Ct. App. 1988) (data-collection software program presumed accurate); People v. Mormon , 422 N.E.2d 1065, 1073 (Ill. 1981) (data-retrieval program presumed accurate); Mark D. Robins, Computers and the Discovery of Evidence – A New Dimension to Civil Procedure, 17 J. Marshall J. Computer & Info. L. 411, 507-08 (1999).

There is some debate as to whether testimony from computer forensics examiners should be considered expert scientific testimony, and thus subject to an analysis under *Daubert*, or non-scientific technical testimony regarding the recovery of data through a technical investigation process, and thus subject to Federal Rule of Evidence 901(a), 901(b)(9). The United States Supreme Court blurred this distinction between scientific vs. non-scientific expert testimony in its *Kumho Tire Company, Ltd. v. Carmichael*,[77] which extended the *Daubert* test to cover technical processes as well as scientific opinion evidence. However, many courts still draw a general distinction between scientific and non-scientific expert testimony.[78]

At least one federal appeals case has referred to this issue in *dicta*, hypothesizing that in light of Rule 901(b)(9), computer or x-ray evidence resulting from a process or system would not fall under a *Frye* analysis as "[t]he underlying principles behind x-ray and computers are well understood; as to these technologies, serious questions of accuracy and reliability arise, if at all, only in connection with their application in a particular instance."[79] The court in *United States v. Whitaker*,[80] held that, without addressing *Daubert,* a foundation for forensically recovered computer evidence could be established by the investigating agent with personal knowledge of the process used to retrieve and print the data.[81]

As noted by the court in *Lorraine v. Markel*, Rule 901(b)(9) was designed in part to account for computer evidence. The *Lorraine* court noted that this was an important method to authenticate electronically-stored information. "Rule 901(b)(9), which is designated as an example of a satisfactory authentication, describes the appropriate authentication for results of a process or system and contemplates evidence describing the process or system used to achieve a result and demonstration that the result is accurate. The advisory committee note makes plain that Rule 901(b)(9) was designed to encompass computer-generated evidence . . .")

In *United States v. Quinn*,[82] the prosecution sought to introduce "photogrammetry" evidence through expert testimony to determine the height of a suspect from surveillance photographs. The trial court allowed the testimony after a simple proffer from the government as to the basis of a photogrammetry process, which the court found to be "nothing more than a series of computer-assisted calculations that did not involve any novel or questionable scientific technique."[83]

The Court of Appeals rejected the defendant's contention that the photogrammetric evidence required an evidentiary hearing under *Daubert*, finding that the trial court acted within its discretion.[84] In *Burleson v. State,*[85] the court held that expert testimony resulting from a complicated computer-generated display showing deleted records was admissible, as the software and computer systems

77 526 U.S. 137 (1999).

78 An excellent discussion of this debate can be found at 31 Federal Practice and Procedure § 7114, Wright & Miller, (2000 Revision), where the authors identify an apparent conflict between the application of Daubert and 901(b)(9).

79 United States v. Downing, 753 F.2d 1224, 1240, fn. 21, (3rd Cir. 1985).

80 127 F.3d 595 (7th Cir.1997).

81 United States v. Whitaker, supra, 127 F.3d at 600.

82 18 F.3d 1461 (9th Cir. 1994).

83 United States v. Quinn, supra, 18 F.3d at 1465.

84 Id.

85 802 S.W.2d 429 (Tx. Ct. App. 1991).

creating the output relied upon by the expert were shown to be standard, accurate and reliable. The court noted that it was unnecessary for the computer system technology to be authenticated under a *Frye* test, finding that the showing of an accurate and reliable system producing the display was sufficient.[86]

In *State (Ohio) v. Cook,* an Ohio Appellate Court upheld the validity of EnCase software, citing, in part, Ohio Rule of Evidence 901(b)(9), which is nearly identical to the corresponding federal rule.

NOTE: Please see Chapter 6 for a detailed analysis of *State v. Cook* and other cases addressing the validity of the EnCase process.

EnCase software is proven to provide an accurate, objective, and complete search-and-recovery process through a substantially automated process. In complex computer forensics cases, evidence concerning the search-and-recovery function and its resulting visual outputs and printed reports is often as important as the recovered data itself.

Some tools exclusively employed by a minority of computer forensics examiners are little more than basic single-function DOS disk utilities that, when combined as a non-integrated suite, are manipulated to perform computer forensic applications. This once common practice presents three fundamental problems:

1. Results from the examiner's search and recovery process are often subjective, incomplete and variant;
2. The data-restoration process can either improperly alter the evidence on the evidentiary image copy or provide a visual output that is not a complete and accurate reflection of the data contained on the target media; and
3. The lack of integration of all essential forensic functions within a single software application presents potential challenges to the authenticity of the processed computer evidence.

Applying Rule 901(b)(9) to the context of electronic data discovery, computer forensic software should provide an objective and automated search and a data-restoration process that facilitates consistency and accuracy.

For example, a group of ten qualified and independently operating forensics examiners analyzing the same evidentiary image should achieve virtually the same search results when entering identical text search keywords or seeking to recover all specified file types on the image, such as all graphical images or all spreadsheet files. If not, the process employed cannot be considered to be either automated or accurate and thus would not be considered a process qualifying for a presumption of authenticity under Rule 901(b)(9).

Further, it is often necessary to duplicate search-processing results during or before trial, and thus

86 Burleson v. State, supra, 802 S.W.2d at 441.

if a colleague or, even worse, an opposing expert obtains significantly differing search results from the same media, the impact or even the very foundation of the evidence may be substantially weakened. While the court in *Gates Rubber* did not expressly cite Rule 901(b)(9), its holding that a computer examiner has "a duty to utilize the method which would yield the most complete and accurate results" is clearly consistent with the statute.

Results from search-and-recovery procedures using DOS utilities will significantly vary depending upon the type and sequence of non-integrated utilities employed; the amount of media to be searched; and the skill, biases, and time availability of the examiner. Further, each piece of acquired media must be searched separately, using the same tedious and time-consuming protocol for each hard drive, floppy disk, CD, or other media involved in the case. In sum, the likelihood of different independently operating examiners duplicating the search and restoration process on the same evidentiary image is extremely remote, if not impossible.

Due to the inordinate burden of searching a Windows image with DOS utilities, some investigators resort to operating Windows Explorer on the evidentiary image disk. In addition to not being able to view file slack, swap files and all other types of unallocated data, Explorer will corrupt the data in such a situation by altering file date stamps, temporary files, and other transient information.

Better practice requires the use of specially designed Windows-based computer forensics software that employs a completely non-invasive and largely automated search process. A more objective search process facilitates results that are more accurate and consistent, thereby enabling duplication of the process at trial and by independently operating examiners. For example, when using EnCase software, simply clicking a request to display all graphical image files contained on an evidentiary image disk will instantaneously list all such files in a graphic interface. The list will include those files that have been "re-named" or hidden in obscure directories by a party attempting to conceal them, and even, in most cases, previously deleted files.

EnCase software duplicates the Windows Explorer interface and viewing functions, with the critical added benefits of viewing deleted files and all other unallocated data, in a completely non-invasive manner. An EnCase search process often significantly reduces an examiner's lab analysis time. Most importantly, an examiner can present the discovered evidence in court with confidence that the search-and-recovery process provides complete, consistent, and objective results.

It should be noted that the line of cases that applied rule 901(a)(b) discussed above preceded *Kumho Tire*, which, as also noted above, extended the *Daubert* test to technical processes as well as scientific opinion evidence. EnCase software has been authenticated at trial under both *Daubert/Frye* and Rule 901(b)(9), and it is advisable that both approaches be considered in authenticating the software.

§ 2.3 Commercial vs. Custom Forensics Software and Authentication Issues

Some computer forensics investigations utilize custom software tools developed by the investigating agency or a private company that are not commercially available to the general public. Courts have addressed issues concerning the type of software involved where computer-generated evidence is at

issue. Such cases provide a presumption of authenticity for evidence resulting from or processed by commercially available computer systems and software over customized systems and software. As noted by one respected treatise on the subject:

> "Evidence generated through the use of standard, generally available software is easier to admit than evidence generated with custom software. The reason lies in the fact that the capabilities of commercially marketed software packages are well known and cannot normally be manipulated to produce aberrant results. Custom software, on the other hand, must be carefully analyzed by an expert programmer to ensure that the evidence being generated by the computer is in reality what it appears to be. Nonstandard or custom software can be made to do a host of things that would be undetectable to anyone except the most highly trained programmer who can break down the program using source codes and verify that the program operates as represented."[87]

In fact, courts in many jurisdictions actually require that any computer-generated evidence be a product of a "standard" computer program or system in order to admit such evidence.[88] This body of authority would seem especially relevant to software used by law enforcement for computer forensics purposes, given the sensitive function of such software. A law enforcement agency that utilized customized proprietary software for computer forensic investigations could face various complications when seeking to introduce evidence processed with such software. Such actual or potential pitfalls could include the following:

1. The defense could seek to exclude the results of any computer investigation that utilized tools that were inaccessible to non-law enforcement. Federal courts are unanimous in holding that computer evidence generated by or resulting from a process is only admissible if the defense has access to such software in order to independently duplicate the results of that process and thus "is given the same opportunity to inquire into the accuracy of the computer system involved in producing such evidence."[89]
2. If the defense is provided with a copy of the proprietary software and all evidentiary images, an expert retained by the defense will require substantial time to learn the software and recreate the process, resulting in substantial cost to the government in cases involving indigent defendants. The government will incur even further costs if the purchase of supporting operating systems and file servers is required to support the custom software.

While, as noted above, the source code for commercially available software is not required to be introduced into evidence in order to establish the authenticity of computer-processed evidence, it is

87 71 Am.Jur. Trials 111 § 118 (1999).

88 Weisman v. Hopf-Himsel, Inc., 535 N.E. 2d 1222, 1226 (Ind. Ct. App. 1st Dist. 1989); People v. Bovio, 455 N.E.2d 829, 833 (Ill. App 1983); Burleson v. State, supra, 802 S.W.2d at 441; People v. Lombardi, 711 N.E.2d 426 (Ill. App 1999).

89 United States v. Liebert, 519 F.2d 542, 547 (3rd Cir. 1975); United States v. Weatherspoon, 581 F.2d 595, 598 (7th Cir. 1978).

apparent that such presumptions of authenticity would not be afforded to *customized* software. Thus, the defense would seek to exclude the results of any computer investigation using custom software tools, unless the source code was made available to the defense for testing and analysis. While theoretically possible, given the copyright holder's strong commercial interest in protecting the source code, it is unlikely that the source code will be released.

Conversely, when questioned in court regarding the reliability of a commercially available software application such as EnCase, the proponent of the evidence can testify that EnCase software is a widely used and commercially available software program and thus any member of the public can purchase, use and test the program. The defense could not claim prejudice by the use of EnCase software, as any reasonably skilled computer examiner would be able to examine the discovery copy of the evidence, nor would the government be subject to questions regarding its access to the source code of the program. The Indiana Court of Appeals directly confronted these issues in the case of *Logan v. State*[90]:

> On August 14, 2003, Logan filed a motion for discovery requesting production of the computer program the State used to discover evidence on the computer. The State failed to produce the computer program, known as iLook, even after the trial court entered an order compelling production.
>
> On January 20, 2004, Logan moved to dismiss the charges based upon First Amendment grounds. On February 20, 2004, the State dismissed the charges and refiled charges using a different forensic computer program, called EnCase. On April 6, 2004, approximately sixty days prior to trial, the State provided Logan with a copy of the EnCase program, thereby complying with the court's discovery order.[91]

As the *Logan* case illustrates, using software that is not commercially available can result in discovery challenges. The resulting delays can imperil the prosecution's case by negatively impacting the defendant's right to a speedy trial.

Even in the civil litigation arena, using custom software can prove problematic. For instance, in the high-profile case of *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, which resulted in a jury verdict of $1.4 billion, Morgan Stanley was strongly criticized by the court because software it had written to collect electronic information had missed thousands of relevant e-mails.

NOTE: Please see Chapter 9 for a detailed discussion of *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*

---

90 Logan v. State, No. 46A03-0502-CR-50, 2005 WL 2840283 (Ind.App. Oct. 31, 2005).
91 Id. at 1.

3. Expert Witness Testimony

§ 3.0 Overview

Are computer forensics investigators considered experts? Many courts outside of the United States, e.g. in the United Kingdom, employ a higher threshold when determining whether a proposed expert is qualified to testify regarding a technical subject. This chapter will discuss the threshold for qualifying a computer investigator as an expert and discuss some cases where the court addressed this issue. This chapter also includes two fictional transcripts of sample direct examinations.

The first example is a transcript from a mock pre-trial evidentiary hearing under either Federal Rules of Evidence 104, 702 and/or *Daubert v. Merrell Dow Pharmaceuticals*. A court may schedule such an evidentiary hearing to consider any foundational questions regarding the EnCase process. The second example is a direct examination in the context of a jury trial presenting evidence obtained from a computer forensic examination.

Although these are only examples, they are based upon actual investigation procedures and techniques taught in Guidance Software's training program and employed every day by hundreds of agencies and organizations. These examples are not mandatory scripts to be strictly followed, but provide a general reference for prosecutors in preparing direct examinations of their computer examiners in the context of either an evidentiary hearing or a jury trial.

§ 3.1 Threshold Under Rule 702

In the United States, *Federal Rule of Evidence* 702 provides that, in order for a witness to be qualified as an expert, the expert must simply be shown to have "knowledge, skill, experience, training, or education" regarding the subject matter involved. Under this standard, trained computer forensics experts have qualified as experts in the United States courts. However, oftentimes prosecutors opt not to offer the examiner as an expert, especially where the records in question can be authenticated under Federal Rule of Evidence 901(b)(9) or a corresponding state statute, or where the examiner can be offered as a percipient witness presenting more objective and empirical findings of his or her investigation. This approach tends to be more prevalent in state courts.

In *United States v. Scott-Emuakpor*[92] the court considered whether the United States Secret Service agents who conducted the computer forensic examination needed to be qualified experts in computer science to present their findings. The defendant brought a motion *in limine* contending that the agents' testimony regarding the results of their computer examinations should not be admitted because one

92 2000 WL 288443 (W.D. Mich. 2000).

of the agents admitted that he was not an expert in the area of computer science. Nevertheless, the court opined that:

"[T]here is no reason why either witness may not testify about what they did in examining the computer equipment and the results of their examinations. The question before the Court at this time is not whether these witnesses have the expertise, for example, to develop sophisticated software programs. The question is whether they have the skill to find out what is on a hard drive or a zip drive. Apparently, they have this skill because they determined what was on the drives. By analogy, a person need not be an expert on English literature in order to know how to read . . . .The fact that (the USSS agent) admitted that he is not an expert in the area of computer science is not binding on the Court."

The court in *Galaxy Computer Services, Inc. v. Baker*[93] reached a similar result. In *Galaxy*, the defendants had filed a motion *in limine* seeking to bar the expert opinion testimony of Paul Taylor. Taylor, who had worked in the field of computer forensics for five years, had analyzed nine hard drives and prepared an expert report detailing the defendants' deletion of certain files. Plaintiff offered Taylor's testimony both to authenticate the recovered documents and to permit jury instructions on spoliation of evidence and consciousness of wrongdoing.[94] As described by the court:

> Defendants argue that Taylor is not qualified to testify as a computer expert because: (1) none of his degrees are in computer science; (2) he is not fluent in any computer language; (3) he is not a computer programmer; (4) he holds no certificates in computer science; and (5) he possesses no training or special education for Microsoft certification . . . .
>
> The Court finds that Taylor qualifies as an expert based on his knowledge, skill, experience, training and education. **The field of computer forensics does not require a background in computer programming or reading and writing code.** Taylor has been working in the field of computer forensics for five years. During this period, he has completed between 1,600 and 1,700 forensic reports based on his findings, some of which have been accepted by various courts.[95] [emphasis added]

It is not uncommon for an examiner to be asked to interpret the recovered data. The case of *United States v. Hilton*[96] provides a very good example of a computer forensics examiner offering expert-witness testimony to interpret the data collected from his examination. Among the issues in *Hilton* was whether the defendant had utilized interstate commerce (i.e. the Internet) in the process of distributing child pornography, thereby satisfying a key element and requirement of the statute. The computer investigator from the United States Customs Service testified that the images in question were located in a subdirectory named "MIRC," which contained software and files related to "IRC" (Internet Relay Chat). The Special Agent testified that, in his expert opinion, because the contraband

93 Galaxy Computer Services, Inc. v. Baker, 325 B.R. 544 (E.D.Va. 2005).

94 Id. at 562.

95 Id. at 563 [Emphasis added].

96 257 F.3d 50 (1st Cir. 2001).

was located in the MIRC subdirectory that contained Internet chat-related files, the images were likely associated with the Internet.

The special agent also testified that the file time and date stamps reflecting the creation time of each of the subject images indicated that the defendant downloaded the images from the Internet via a modem. The special agent based this conclusion on the fact that the images were created on the defendant's computer at intervals of time consistent with downloading the images via a modem. The special agent's expert testimony, among other factors, convinced the court the subject images were transmitted to the defendant's computer via the Internet, thereby satisfying the interstate commerce requirement of section 18 U.S.C. § 2252A(a)(5)(B).

In *United States v. Ganier*[97], the Sixth Circuit Court of Appeals classified the proposed testimony of a government-retained forensic computer specialist as expert testimony, thereby subjecting it to pre-trial disclosure requirements under Federal Rule of Criminal Procedure 16(a)(1)(G). The government unsuccessfully asserted that the federal law enforcement examiner's testimony based upon his created report was not "scientific, technical, or specialized knowledge," but instead mere facts that could be observed by any layperson and therefore was not subject to Rule 16 disclosure. In reply, the Court's stated:

> The reports generated by the forensic software display a heading, a string of words and symbols, date and time, and a list of words… The government asserts that these reports reveal three different types of searches performed with particular search terms at particular times, but such an interpretation would require (the examiner) to apply knowledge and familiarity with computers and the particular forensic software well beyond that of the average layperson. This constitutes "scientific, technical, or other specialized knowledge" within the scope of Rule 702. [98]

However, a somewhat different result was reached in *Furmanite America, Inc. v. T.D. Williamson, Inc.*,[99] where the party seeking to introduce the testimony of its retained computer forensics consultant failed to timely designate the witness for trial as an expert under Federal Rule of Civil Procedure 26, but timely disclosed the witness as a fact witness for the scheduled trial. The court found that a computer forensics specialist could be a fact witness as to certain matters and an expert witness as to others:

> "The Court finds that Mr. Lakes is a fact witness, properly disclosed as such to TDW, and thus will be permitted to testify at trial as to factual matters such as what he ascertained from Furmanite's computers when initially engaged to examine them. However, because Mr. Lakes was not timely disclosed as an expert witness and did not prepare an expert witness report in accordance with the Court's Case Management and Scheduling Order, he will not be permitted to testify as an expert at trial or provide expert opinion.

97 468 F.3d 920 (6th Cir. 2006).

98 Id. at 926.

99 506 F.Supp.2d 1126 (M.D.Fla.,2007)

> Mr. Lakes cannot be asked his expert opinion regarding the highly technical question of whether and when a defendant performed a 'selective restoration' of a computer's hard drive in order to maliciously overwrite data on a misappropriated laptop computer. Rather, the scope of Mr. Lakes' testimony, as disclosed by Furmanite, is simply to testify regarding the information on Furmanite's computers. Thus, Mr. Lakes is permitted to testify regarding the data obtained from such computers, the dates of the elimination of material from such computers, if based on fact and not opinion, and the procedures used to extract such information. Expert opinion testimony by this witness, however, will not be permitted."[100]

The decision of the *Furmanite* court establishes that a computer forensics professional who performs basic copying, imaging, searching, collection and production of data arguably is not necessarily performing such duties as an expert witness, and thus can present his or her results as a fact witness. However, if that professional needs to conduct detailed analysis of the recovered data or interpretation of reports and other analysis, then the witness would likely be offering expert testimony.

§ 3.2 Importance of Well-Established Certifications, such as the EnCE for Expert Testimony

Courts increasingly recognize the importance of well-established certifications, such as the EnCase Certified Forensic Examiner ("EnCE") for purposes of establishing the admissibility of computer evidence. For example, in *Commonwealth v. Piasecki*,[101] the defendant appealed a conviction of sexual abuse of children and possession of child pornography. The court affirmed the conviction and provided a detailed description of the process police used to obtain and examine the defendant's computers. The court observed that the agent responsible for performing the analysis was an expert in computer forensics and an EnCase Certified Examiner (EnCE).

§ 3.3 Illustrations of Testimony

DIRECT EXAMINATION -- PRE-TRIAL EVIDENTIARY HEARING

A. PREFACE

If any challenge is raised to the qualifications of the computer examiner or the foundation of the evidence concerning the tools or methodologies used in the course of a computer forensics investigation, many prosecutors prefer to address such objections outside the presence of the jury through a hearing initiated under Federal Rule of Evidence 702, Rule 104 or *Daubert*. Judges are typically more receptive toward technical evidence and it is obviously desirable to avoid presenting complex testimony on contested technical issues before a jury by resolving such foundational issues in

100 Id. at 1133

101 2010 Pa. Dist. & Cnty. Dec. LEXIS 618 (Common Pleas Ct. Bucks Cty, PA, Crim. Div. 2010)

a separate hearing beforehand. The following fictional "mock trial" direct examination is designed to illustrate how a proper foundation may be established for the EnCase process under both Rule 901(b)(9) and *Daubert*. For illustration purposes, the below example contains more detail than what would normally be presented on direct examination, even in the context of a court trial or hearing. However, much of the information may be useful for re-direct examination.

B. BACKGROUND

[After stating name for the record]

Q: Sir, are you a Senior Special Agent for the United States Customs Service?

A: Yes I am.

Q: And do you have any specialized duties as a Customs agent?

A: I am a computer evidence examiner certified as a Seized Computer Evidence Recovery Specialist by the United States Department of the Treasury.

Q: Please tell us how long you have been a computer evidence examiner.

A: I have been a Seized Computer Evidence Recovery Specialist with Customs for eight years.

Q: Tell us about your educational background.

A: I received a Bachelor of Science degree in electrical engineering from University of _____ in 19__.

Q: And could you briefly describe your training for the handling and examination of computer evidence?

A: In 19__ I received three-weeks of intensive training, known as Seized Computer Evidence Recovery Specialist training, at the Federal Law Enforcement Training Center. In 19__ I obtained Computer Forensic Examiner Certification from the International Association of Computer Investigative Specialists, known as IACIS, after receiving two weeks of their intensive training. The next year I received Advanced Course Certification from IACIS after taking their two-week advanced training course. I have also received computer forensic training from The National Consortium for Justice Information and Statistics, known as SEARCH and have received training from Guidance Software on their EnCase computer forensic application.

Q: Are you a member of any professional organizations?

A: Yes I am.

Q: Which ones?

A: I am a member of the International Association of Computer Investigative Specialists, and the High Tech Crime Investigation Association.

C. OVERVIEW OF COMPUTER FORENSICS

Q: You mentioned the subject of computer forensics. Can you provide an overview of what computer forensics is?

A: Computer forensics is the acquisition, authentication, and reconstruction of electronic information stored on computer media, such as hard drives, floppy disks or zip drives. A computer forensics technician is needed whenever there is evidence stored in a computer.

Q: Can you briefly tell us how a computer forensics specialist such as yourself conducts a typical investigation?

A: First, the electronic information contained on computer storage media must be acquired by making a complete physical copy of every bit of data located on computer media in a manner that does not alter that information in any way. Then the information must be authenticated in a special process that establishes that the acquired electronic information remained completely unaltered from the time the examiner acquired it. Finally, the examiner must use special software and processes to recover and reconstruct the information in its forensic state, even if such information is found in files that have been deleted by the user.

D. THE ACQUISITION PROCESS

Q: You described three basic steps, and I want to discuss them one at a time beginning with the acquisition process. How is digital information copied from computer media in a proper forensic manner?

A: Specialized computer forensics software, such as EnCase, utilizes a special boot process that ensures the data on the subject computer is not changed. After the boot procedure is initiated, the examiner utilizes the forensics software to create a complete forensic image copy or "exact snapshot" of a targeted piece of computer media, such as a hard drive, or external media, such as floppy or zip disks. This forensic image is a complete sector-by-sector copy of all data contained on the target media and thus all information, including available information from deleted files, is included in the forensic image created by the examiner.

E. THE AUTHENTICATION PROCESS

Q: The second step you mentioned was the authentication process. Please briefly describe how the acquired electronic information is authenticated and verified.

A: Computer forensics examiners rely upon software that generates a mathematical value based upon the exact content of the information contained in the forensic image copy of the seized computer media. This value is known as an MD5 hash value and is often referred to as a special type of digital signature. The same software also verifies that this value remains the same from the time it is generated. If one bit of data on the forensic image copy is subsequently altered in any way, meaning that even if a single character is changed or one space of text is added, this value changes. So if the hash value of the information contained on seized media remains the same, then it is established that the electronic data has not been altered in any way.

Q: What are the odds of two forensic images with different contents having the same hash value?

A: The odds of two computer files, including a forensic image file, with different contents having the same hash value is roughly ten raised to the 38th power. If you wrote out that number, it would be a one followed by 38 zeros. By contrast, the number one trillion written out is one followed by only twelve zeros.

F. THE RECOVERY PROCESS

Q: Because the third step of data recovery is complex, I am going to first ask you a few basic questions about how a computer works. First, and without being too technical, could you give us a description of how information on a hard drive is stored by the computer?

A: Yes. Basically, computer disks are storage media that are divided into concentric circles or tracks. This can be thought of as a small version of the old 78 rpm records people used to play on phonographs. The tracks are divided into sectors. Each sector has its own address, a number that is unique to that part of the disk. The operating system assigns and stores the address, so that it may retrieve all information constituting a computer file stored in a specific sector when requested by the user.

Q: How is the information recorded on the hard disk?

A: The disk is covered with a thin coat of magnetic material. When information is written to the disk, the data is recorded by magnetizing specific parts of the disk coating. The information resides there until it is overwritten.

Q: Thank you. I think we have the basic idea. I am very interested in how a computer technician can recover electronic information that has been deleted or automatically purged. Please tell us what is involved in this process.

A: When the computer user deletes electronic information, it is often assumed that the information is removed from the computer forever. That is not necessarily true. The information is still in the computer; only it is now marked by the computer to allow it to be overwritten. A general analogy would be a library card catalogue system, where the books represent files and the card catalogue represents the file directory with information as to where the files are located on the disk. When a file is deleted, its location information is removed from the card catalogue index, but the book remains on the shelf until another book randomly replaces it.

Q: To what extent can this deleted information be retrieved?

A: If the information has not yet been overwritten by other data, it is still there and can be retrieved using specialized software.

G. AUTHENTICATING THE ENCASE PROCESS UNDER RULE 901

Q: And what specialized software did you use for this investigation?

A: I used the computer forensics software known as EnCase.

Q: Tell us a little about the EnCase software.

A: EnCase is a standard, commercially available software program that is specifically designed as a tool for computer forensics investigations. It is a fully integrated tool, meaning it performs all essential functions of a computer forensics investigation, including the imaging of a target drive, the generation of an MD5 hash of the evidentiary forensic image, and the analysis of the subject evidence. The software allows for a completely non-invasive investigation in order to view all information on a computer drive, whether it is in the form of a deleted file, a non-deleted file, file fragments, and even temporary or buffer files.

Q: How does the investigator use the EnCase software to recover deleted files?

A: First, EnCase creates a complete forensic image copy or "exact snapshot" of a targeted computer drive. EnCase will be able to read all existing information on that forensic image, regardless of whether the information is in the form of a deleted file that is marked by the operating system to be overwritten. Any information that has not been actually overwritten will be recovered for analysis. EnCase will organize all the files, deleted files and blocks of physical data, also known as unallocated clusters, in a graphical user interface to allow the evidence to be viewed and sorted more easily by the examiner.

Q: Does the same software perform these functions?

A: Yes. EnCase is a software process that is much more automated than other computer forensic investigation processes, as it is a fully integrated program where all the required computer forensics investigation functions are integrated into a single application in a Windows-based graphical user interface.

Q: How is the EnCase process more automated than other tools?

A: To a large extent EnCase duplicates the Windows Explorer interface and file-viewing functions, with the critical added benefits of viewing deleted files and all other information on the disk that the user normally cannot see or detect without specialized software. Just as Windows Explorer presents the entire file directory and folder structure on a computer to the user in a very organized manner, EnCase will also present that information in addition to other data on the target drive in a similar manner. Other forensic software tools require a great deal more manual steps utilizing a series of arcane DOS commands and separate tools to recreate file structures and perform separate searches on different areas of a drive.

H. ADDRESSING *DAUBERT* FACTORS

Q: To your knowledge, is EnCase software generally accepted in the computer forensics investigation community?

A: Beyond being generally accepted, EnCase is widely used in the computer forensics industry, and in my experience it is the tool of choice of the majority of computer forensics investigators in law enforcement. It is the primary computer forensic tool used by U.S. Customs, which is my agency, and I am aware that it is the primary tool of other federal agencies, including United States Secret Service, as well as hundreds of state and local agencies. EnCase is a major part of the Seized Computer Evidence Recovery Specialist training curriculum for federal agents, and

is part of the curriculum in many computer forensics training courses offered by professional organizations — most notably the annual IACIS training conference.

Q: How would one go about testing computer forensic software?

A: There are three main steps in testing computer forensic software. The first step is to generate an MD5 hash value for an image of a targeted computer drive using the forensics tool being tested, and then using another standard tool to repeat the process for the same drive. The MD5 hash values generated by both tools for the same drive should be exactly the same. The second step is to verify that whatever evidence is recovered from an evidentiary forensic image can be independently confirmed by a standard disk utility. With EnCase, for instance, the program will identify the precise location on the original drive for each bit of data recovered by the examiner. With that information, the examiner can then use a disk utility such as Norton DiskEdit to independently confirm the existence and precise location of that data. The third step is to confirm that, throughout the examination process, the content on the forensic image has not been altered in any way by repeating the MD5 hash analysis of the forensic image to verify that the MD5 hash has not changed since the time of acquisition. These tests should be performed several times with different pieces of computer media.

Q: To what extent can EnCase be tested by a third party?

A: EnCase is commercially available, and thus any examiner can purchase, use, and test the program on their own. One of the advantages of the program is that all the required forensic functions are integrated into a single program with a Windows-based graphical user interface. Thus, compared to other computer forensics software, the program is easy to use.

Q: Has your agency tested the software?

A: Yes.

Q: How was it tested?

A: Before we purchased the software on a large scale, there were two computer investigation agents in my agency who conducted an extensive evaluation of the software employing the three steps I just described. I am aware that the Secret Service conducted a similar testing procedure as well. Also, since our agencies' adoption of the software, we have had nearly 100 computer examination agents using the program on a daily basis in the field.

Q: What were the results of those tests?

A: By all accounts, the software has met the three standards I described above.

Q: Has EnCase been tested by any independent third parties?

A: Yes. The U.S. Government conducted extensive testing of computer forensics tools and published its results in October 2008.[102] The testing was conducted as part of the Computer Forensics Tool Testing (CFTT) project, which was a joint effort of the National Institute of Justice, the National Institute of Standards and Technology (NIST), the U.S. Department of Defense, the Technical Support Working Group, and other related agencies. The CFTT testing process for EnCase was remarkably comprehensive, involving over 50 separate test scenarios

102 Available at http://nij.ncjrs.gov/publications/Pub_Search.asp?category=99&searchtype=basic&location=top&PSID=55.

of IDE and SCSI hard drives, including using the FastBloc hardware write-blocking device. All performed NIST testing was disclosed in the Report.

Q: What were the results of the CFTT project testing of EnCase?

A: The results were impressive. First, EnCase flawlessly imaged all sectors and achieved expected results on tests utilizing direct disk-access mode. EnCase also flawlessly imaged all sectors and achieved expected results on tests utilizing BIOS disk access, with one exception. There was one reported anomaly when accessing IDE drives on an older computer using a legacy BIOS. This anomaly reflects a flaw in the legacy BIOS technology. As noted by the CFTT report, Guidance Software has previously addressed this limitation of legacy BIOS technology by easily enabling direct disk access through the ATAPI interface. Second, EnCase properly verified the imaged media in all test scenarios. Third, EnCase properly reported and logged I/0 errors during the imaging process in all test scenarios. Fourth, EnCase properly detected and reported verification errors when the image files were intentionally altered by a disk editor.

Q: You mentioned one anomaly. Were there any others?

A: Two items were noted regarding the restore function, which is not related to the imaging process, and were solely reflective of the limitations of the Windows operating systems. All told, the three identified anomalies in the report reflected limitations of third-party technology, with proper workarounds documented. The results of the CFTT report establish that no changes or modifications to the code of the EnCase imaging engine is warranted.

Q: Has EnCase been subjected to any publication in the industry that you are aware of?

A: Yes, I have read various published articles in the information security and high-tech crime investigation industries that either favorably review the product or mention the product favorably. An article in the April 2001 issue of *SC Magazine* featured the most detailed and documented published testing results to date. The magazine gave EnCase its highest rating and noted that in its testing EnCase "outperformed all the other tools" that were tested by the magazine.

Q: At this time, Your Honor, I'd like to submit as the Government's exhibit ___, which are copies of published articles in the industry discussing the EnCase software.[103]

THE COURT: So received.

Q: Thank you, Your Honor, nothing further.

DIRECT EXAMINATION FOR THE PRESENTATION OF COMPUTER EVIDENCE BEFORE A JURY

A. PREFACE

Many prosecutors maintain that when presenting computer evidence before a jury, the testimony should be as simple and straightforward as possible. Burdening the jury with overly technical information

103 See http://www.encase.com/corporate/news/index.shtm for a comprehensive listing of peer review publications concerning EnCase.

could prove counter-productive and may actually open the door to areas of cross-examination that the court would normally have disallowed. As such, the following direct examination is more detailed than is likely needed, but again, should provide a general resource in preparing direct examinations or for responding on re-direct. Further, there are many other foundational areas that are normally outside the scope of the EnCase process, such as establishing how an Internet chat room works, what the Windows operating system is, or establishing that the computer belonged to the defendant, which are not addressed here. (For a good discussion of establishing a foundation for a printout of a chat room conversation, see *United States v. Tank*.[104])

When presenting EnCase-based evidence, it is recommended that the proponent take full advantage of the EnCase process and graphical user interface by presenting screen shots of the EnCase "All Files" and other views, in order to show the full context of the electronic evidence. This technique may also be required to comply with Best Evidence Rule considerations in computer evidence. Federal Rule of Evidence 1001(3) provides "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" When presenting evidence contained within a computer file, a screen shot of the EnCase File View may be the best means to present a visual output which is "shown to reflect the data accurately," and thus constitute an "original" under Rule 1001(3). (See Chapter 4 for a more detailed discussion of the Best Evidence Rule.)

When seeking to establish a defendant's state of mind by presenting an electronic audit trail or connecting file date stamps, the ability to display a visual output showing various file attributes and other metadata provides a tremendous advantage to the advocate of such evidence. EnCase software provides the best method to visually display all physical and logical data contained on the target drive, while showing the context of such files by displaying file metadata and other means. When providing testimony, many examiners present evidence through screenshots in a PowerPoint presentations format, or take EnCase software with them into court for a live demonstration. In *United States v. Dean*, (discussed further in § 4.2), the opinion reflects that the prosecution presented results of its computer forensic examination through PowerPoint.[105]

Please note that for sake of brevity, many of the foundational portions of the direct exam are incorporated by reference from the above section.

[After stating name for the record]

A. BACKGROUND

Q: Sir, what is your current occupation?
A: I am a Senior Special Agent for the United States Customs Service.
Q: And do you have any specialized duties as a Customs agent?

104 200 F.3d 627, 630-631 (9th Cir. 2000).

105 135 F.Supp 207, fn. 1 (D.Me. 2001). According the prosecutor in Dean, EnCase was used in the examination and provided an effective means for presenting the results of the examination at trial.

A: I am a computer evidence examiner certified as a Seized Computer Evidence Recovery Specialist by the United States Department of the Treasury.
Q: What was your involvement in the investigation of this case?
A: I conducted a computer forensic investigation of the Defendant's computer to recover relevant evidence.
Q: OK, before we discuss the results of your investigation, please tell us how long you have been a computer evidence examiner.

[Please refer to previous section, which is incorporated herein by reference, for foundation testimony.]

* * * *

Q: Turning to the computer forensic investigation you conducted in this case, please tell us when you first came into contact with the Defendant's computer and computer disks.
A: Pursuant to a search warrant, on May 18, 2000 I seized the Defendant's computer at his home, along with seven CD-ROMs and sixteen floppy disks that were in his desk or otherwise in the vicinity of his computer.
Q: What did you do with the Defendant's computer equipment and disks after you seized them?
A: After leaving receipts for the computer and disks, I transported the items back to our lab, where I immediately proceeded to make forensic image copies of the hard drive found in the Defendant's computer. I also made forensic images of each of the CD-ROM and floppy disks. Using EnCase software, I also generated MD5 hash values for the hard drive and for each floppy and CD-ROM disk at the same time the forensic images were made. I then logged the Defendant's computer and the floppy and CD-ROM disks as evidence and secured them into our evidence storage room.
Q: Did you then analyze the forensic images you made?
A: Yes, I did.
Q: Please describe your analysis on the forensic image of the Defendant's hard drive.

B. <u>RECOVERY OF HIDDEN FILES WITH RENAMED FILE EXTENSIONS</u>

A: In my analysis of the forensic image of the hard drive, I first employed an automated function of the EnCase forensic software that analyzes all the computer files on an image of a computer drive and identifies any file signature mismatches.
Q: What are file signature mismatches?
A: A file signature mismatch is a situation where the file name extension that normally identifies the file type has been renamed, usually in order to hide the true contents of a file.
Q: What is a file name extension?
A: A file name extension is an optional addition to the file name that allows a file's format to be described as part of its name so that users can quickly understand the type of file it is without

having to open files on a trial-and-error basis. For instance, a text file will usually have a ".txt" extension and the most common type of picture file has a ".jpg" extension.

Q: How does EnCase identify file signature mismatches?

A: Most computer files containing text or graphical images have a well-defined signature of electronic data unique to that file type. This allows file viewers to recognize the type of file, regardless of the file extension. EnCase utilizes the same process as file viewers in order to identify files that have renamed file extensions.

A: What was the result of the file mismatch analysis that you conducted in this case?

Q: The file signature mismatch analysis revealed 16 files that were renamed as text files with a ".txt" extension, but were actually graphical image files that originally had a ".jpg" extension until they were renamed manually. I viewed those files and upon determining that those images appeared to be child pornography, I printed out those images.

Q: Showing to you what have been pre-marked as United States exhibits 1 through 16, can you identify these exhibits?

A: Yes. These are the printouts I made of the 16 images in question that I recovered from the Defendant's hard drive.

[Exhibits are introduced into evidence.]

C. RECOVERY OF DELETED FILES

Q: Did you examine the images you made of the Defendant's floppy disks?

A: Yes, I did.

Q: What did you find?

A: I found that one of the floppy disks had five files with a ".jpg" extension that had been deleted, meaning that that the computer had marked the data of those files to be overwritten. However, we were able to still recover those deleted graphical image files as the data had not actually been overwritten by the computer.

Q: How did you identify those deleted files?

Q: EnCase software will automatically identify any files that are marked by the computer to be overwritten. I located and viewed those five graphical image files and, upon determining that those images appeared to be child pornography, I printed out those images.

Q: Showing to you what have been pre-marked as United States exhibits 17 through 22, can you identify these exhibits?

A: Yes. These are the printouts I made of the five images that I recovered from the Defendant's reformatted floppy drive.

[Exhibits are introduced into evidence.]

D. RECOVERY OF FILES "DELETED" FROM MULTIPLE CD-ROM SESSIONS

Q: Special Agent _____, did you examine the images you made of the Defendant's CD-ROM disks?

A: Yes, I did.

Q: And what did you find?

A: I found that the CD-ROM disks were actually writeable, meaning that data can be written to this type of compact disc to store computer files. A special CD writing software program, such as CD Creator, is needed to write data to a writeable compact disc. One of the writeable CDs we seized from Defendant's home had multiple sessions on it. A CD session is created when the user writes any number of files to the CD. When this is done, the CD writing software will create a table of contents for that session that points the operating system to the location of the files on the CD within the session.

Q: Can files on a writeable CD be deleted?

A: Not really. Unlike a hard drive or floppy disk, data written to a CD is actually burned to the media by a small optical laser instead of being magnetized. Once data is burned to a CD, it cannot be overwritten. However, if a new session is created on the CD, the user can omit existing files from the new table of contents created for the new session. A computer operating system will only read the table of contents from the latest created session on a CD. Thus, by omitting existing files from the table of contents of a new session, those files will normally be hidden from the view of a user. Specialized software, such as EnCase, will see all the sessions on a writeable compact disc and will allow the user to compare any differences in the file contents of each session.

Q: You mentioned that one of the CDs you examined had multiple sessions. What did your analysis of the multiple-sessions CD reveal?

A: The CD actually had two sessions on it. Using EnCase, we discovered that the second session contained seven files with ".jpg" extensions that were not included in the table of contents of the first session. I then examined those seven files, which turned out to be graphical images appearing to be child pornography, and printed out those images.

Q: Showing to you what have been pre-marked as United States exhibits 23 through 30, can you identify these exhibits?

A: Yes. These are the printouts I made of the seven images that I recovered from the first session of Defendant's writeable compact disc.

[Exhibits are introduced into evidence.]

E. EVIDENCE FROM SWAP FILES

Q: What else did you find in your examination of the Defendant's computer?

A: I conducted a text string search of the forensic image of the Defendant's hard drive. In the course of our investigation, we received information that the Defendant had contacted a minor

over the Internet who had an America Online account under the screen name "Jenny86." I ran a text search by entering the keyword Jenny86, again using EnCase software. The search registered several hits in an area of unallocated clusters identified by EnCase as a swap file.

Q: What is a swap file?

A: A swap file is a random area on a hard disk used by the computer's operating system to temporarily store data as a means to manage the available operating memory of a computer. The operating system will swap information as needed between the memory chips and the hard disk in order to process that information. As a result, temporary data is placed on the computer that cannot be viewed without special software designed for that purpose.

Q: What type of data is typically written to the swap file?

A: Any data that appears on the computer screen, even in the form of an unsaved word-processing document or a Web page being viewed by the user, is often written to the swap file by the operating system.

Q: What did you do after you identified search hits for the keyword Jenny86 in the swap file area?

A: I retrieved the full text of the information contained in the swap file and printed it out.

Q: I'm now handing you what has been previously marked as Exhibit 31, and ask if you can identify it?

A: Yes. This is the print-out I made of the data contained in the swap file where my keyword search registered hits for the keyword Jenny86.

Q: If you would, please read the text as it appears on this printout.

A: The text appears in transcript form and reads, "Welcome to Yahoo Young Teen Chat …." [full text is read].

[Exhibit is introduced into evidence.]

F. EVIDENCE FOUND IN FILE SLACK

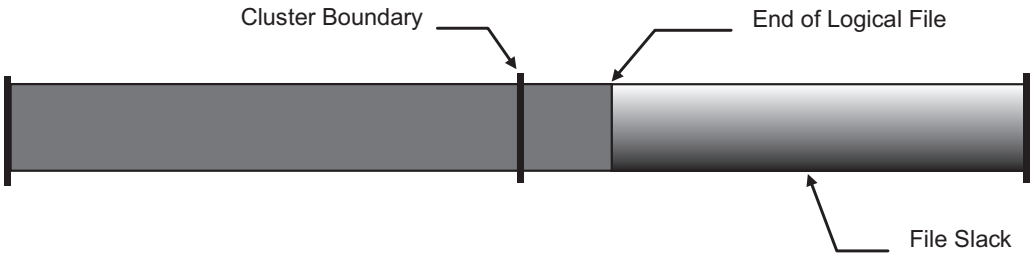
Q: What else did you find in your examination of the Defendant's computer?

A: I conducted a separate text string search of the forensic image of the Defendant's hard drive. In our investigation, we received additional information that the Defendant had corresponded approximately one to two years ago to another individual on more than one occasion. That person has since been convicted of possession of child pornography and sexual assault on a minor. This person's name is John Doe, and he commonly went by the nickname "Lolita's Man." We conducted a text string search with the keyword Lolita's Man and registered a hit in an area of data known as file slack, which contained remnants of a deleted file.

Q: What is file slack?

A: Data storage areas on a hard disk are segmented into clusters. All the data constituting a file may occupy an entire cluster, or the file data may not take up all of the space in the physical cluster. The space between the end of a file and the physical end of a cluster is called the file slack. After the point in the cluster where the file ends, there may be pre-existing bytes in a

cluster that are remnants of previous files or folders. *[NOTE: A projected PowerPoint slide or other form of demonstrative graphic illustrating this issue would be effective at this part of the examination.]*



Example of a Demonstrative Trial Graphic

Q: What did you do after you identified search hits for the keyword "John Doe" in the area of file slack?

A: I retrieved the full text of the remainder of the document contained in the file slack, and printed it out.

Q: Could you determine what kind of document the remnant text in file slack was a part of?

A: Based upon my observation of the format of the two remaining paragraphs in the document and the signature block at the end of the document, it appears that the text recovered from file slack was the remnants of a correspondence of some type.

Q: I'm now handing you what has been previously marked as Exhibit 32, and ask if you can identify it?

A: Yes. This is the print-out I made of the data contained in the file slack area where my text search registered a hit for the text string search "Lolita's Man."

Q: If you would, please read the text as it appears on this print-out.

A: [The text is read into the record]
[NOTE: Because oral testimony of the recovery of file slack may seem too abstract to the jury and the court and because of best evidence rule considerations, it is recommended that a full screen shot of EnCase in "File View" with the highlighted text hit in file slack be projected in order to show the full context of the relevant text.]

Q: Showing what has been pre-marked as Exhibit 33 on the projection screen, does this look familiar to you?

A: Yes, that is a screen shot of the File View of EnCase I created, showing the search hit for "Lolita's Man" in file slack.

Q: Part of the text on the screen is in red, while the text before it is in normal black font. Does the text coloring have any significance?

A: The black text is the active, or non-deleted file that occupies the point from the beginning of the cluster to the end of that file. The red text represents the file slack in the area from the end of the non-deleted file to the end of the cluster.

[Exhibits 32 and 33 are introduced into evidence.]

G. EVIDENCE OF WINDOWS METAFILES RECOVERED FROM UNALLOCATED CLUSTERS

Q: What else did you find in your examination of the Defendant's computer?

A: As part of my routine practice, I recovered all Windows metafiles that were located on the hard drive.

Q: What are Windows metafiles?

A: When a user sends a command to print a file, the Windows operating system makes a copy of that file and sends the copy to the printer. After the file is sent to the printer, Windows deletes that file. Windows does not inform the user that the copy, or metafile, has been made, nor can the user usually detect the existence of the metafiles without special software.

Q: How did you recover the metafiles in this case?

A: The EnCase software has an automated function that locates all the metafiles residing in normally unseen areas on a hard drive, decodes them, and outputs them to a separate folder allowing them to be viewed.

Q: What did you do after you utilized this software function that located the metafiles and outputted them to a folder?

A: I opened the folder and viewed each of the recovered metafiles.

Q: What did you find?

A: I found a text document in an e-mail format addressed to the Defendant's e-mail account. According to the e-mail header information, the message was sent from the account of "Jenny86@hotmail.com."

Q: What does the fact that this e-mail document existed in the form of a metafile mean to you?

A: This recovered metafile means that this e-mail message was printed out from the Defendant's computer.

Q: I'm now handing you what has been previously marked as Exhibit 34, and ask if you can identify it?

A: Yes. This is the printout I made of the metafile of the e-mail document from Jenny86@hotmail.com to the e-mail account of the Defendant.

Q: If you would, please read the text as it appears on this printout.

4. The Best Evidence Rule

§ 4.0 Overview

The Best Evidence Rule is probably the most misunderstood rule of evidence among many computer forensics investigators. The Best Evidence Rule is a doctrine of evidentiary law in the United States, Canada, and certain other countries that essentially requires that the original of a writing must be admitted into evidence in order to prove its contents. As one might imagine, significant questions arise when applying this evidentiary doctrine to computer data. Among the issues raised by this rule are how to present computer evidence at trial, what constitutes a valid image of a computer drive, and data compression. This chapter will outline the law in this area and highlight some common misconceptions.

§ 4.1 "Original" Electronic Evidence

The Best Evidence Rule under the US Federal Rules of Evidence provides that "[t]o prove the content of a writing, recording or photograph, the original writing, recording or photograph is required…"[106] Notably, electronic evidence falls under the Federal Rules definition of "documents."[107] However, with electronic evidence, the concept of an "original" can be difficult to define. For example, when seeking to reproduce an original photographic image, a negative of that photograph, while containing all the "data" of the original, must be processed in order to provide an accurate visual replication of the original photograph. Fortunately, the Federal Rules of Evidence have expressly addressed this concern. Rule 1001(3) provides "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Under this rule and similar rules in state jurisdictions, multiple or even an infinite number of copies of electronic files may each constitute an "original."[108] Note that the law in the United Kingdom (UK) regarding civil matters is even broader:

1. Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved—
   a. by the production of that document, or

106 Fed. R. Evid. 1002.

107 Fed. R. Evid. 1001(1).

108 The treatise. Overly On Electronic Evidence in California, (1999) § 9.02; 9-3, comments on California Evidence Code section 255, an identical statute to Rule 1001(3), noting, "The approach adopted in Evidence Code section 255 allows for the possibility that multiple or, even, an infinite number of originals may exist. Each time an electronic document is printed, a new 'original' is created."

b. whether or not that document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such manner as the court may approve.

2. It is immaterial for this purpose how many removes there are between a copy and the original.[109]

Thus, the UK rule in civil matters allows for admission of copies and indirect copies (copies of copies).[110].

The operative language in Rule 1001(3) is "accurate reflection." It is a mistake to analogize computer files to hard-copy documents for purposes of the Best Evidence Rule. A mere bit-stream copy of a graphical image file does not provide a completely accurate "printout or other output readable by sight" unless Windows-supported forensics tools or other viewers are used to non-invasively create an accurate visual output of the recovered data, without changing any of the data.

Conversely, if a computer file is compressed, encrypted, transmitted as an email attachment (thus sending a copy of that decrypted, compressed file in a different file format and even divided into many packets), and then received, decompressed, decrypted, and opened, the file now in possession of the recipient would be another "original" of that file under the Federal Rules. Printing that file also converts it to another file format. However, as long as the printout is an accurate reflection of the original data, it is irrelevant what the operating system or the network does to that file during the printing process.

The important concept here is the accuracy of the visual output once the image is mounted. If an examiner were to simply extract key data from slack space and export that data to a text file, would a printout of that text file always constitute an accurate reflection of the original data? Many prosecutors do not think so, because the context of computer data is often as important as the data itself. Congress, by enacting Rule 1001(3), placed the emphasis on the accuracy of the visual output of computer data (printout or otherwise) once the image or file is mounted, not on the stored state of that file or image. Obviously, if the original data is actually compromised, the visual output will not be accurate.

It is mandatory that the original data remain unchanged, but whether that data is compressed, encrypted or converted to a different file format in its stored state is immaterial as long as the data itself is not compromised. This is one of the reasons the MD5 hash and verification processes are so important. Even though the file format of the data in question may change, the integrity of that data must remain intact.

The Best Evidence Rule has been raised in the context of an entire drive image as well as an individual file. The Eighth Circuit Court of Appeals described one such situation as follows: ". . . the district court

109 Civil Evidence Act 1995 (c.38) at § 8.

110 See Smith, et al. INTERNET LAW AND REGULATION (Sweet & Maxwell 2007) (4th ed.) at 870 (discussing UK law): Even if an 'original' can be identified and is relevant, what constitutes an original depends on what is sought to be proved. For the purpose of establishing a hacking offence, an electronic document on the system may be regarded as an original document. But for the purpose of proving the contents of a letter sent from the organisation, the same electronic document is only a copy of the original document sent out. . . .In the light of the apparent demise of the best evidence rule as a rule of admissibility, this provision [Civil Evid. Act. 1995 (c.38) at § 8] may now be regarded as merely governing the fashion in which copies are to be proved rather than rendering copies admissible.

permitted [defendant's] probation officer to describe briefly one image of child pornography found on a computer disk in his apartment. Although the court initially overruled [defendant's] objection that the admission of testimony describing the contents of the computer disk violated the best evidence rule, *see* Fed.R.Evid. 1002, it later reversed course and instructed the jury to disregard that portion of the officer's testimony."[111] A Texas Appellate Court ruled that an image copy of a hard drive qualifies as an "original" for the purposes of the Best Evidence Rule.[112] The issue of whether an EnCase Evidence File suffices as an "original" under the Best Evidence Rule was litigated successfully in U.S. Federal District Court, New Hampshire (see § 4.4 for a full discussion).

In situations where computer evidence is collected from a business, a drive image copy is often the only "original" available to the examiner, as the company often requires immediate return of the original drives in order to remain in business, or the company does not allow its mission-critical servers to be shut down, thereby necessitating a live acquisition of the forensic image. See Section 1.5, above, for a discussion of the authentication issues concerning live acquisition.

§ 4.2 Presenting Electronic Evidence at Trial

The United States Department of Justice (DOJ) Guidelines on Searching and Seizing Computers states, "an accurate printout of computer data always satisfies the best evidence rule."[113] This certainly is true in general. However, in *Armstrong v. Executive Office of The President,*[114] the court correctly ruled that a "hard copy" paper printout of an electronic document would not "necessarily include all the information held in the computer memory as part of the electronic document."[115] The Court further noted that without the retention of a complete digital copy of an electronic document such as an email message, "essential transmittal relevant to a fuller understanding of the ***context and import*** of an electronic communication will simply vanish."[116] [emphasis added]

As illustrated by the *Armstrong* case, the presentation of electronic evidence often requires the visual display of the logical data structure of a file, its context, and its associated metadata, in addition to the physical data of that file. When seeking to establish a defendant's state of mind by presenting an electronic audit trail, the ability to display a visual output showing various file attributes and other metadata and demonstrating the logical connection to various data files—instead of relying upon dry and technical expert testimony—provides a tremendous advantage to the advocate of such evidence. EnCase software provides the best method of visually displaying all physical and logical data contained on the target drive, while showing the context of such files by, *inter alia*, displaying file metadata. When providing testimony, many examiners present evidence through screenshots in a PowerPoint

111 United States v. Crume, 422 F.3d 728, 730-31 (8th Cir. 2005).

112 Broderick v. State, 35 S.W.3d 67(2000).

113 Section V.D.1, citing, Doe v. United States, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992).

114 1 F.3d 1274 (D.C. Cir 1993).

115 Armstrong v. Executive Office of The President, supra, 1 F.3d at 1280.

116 Id. (See also, Recovery and Reconstruction of Electronic Mail as Evidence (1997) 41 AMJUR POF 3d 1 §19 ["If the document is a computer printout of an e-mail message, the proponent is required to prove that the printout accurately reflects what is in the computer."])

presentation format, or take EnCase software with them into Court for a live demonstration. In *United States v. Dean*, the opinion reflects that the prosecution presented results of its computer forensic examination through PowerPoint slides.[117] PowerPoint presentations are quickly becoming the standard in modern trial practice, but it is virtually impossible to incorporate command-line utilities into PowerPoint presentations.

In *Dean*, the prosecution sought to establish that the defendant accessed and viewed files on a series of floppy disks. While the defendant denied ever accessing and viewing those files, his computer operating system created temporary link files when he accessed the files on the floppy disk. A forensic investigator from the U.S. Customs Service recovered those temporary link files from the defendant's hard drive.

In order to show the context and metadata associated with the link files, including file-created dates, full path location and other information, the prosecution successfully presented EnCase screen shots as evidentiary exhibits. These screen-capture exhibits provided the most accurate visual display of the data as it existed on the defendant's computer at the time of seizure. The court allowed the screenshots into evidence and convicted Dean on all counts.

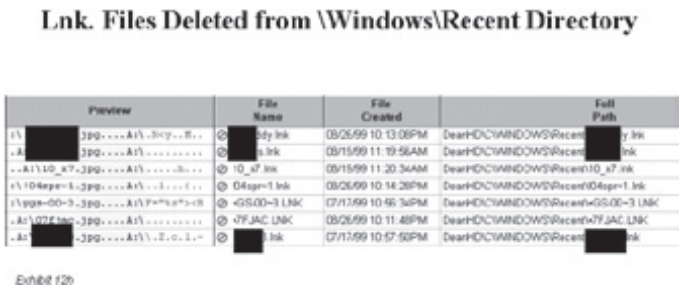


Figure 3: A screenshot exhibit offered by the prosecution and entered into evidence in *United States v. Dean*. The Court ordered the redaction of certain filenames on the grounds that their probative value was outweighed by their prejudicial nature.

Dean is an important illustration of the fact that the context of computer evidence is often just as important as the data itself. If portions of relevant data are recovered in unallocated or slack space areas of a drive, how is that evidence presented? For example, if that data recovered from slack space is simply exported to a text file and then printed out, a proponent will likely face significant difficulty in admitting that evidence without establishing its context.

Relevant questions include: Which file partially overwrote the first section of the cluster where the slack data still resides? When was the file currently occupying that cluster created and last modified? What is the precise address (physical cluster, sector offset, etc.) of the data recovered from slack space? Figure 4 illustrates how such data should be presented both for demonstrative purposes and to comply with the Best Evidence Rule.

117 135 F.Supp.2d 207, fn. 1. (D.Me.) According to the prosecutor in Dean, EnCase was used in the examination and provided an effective means for presenting the results of the examination at trial.

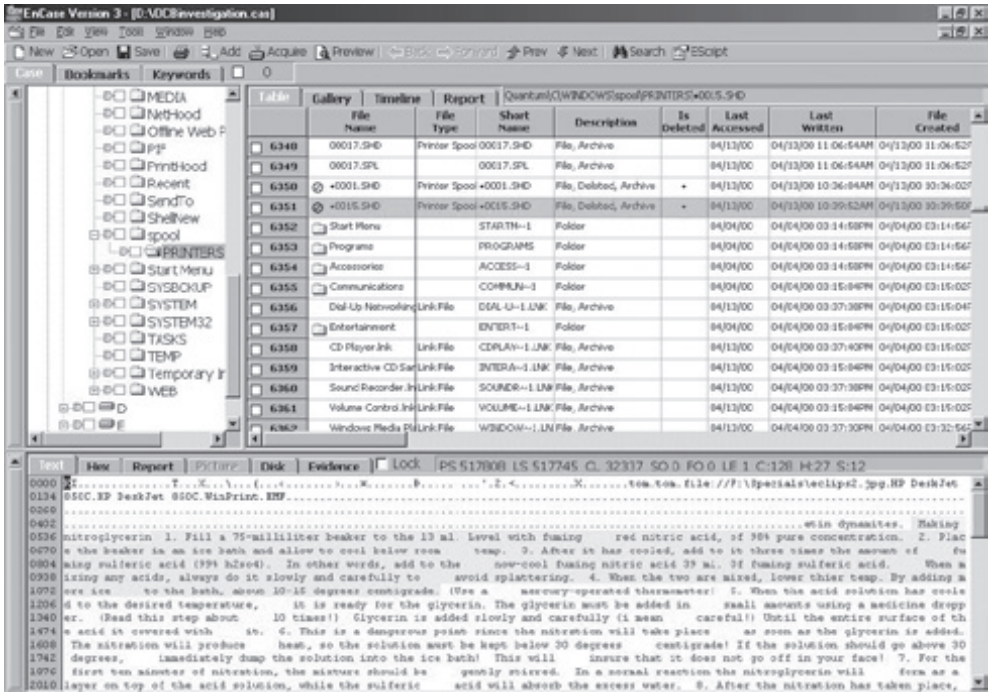


Figure 4: Key evidence of bomb-making instructions found in the slack area of a cluster also occupied (at the beginning) by a deleted printer spool file. Screen shot presentation enables full contextual presentation of the data.

In a 2005 case that did not involve computer forensics, there was an interesting best-evidence discussion involving a digitally enhanced videotape. In *United States v. Seifert*,[118] a defendant charged with arson challenged whether a digitally enhanced videotape recovered from the fire was "best evidence." The defendant asserted that the technician's modification of brightness and contrast and enlargement of the image rendered the tape untrustworthy as an original. The court did not agree, holding the enhanced tape to be a duplicate "which accurately reproduces the original." While the process used by the technician was satisfactory, the court suggested in dicta, "that technology that provides a digital trail could provide an even stronger forensic basis for admission of enhanced electronic evidence."[119]

§ 4.3 Compression and the Best Evidence Rule

The issue of compression in the context of computer evidence is one that has never been addressed by the courts in any known published decisions. However, there is some appreciable authority where U.S. courts have discussed data compression in the context of intellectual property disputes. These rulings do provide a degree of guidance on how the courts would address compressed computer files as evidence.

In *Storer v. Hayes Microcomputer Products*, the court defined computer data compression as follows: "Data compression is the process of reducing the size of the representation of a string of

118 United States v. Seifert, 2005 WL 44749 (D.Minn. Jan 7, 2005).

119 Id. at note 2.

electronic data in order to permit it to be transmitted or stored more efficiently and later to be reconstructed without error."[120] While the *Storer* case addressed whether a company's compression technology infringed upon a patent held by a competitor for similar technology, the court articulated a clear and concise definition of data compression. In *Universal City Studios v. Reimerdes,*[121] a Napster-type copyright infringement case, the court determined that a software application that compresses and then decompresses DVD recordings using "lossy" compression infringes upon the copyright of the publisher. This is so even though "lossy" compression involves inexact replication of the original file through loss of data. Thus, the compressed and then decompressed end product infringes upon the copyright of the original material.

Compression technology allows EnCase software to store a large disk image in a relatively small file. An Evidence File can be compressed upon acquisition or at a later point in the investigation. Compressed Evidence Files can be searched and examined by EnCase software in the same manner as uncompressed Evidence Files. EnCase software uses an industry-standard "lossless" compression algorithm to achieve an average of 50% size reduction.[122]

As noted above, Federal Rule of Evidence 1001(3) provides "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Compression does not have any effect on the actual content of the Evidence Files or the integrity of the evidence. Importantly, a compressed Evidence File will register the same CRC and MD5 hash values as an uncompressed Evidence File of the same drive, as the file content is identical. Further, in the post-acquisition verification process, EnCase software verifies the compressed blocks as well as the MD5 hash for the entire image in the same manner as with uncompressed Evidence Files.

As a compressed Evidence File will contain the exact same contents and the same CRC and MD5 hash values as an uncompressed Evidence File of the same disk image, both will constitute an "original" under Fed.R.Evid. 1001(3). For the same reason, an Evidence File that is acquired uncompressed and is subsequently copied in a compressed format also constitutes an "original" under Rule 1001(3).

§ 4.4 United States v. Naparst – The EnCase Evidence File Validated as Best Evidence

The issue of whether EnCase Evidence Files constituted the best evidence of the computer data contained therein was litigated in a federal criminal prosecution in New Hampshire. The prosecution offered to allow the defense access to a copy of the EnCase Evidence File for discovery purposes. However, the defense contended that it required access to the original computer systems in question so that they could operate those computers and examine them in their native environment, and filed

120 960 F.Supp. 498, 501 (D.Mass. 1997).

121 111 F.Supp.2d 294 (S.D.NY 2000).

122 Lossless data compression, where the compressed-then-decompressed data is an exact replication of the original data, is a very basic and standard aspect of computer science. It is also important to note that whenever a computer file is transmitted over the Internet or sent to the printer, it undergoes compression. Some excellent resources on lossless data compression and data compression in general can be found at http://www.data-compression.com.

a formal written request for a court order allowing such unfettered access to the "original" computer evidence.

The government filed a successful objection to the request, asserting that the "mirror image" created by the special agent is the proper way to preserve the original evidence, as turning on the computer, as the defense requested, will change the state of the evidence by altering critical date stamps and potentially overwriting existing files and information.

The court ruled that the EnCase Evidence File qualified as the Best Evidence and that a discovery copy of the Evidence File would be sufficient discovery disclosure. Alternatively, the court ruled that the defense could have access to the original computer systems only if its expert created another proper forensic image under the supervision of the special agent. The defense was barred from booting the original computer systems to their native operating systems. A copy of the three-page brief filed by the government in support of its successful objection is reprinted here with permission.

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

(United States of America
(
(v. Cr.: 00-11-1-M
(
(Harold Naparst

GOVERNMENT'S OBJECTION TO DEFENDANT'S
MOTION FOR ACCESS TO COMPUTER EVIDENCE

NOW COMES the United States of America, by Paul M. Gagnon, United States Attorney for the District of New Hampshire and states the following:

1. On August 16 & 17, 2000, an expert retained by the defense in this matter was permitted access to the government's expert witness, all of his reports, and an exact mirror image of the defendant's computer hard drives.
2. The defense has now moved this Court to grant them access to the defendant's actual computer equipment which was seized from his home on January14, 2000.
3. The defense argues that this is necessary for preparation of their defense; however, the government submits that if the defense has truly consulted with an expert, then they are aware that the mere act of turning on or "booting up" the defendant's computer will alter that evidence forever.
4. Turning on the computer will change the state of the evidence by altering critical date stamps, and will potentially write over and erase existing files. See affidavit of Shawn McCreight attached as Exhibit 1.

5. The "mirror image" created by Supervisory Special Agent Marx is the proper way to preserve the original evidence and the government will demonstrate that this evidence is the original evidence of the defendant's hard drives. See affidavits of Shawn McCreight and SSA Stephen Marx attached as exhibits 1 and 2.
6. The importance of conducting reviews of computer evidence on mirror image backups is so universally understood that in one civil action, the plaintiffs were sanctioned for failing to create a mirror image of the defendant's hard drive before their review. See Gates Rubber Company v. Bando Chemical Industries, Limited, 167 F.R.D. 90, (D. Colorado, 1996). Instead, they ran a program on the original hard drive which "obliterated, at random, 7 to 8 percent of the information which would otherwise have been available." 167 F.R.D. 90, 112. The Court, therefore ruled that sanctions were appropriate because the plaintiff "had a duty to utilize the method which would yield the most complete and accurate results" and "should have done an 'image backup' of the hard drive which would have collected every piece of information on the hard drive…" Id.
7. Defendant has not demonstrated that he has been deprived of access to any of the evidence of this matter [123] or prejudiced in any way.
8. In fact, prior to the defendant's expert retention, on July 7, 2000, defense counsel was notified by correspondence that any expert retained should be familiar with EnCase software to facilitate their review of the computer evidence. No objection was raised at that time, nor did the defense ever ask for or suggest different imaging software.

WHEREFORE for the above stated reasons, the government respectfully requests that this honorable Court deny the defendant's motion for access to the defendant's computer.

Respectfully submitted
PAUL M. GAGNON
United States Attorney

By:
Helen White Fitzgibbon
Assistant United States Attorney

123 Presumably, the defense has made allegations about the quality or handling of the evidence in their Asecret@ affidavit; the government is obviously in no position to respond to any such allegation(s).

5. Legal Analysis of the EnCase Evidence File

§ 5.0 Overview

The central component of the EnCase methodology is the Evidence File, which contains the forensic bit-stream image backup made from a seized piece of computer media. The Evidence File consists of three basic parts -- the file header, the checksums and the data blocks — which work together to provide a secure and self-checking "exact snapshot" of the computer disk at the time of analysis. The EnCase Evidence File is unique in that it is a secure, self-verifying, and fully integrated forensic image specifically designed as read-only random access data in the context of a computer forensic investigation. Many other imaging tools are backup utilities modified for forensic purposes, and as a result do not contain integrated authentication and verification processes.

This section discusses in detail the major components and functions of the EnCase Evidence File that may be relevant for purposes of authenticating the Evidence File in a court of law.

§ 5.1 Evidence File Format

The EnCase process begins with the creation of a complete physical bit-stream forensic image of a target drive in a completely non-invasive manner. With the exception of floppy and CD-ROM disks, all evidence is acquired by EnCase software in either a DOS environment or in a Windows environment, where a specially designed hardware write-blocking device is utilized. The ability of EnCase software to image in Windows in conjunction with a write-blocking device presents several advantages to the examiner, including dramatically increased speed, more flexibility, and superior drive recognition.

The acquired bit-stream forensic image is mounted as a read-only "virtual drive" from which EnCase software proceeds to reconstruct the file structure by reading the logical data in the bit-stream image. This allows the examiner to search and examine the contents of the drive in a Windows graphical user interface (GUI), all in a completely non-invasive manner. Additionally, the integrated process enables EnCase software to identify the exact original location of all evidence recovered from a targeted drive without the use of invasive disk utilities.

Every byte of the Evidence File is verified using a 32-bit CRC, which is generated concurrent to acquisition. Rather than compute a CRC value for the entire disk image, EnCase software computes a CRC for every block of 64 sectors (32KB) that it writes to the Evidence File. A typical disk image contains many tens of thousands of CRC checks. This means that an investigator can determine the location of any error in the forensic image and disregard that group of sectors, if necessary.

The CRC is a variation of the checksum and works in much the same way. The advantage of the CRC is that it is order sensitive. That is, the strings "1234" and "4321" will produce the same checksum,

but not the same CRC. In fact, the odds that two sectors containing different data will produce the same CRC is roughly one in a billion. The CRC function allows the investigators and legal team to confidently stand by the evidence in court.

In addition to the CRC blocks, EnCase software calculates an MD5 hash for all the data contained in the evidentiary bit-stream forensic image. As with the CRC blocks, the MD5 hash of the bit-stream image is generated and recorded concurrent to the acquisition of a physical drive or logical volume. The MD5 hash is calculated through a publicly available algorithm developed by RSA Security.

The odds of two computer files with different contents having the same MD5 hash value is roughly ten raised to the 38th power. If one were to write out that number, it would be a one followed by thirty-eight zeros. By contrast, the number one trillion written out is one followed by only twelve zeros. The MD5 hash value generated by EnCase software is stored in a footer to the Evidence File and becomes part of the documentation of the evidence.

Throughout the examination process, EnCase software verifies the integrity of the evidence by recalculating the CRC and MD5 hash values and comparing them with the values recorded at the time of acquisition. This verification process is documented within the EnCase-generated report. It is impossible for EnCase software to write to the Evidence File once it is created. As with any file, it is possible to alter an EnCase Evidence File with a disk utility such as Norton Disk Edit.

However, if one bit of data on the acquired evidentiary bit-stream image is altered after acquisition, even by adding a single space of text or changing the case of a single character, EnCase software will report a verification error in the report and identify the location where the error registers.

§ 5.2 CRC and MD5 Hash Value Storage and Case Information Header

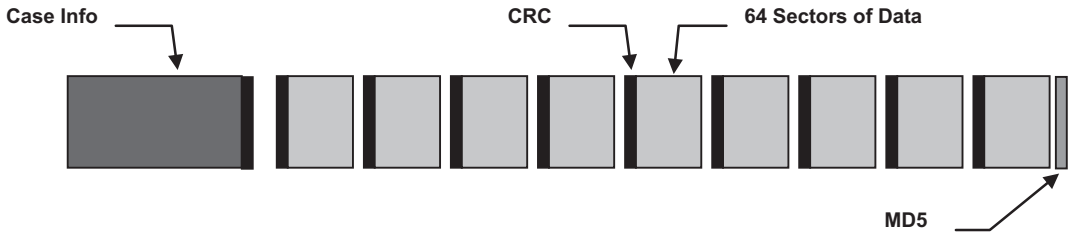


Figure 1: A Graphical Representation of the EnCase Evidence File

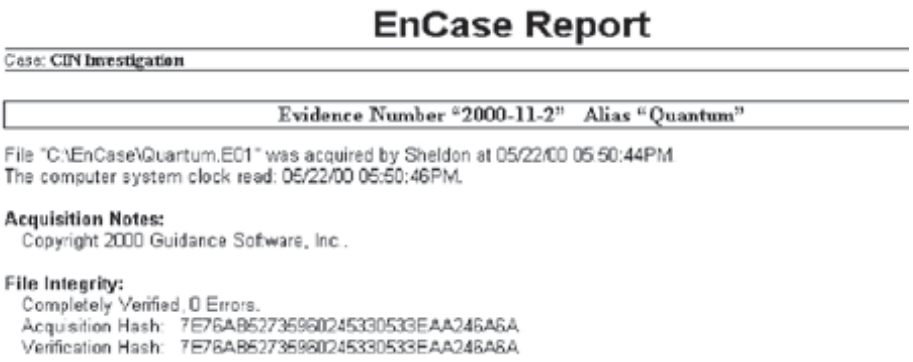
The CRC and MD5 hash values are stored in separate blocks in the EnCase Evidence File that are external to the evidentiary forensic image itself. Those blocks containing the CRC and MD5 hash values are separately authenticated with separate CRC blocks, thereby verifying that the recordings themselves have not been corrupted. If any information is tampered with, EnCase software will report a verification error. Conversely, merely generating an MD5 hash with another tool and recording it manually or in an unsecured file where it may be altered without detection may not fully insulate the examiner from questions of evidence tampering. For this reason, the CRC and MD5 hash-value calculations generated with EnCase software are secured and tamper-proof.

The Case Info header contains important information about the case created at the time of the acquisition. This information includes system time and actual date and time of acquisition, the

examiner name, notes regarding the acquisition, including case or search warrant identification numbers, and any password entered by the examiner prior to the acquisition of the computer evidence. There is no "backdoor" to the password protection. All the information contained in the Case Info File header, with the exception of the examiner password, is documented in the integrated written reporting feature of EnCase software. The Case Info file header is also authenticated with a separate CRC, making it impossible to alter without registering a verification error.

§ 5.3 Chain of Custody Documentation

A distinct advantage of the EnCase process is the documented chain of custody information that is automatically generated at the time of acquisition, and continually self-verified thereafter. The time and date of acquisition, the system clock readings of the examiner's computer, the acquisition MD5 hash value, the examiner's name and other information are stored in the header of the EnCase Evidence File. This important chain of custody information cannot be modified or altered within EnCase software, and EnCase software will automatically report a verification error if the Case Info File is tampered with or altered in any way.


EnCase Report

Case: CIN Investigation

Evidence Number "2000-11-2" Alias "Quantum"

File "C:\EnCase\Quantum.E01" was acquired by Sheldon at 05/22/00 05:50:44PM
The computer system clock read: 05/22/00 05:50:46PM.

Acquisition Notes:
Copyright 2000 Guidance Software, Inc.

File Integrity:
Completely Verified, 0 Errors.
Acquisition Hash: 7E76AB52735960245330533EAA246A6A
Verification Hash: 7E76AB52735960245330533EAA246A6A

Figure 2: Chain of custody information is documented in an automatically generated report

§ 5.4 The Purpose of Sterile Media and The EnCase Process

Computer forensic investigation procedures developed before the EnCase process require that sterile computer media be used to restore an image backup for analysis by separate search utilities that conduct a physical or "end-to-end" analysis of a single drive. Sterile media is required under such a procedure because the non-integrated disk utilities cannot identify the boundaries of the restored forensic image file. Thus, if an image file of an eight-gigabyte drive is restored to a ten-gigabyte, non-sterile drive filled with data, the two gigabytes of "slack" will be improperly read and analyzed by non-integrated DOS tools.

In the past, examiners have experienced problems when utilizing media they believed to be brand new and thus sterile, only to eventually learn that that the storage media was actually only recycled and reformatted. For these reasons, a manually created sterile environment must exist when utilizing search tools that cannot differentiate data residing outside of the original boundaries of the disk image.

The EnCase process does not require the use of sterile media for the same reasons that a word-processing program does not require that its text files be stored on sterile media in order to be accurately read. As described above, the EnCase Evidence File is a logical file with logical file boundaries that EnCase software recognizes in the same way that MS Word for Windows recognizes a MS Word document. There is no concern that when reading one file, data from another file on the disk will inadvertently bleed onto your screen.

As such, the requirement that "sterile media" be used for a computer forensic investigation actually reflects the limitations of the software employed as opposed to being an absolutely necessary item of protocol. EnCase software is specifically designed to only read data contained within the Evidence File. As such, there is no possibility that data residing outside of an EnCase Evidence File will be inadvertently searched or analyzed by EnCase software.

§ 5.5 Analyzing the Evidence File Outside of the EnCase Process

The EnCase Evidence File is designed to contain not only a forensic image, but also a forensic image of a targeted drive that is secured and verified through an integrated process. If an investigator wishes to conduct an analysis of the forensic image contained in the EnCase Evidence File with a tool other than EnCase software, the best practice is to restore the physical drive to a separate and dedicated partition before proceeding with the analysis. Otherwise, an investigator may face problems authenticating evidence extracted from an EnCase Evidence File with third-party software for several reasons.

First, the CRC and MD5 hash values that EnCase software generates and records concurrent to acquisition can only be read and reported by EnCase software. The continual verification by EnCase software of the integrity of the Evidence File throughout the course of the examination is a key component of the EnCase process. While an MD5 hash of the targeted drive can be independently taken with a separate utility for verification purposes, software operating outside of the EnCase environment cannot confirm the Evidence File data integrity based upon the information recorded by EnCase software upon acquisition and stored within the Evidence File. For security reasons, the MD5 hash, CRC values and other case information is secured within the Evidence File and is not designed to be read by third-party software that Guidance Software cannot verify and thus cannot provide testimony regarding its functionality.

Further, allowing the EnCase Evidence File to be reverse-engineered or "cracked" by third-party software is inconsistent with the fundamental principles of computer forensic investigations. The EnCase process has been designed specifically for computer forensic investigations and has been widely shown to produce consistent and accurate results. When third-party software outside of the design and intent of the EnCase process is utilized, any presumption of authenticity, such as that afforded under Fed.R.Evid. 901(b)(9), may be lost.

Secondly, various acquisition data (investigator's name, dates, passwords, etc.), jump tables, file pointers, CRC data, and the MD5 hash block are stored either in the Evidence File header or at intervals between blocks of acquired data to allow integrated verification of data integrity and to enhance error detection and speed. While EnCase software recognizes this "external" data as outside

of the evidentiary forensic image, third-party search tools cannot so differentiate and thus will scan this data when running a search directly on an EnCase Evidence File. In other words, these programs may "find" something that was not placed there by the suspect or user. Further, if any such "non-evidentiary" data happens to fall in between blocks of acquired data that make up a picture or document, the evidence will likely not be recovered at all, leading to incomplete results. At best, the investigator will have to repeat the whole exercise in a forensically proper manner.

Another critical factor involves the important EnCase function of identifying the precise location of each byte of data on the original drive. This is an important feature of the EnCase process, as any evidence recovered by EnCase software can be independently verified by disk utilities such as the Norton tools when utilizing the precise disk location information automatically provided by EnCase software.

However, even if data is successfully extracted from an EnCase Evidence file by a third-party utility, that tool cannot identify the precise location where that data resided on the suspect's media at the time of acquisition. While it is possible to attempt to manually approximate the location under such a methodology, such a practice is forensically unsound for obvious reasons.

Finally, in the same way that a zip file's contents are not readable until "unzipped," raw information on a hard drive or in a forensic image file is not "evidence." It only becomes evidence when it is "mounted" as a file system in the same way that the suspect used it. EnCase software reads file system partition tables and fragmentation blocks by analyzing the file system structure (MBR, FAT tables, etc.). Only by knowing the "cluster chain" of all the files (and the unallocated areas) can a complete recovery process be possible.

By simply conducting a physical "end-to-end" search of the Evidence File, third-party utilities ignore this crucial information and therefore cannot attain the complete recovery of data. At worst, the process could result in "splicing" together pieces of unrelated documents and pictures, and thus "creating" evidence in the process.

For the same reasons, EnCase software is not designed to mount images created by other proprietary imaging tools, such as Safeback or Ghost images. In addition to the verification and rule 901(b)(9) issues, there are significant questions surrounding whether reverse-engineering a proprietary file format constitutes copyright infringement.[124] Further, the concerns regarding infringement raise symmetrical questions about the accuracy of a process that involves reverse-engineering a proprietary image file format without the consent of the developer. Because of such questions, EnCase software is not designed to mount or "crack" other proprietary file images.

124 Whelan Associates, Inc. v. Jaslow Dental Laboratories, Inc., 797 F.2d 1222 (2d Cir. 1986) (Comprehensiveness and complexity of the file structures within the program made the file structures sufficiently informative to warrant copyright protection); CMAX/Cleveland, Inc. v. UCR, Inc., 804 F. Supp. 337 (M.D. Ga. 1992); DVD Copy Control Association v. McLaughlin, No. CV 786804, 2000 WL 48512 (Cal. Super. Jan. 21, 2000).

6. Challenges to EnCase Software and Cases Involving EnCase Software

Computer forensic investigators throughout the world use EnCase software for the seizure, analysis and court presentation of computer evidence. With more than tens of thousands of licensed users, computer evidence processed with EnCase software has been successfully admitted into evidence in thousands of criminal and civil court cases.

To date, there are no known instances of sustained objections to EnCase-based computer evidence on authentication grounds relating to the use of EnCase software. Courts have on occasion entertained--and subsequently overruled--objections to the authenticity or foundation of EnCase-based evidence, and we have documented several such favorable rulings at the trial court level.

In a few instances, US appellate courts have addressed the validity of the EnCase process in published decisions. Appellate court rulings are important as they stand as binding law in their subject jurisdictions, while providing compelling "persuasive authority" everywhere else. In addition, courts in Canada, Australia, and Singapore have published decisions accepting evidence gathered using EnCase software.

§ 6.0 Validation v. Reference

There is an important distinction between a court "validating" the use of EnCase and the court merely "referencing" or "mentioning" the use of EnCase. While a "mention" of EnCase in a court opinion presumes the court approved of its use, in some cases a court explicitly "validates" EnCase for use in obtaining digital evidence. The cases in which the court validates the use of EnCase are strong precedents which make future evidentiary challenges to EnCase in that same jurisdiction extremely difficult.

Merriam-Webster's dictionary defines "Validate" and "Mention" as follows:

> Validate (v.): 1. To make legally valid; ratify; 2. To support or corroborate on a sound or authoritative basis; 3. To recognize, establish, or illustrate the worthiness or legitimacy of.
>
> Mention (n): 1. The act or an instance of citing or calling attention to someone or something especially in a casual or incidental manner.

A validation of EnCase software from a court means the court is satisfied that the software is sound, and not just for use in the case before it, but for use by other courts in the jurisdiction in future cases, as well.

In the discussion of cases that follows, there are several cases that stand out as examples of the

court validating EnCase software, thus making future challenges to EnCase in those jurisdictions nearly impossible. Some of these cases, and the jurisdiction in which EnCase was validated, include:

- *Xpel Technologies Corp v. American Filter Film Distributors* (W.D. Texas)
- *People v. Shinohara* (Illinois)
- *State v. Cook* (Ohio)
- *People v. Rodriguez* (California)
- *United States v. Habershaw* (D. Mass.)
- *State of Nebraska v. Nhouthakith*
- *State of Washington v. Leavell*
- *Grant v. Marchall* (Australia).

The discussions of EnCase in two distinct cases from Texas, *Williford v. State of Texas*, and *Sanders v. State*, illustrate the preclusive effect a validation of software such as EnCase can have on future evidentiary objections in future cases. *Williford*, decided by the Texas Court of Appeals in 2004, held that the computer forensics investigator's testimony regarding his use of EnCase, and the use of EnCase, itself, satisfied the *Kelly* criteria for reliability.

In 2006, a Texas Appellate Court decided the *Sanders* case. Based on the *Williford* court's acceptance of EnCase and its own cursory showing of the *Kelly* standard, the *Sanders* court accepted the reliability of EnCase as well.

The *Williford* court described the factors the trial court should analyze when viewing evidence based on scientific theory:

1. The extent to which the underlying scientific theory and technique are accepted as valid by the relevant scientific community, if such community can be ascertained
2. The qualifications of any expert testifying
3. The existence of literature supporting or rejecting the underlying scientific theory and technique
4. The potential rate of error of the technique
5. The availability of other experts to test and evaluate the technique
6. The clarity with which the underlying scientific theory and technique can be explained to the court
7. The experience and skill of any person who applied the technique on the occasion in question.[125]

Then, in analyzing whether these factors weighed in favor of finding the investigator's use of EnCase to be reliable, the *Williford* court stated: "[The investigator] testified that EnCase is generally accepted in the computer forensic investigation community, that EnCase is used worldwide, that he knew how to use EnCase, that he knew how EnCase worked, that he had successfully used EnCase in the past, that EnCase can be tested by anyone because it was commercially available and anyone could purchase

125 127 S.W.3d 309, 313-314 (Tex.App. 2004).

it, that EnCase has been tested, that there have been several articles written about EnCase and other computer forensic software programs, that *SC Magazine* gave EnCase an overall five-star rating out of five stars, that EnCase has a low potential rate of error, that he successfully copied appellant's hard drive by using EnCase, and that EnCase verified that he had successfully copied appellant's hard drive…[The investigator's] testimony established EnCase's reliability."[126] Thus the *Williford* court validated EnCase for use in computer forensic investigations throughout the State of Texas.

In *Sanders*, the court accepted the use of EnCase by taking judicial notice of the validation of EnCase in *Williford*. In a footnote, the *Sanders* court cites the portion of the *Williford* decision containing the *Kelly* analysis and the *Hernandez v State*[127], ,case for the following: "once some courts have, through a *Daubert/Kelly* 'gate keeping' hearing, determined the scientific reliability and validity of a specific methodology to implement or test the particular scientific theory, other courts may take judicial notice of the reliability (or unreliability) of that particular methodology."[128]

Whether a court decides to take judicial notice of the reliability of EnCase, as in *Sanders*, or whether the court decides to follow precedent in analyzing the *Kelly/Daubert* factors of EnCase's reliability, a court will find EnCase reliable when EnCase was previously validated in that jurisdiction.

The following are summaries of notable appellate and trial court decisions that address EnCase software.

U.S. v. Siciliano

The *Siciliano*[129] case involves a suspected producer of ecstasy and child pornographer. Here, while reviewing the suspect's computer for pornography, DEA Computer Forensic Examiner Jill Mossman ("Mossman") conducted a file-by-file "hash" of the hard drive. Mossman explained to the Court how the process of "hashing" involves applying a mathematical algorithm to each file to create a "hash value" for each file. The hash value is similar to a digital fingerprint in that each file has a unique hash value and whenever a file is altered its hash value is also altered. Hashing files is part of DEA protocol and is done in every case, and if the hash values of two files match, the files are then said to be identical. Mossman said that the DEA uses a computer software program, EnCase, which allows the user to image a hard drive and examine its contents. Mossman used EnCase to obtain the hash values for all of the files on the first computer ("N16"). She further stated, "EnCase has a hash value library that contains the hash values for various known files, such as certain viruses and system files. The library also contains a compilation of hash values for known child pornography files known as the "Innocent Images" hash set." These files are compiled by law-enforcement personnel trained as experts in child pornography. While some of the files have been adjudicated and determined to be child pornography, others are included because the law-enforcement personnel believe them to be child pornography.

126 Id.

127 116 S.W.3d 26, 28-29 (2003)

128 Sanders v. The State of Texas, 191 S.W.3d 272, (Tex.App. 2006); Cert. Denied, 127 S.Ct. 1141, 166 L.Ed.2d 893 (U.S.).

129 U.S. v. Siciliano, 2008 WL 724032 (D. Mass.)

Mossman compared the hash values of the files on N16 with the hash values from the EnCase library of known child pornography files and found five files with matching hash values. The court stated:

> To the extent defendant complains of the deliberate opening and printing of one file each from N16 and N17 in support of the March 29, 2007, warrant application, I find that the images would inevitably have been discovered. Mossman testified that she would have reviewed every single file on both N16 and N17 during the course of her examination pursuant to the March 9, 2007, warrant's broad definition of "data," which includes "all information stored on storage media of any form (such as documents, tables, metadata, audio and visual files, their drafts and their modifications, whether deliberately, inadvertently, or automatically stored)." (Ex. 19, Attach.B.) Additionally, although she deliberately compared the hash values of the files on N16 and N17 with the "Innocent Images" set, it is DEA protocol to run this comparison when examining a hard drive, and Mossman testified that she does so in every case pursuant to that protocol. The court credits her testimony in full. Accordingly, the prosecution has "establish[ed] by a preponderance of the evidence that the [files] ultimately or inevitably would have been discovered by lawful means" had the initial seizure of the computers been lawful. *Nix v. Williams*, 467 U.S. 431, 442-43 (1984); *see also United States v. Silvestri*, 787 F.2d 736, 744 (1st Cir.1986).

This case shows the software's precise scope collection capabilities. Increasingly courts desire more narrow searches by the prosecution. This narrow search for specific words or terms is less expensive and takes less time to complete than a "full search" of the computer. Unfortunately, the case has a bad result as the Massachusetts federal judge granted the motion to suppress. The court found that the agents proceeding in getting the warrant were unlawful and as a result the evidence obtained using EnCase was fruit of the poisonous tree.

Xpel Technologies Corp. v. American Filter Film Distributors

In *Xpel Technologies*[130], the court granted a motion for expedited computer forensic imaging of the electronic storage devices in defendant's possession specifically suggesting EnCase. *This is much more than a passive reference and tends to show a validation by the courts of the software*. The court held that "Imaging of the Computer(s), Server(s), any other electronic storage devices in Defendants' possession, custody, or control, and Brett Wassell's laptop shall be created using Encase [sp] or a similar hardware or software tool that creates a forensically sound, bit-for-bit, mirror image of the original hard drives." A bit-stream mirror image copy of the media item(s) will be captured and will include all file slack and unallocated space. [emphasis added]

130 2008 WL 744837 (W.D. Tex)

United States v. Salcido

In *Salcido*[131] , the government introduced into evidence five videos and six still images that had been found on the defendant's CD-ROM and computer. The detective testified that EnCase is well known and generally accepted means of conducting a forensic examination of a computer for the purpose of retrieving evidence. *Significantly, there was no objection by the defense to the EnCase program, and the court concluded that the evidence taken from defendant's computer was authentic.*

Williford v. State of Texas[132]

The Court of Appeals of Texas, in a case called *Williford v. State*, explicitly validated the reliability of EnCase software and a police investigator's status as an expert witness. The *Williford* case involved a defendant who had taken his home computer to a repair shop, which found child pornography on the computer and notified the police. The defendant then consented to a search of the hard drive. The police computer forensics investigator used EnCase software to image the drive and analyze its contents. When the investigator testified at trial, the defendant objected on the grounds that the investigator "was not qualified as an expert to testify about the theory or technique in developing the EnCase software or its reliability."[133] The defendant further contended that the investigator "was not qualified to testify as an expert witness regarding the scientific technique that he used to reproduce pictures . . . from appellant's computer."[134] In rejecting the defendant's claims, the Court held that:

> We find that Detective Owings's testimony satisfied the *Kelly* criteria for reliability. Detective Owings provided testimony on each of the seven factors identified in *Kelly*. Detective Owings is the computer expert for the Brownwood Police Department and is knowledgeable about EnCase. He testified that EnCase is generally accepted in the computer forensic investigation community, that EnCase is used worldwide, that he knew how to use EnCase, that he knew how EnCase worked, that he had successfully used EnCase in the past, that EnCase can be tested by anyone because it was commercially available and anyone could purchase it, that EnCase has been tested, that there have been several articles written about EnCase and other computer forensic software programs, that *SC Magazine* gave EnCase an overall five-star rating out of five stars, that EnCase has a low potential rate of error, that he successfully copied appellant's hard drive by using EnCase, and that EnCase verified that he had successfully copied appellant's hard drive. Detective Owings described in detail for the trial court how EnCase worked. Detective Owings's testimony established EnCase's reliability.[135]

131 U.S. v. Salcido 506 F.3d 729 (9th Cir. 2007)
132 127 S.W.3d 309 (Tex.App. 2004).
133 Id. at 311.
134 Id. at 312.
135 Id. at 313-14.

The *Williford* case is important because it re-emphasizes (and from an appellate court, no less) two key points:

1. A computer forensics investigator need not have developed EnCase software himself to serve as an expert witness at trial regarding the forensic examination conducted
2. EnCase software is a reliable, widely available, thoroughly tested, and court-approved computer forensics tool.

Sanders v. State (Texas)[136]

In *Sanders v. State*, the Texas Court of Appeals reaffirmed the reliability and accuracy of EnCase Forensic software. Roger Lee Sanders was convicted of ten counts of aggravated sexual assault of a child under the age of fourteen. Sanders appealed his conviction by attempting to discredit crucial pieces of evidence recovered from his computer using EnCase software. Specifically, the defendant challenged the evidence on the *pro forma* assertion that the prosecution failed to show that the software used during its investigation was reliable and accurate.

At trial, the prosecution's forensic expert explained that EnCase took an image of Sander's hard drive and used a MD5 Hash to validate the image. The expert stated that using a MD5 hash ensures that there is no possibility an error could occur during the investigation process. The *Sanders* court utilized the three-prong test set forth in *Kelly v. State* in determining the admissibility of evidence retrieved with EnCase. The *Kelly* test is analogous to the *Daubert* and *Frye* tests, and determines the reliability and ultimate admissibility of evidence obtained through a scientific or technical analysis. In *Williford v. State,* a case with a similar fact pattern, the Court approved the use of EnCase software after detailing the software's compliance with each factor of the *Kelly* test. Citing *Williford,* the appellate court affirmed the trial court's admittance of the evidence retrieved with EnCase. EnCase software was held to be a reliable means of obtaining digital evidence from a defendant's computer system.

Significantly, the *Sanders* court also took judicial notice of the reliability of EnCase software. "[O]nce some courts have, through a *Daubert/Kelly* 'gate keeping' hearing, determined the scientific reliability and validity of a specific methodology to implement or test the particular scientific theory, other courts may take judicial notice of the reliability (or unreliability) of that particular methodology."[137] Judicial notice is the act by a court to "recognize the existence and truth of certain facts, having bearing on the controversy at bar, which, from their nature, are not properly the subject of testimony, or which are universally regarded as established by common notoriety."[138]

This decision is important, as the validation process of EnCase is greatly reinforced and streamlined with such courts taking judicial notice of the acceptance and reliability of the EnCase technology. With this ruling, the reliability of EnCase is presumed to be established in a Texas court of law.

---

136 Sanders v. The State of Texas, 191 S.W.3d 272, (Tex.App. 2006); Cert. Denied, 127 S.Ct. 1141, 166 L.Ed.2d 893 (U.S.)
137 Id.
138 Black's Law Dictionary, 6th Edition

This case is controlling authority in Texas. Notably, the defendant appealed the appellate court's judicial notice finding regarding the reliability of EnCase to the U.S. Supreme Court. In January 2007, the Supreme Court denied certiorari petition, thus allowing the Texas appellate court's decision to stand.[139] The Supreme Court's denial of the defendant's certiorari petition gives even stronger weight to this important decision regarding the established acceptance and reliability of the EnCase Software.

Williams v. Massachusetts Mutual Life Insurance Company[140]

Williams v. Massachusetts Mutual Life Insurance Company is a case in which the plaintiff alleged the existence of an email that "'spelled out' a policy or practice by MassMutual of using disciplinary actions as a pretext for terminating minority employees." When MassMutual did not produce the email, plaintiff filed a motion seeking "to have the court appoint a 'neutral' forensic computer expert to inspect Defendants' computer hard drives and/or electronics communication system in an attempt to recover the . . . e-mail message which he claims exists." In refusing what the Court described as "an intrusion into an opposing party's information system," the Court noted that MassMutual had already performed its own computer forensics search and collection effort in response to the litigation. The affidavit that MassMutual had submitted in support of its response to plaintiff's motion stated in part as follows:

> Robert Bell is a member of the team of information security professionals [at MassMutual]. . . Mr. Bell has performed over seventy-five (75) investigations using Encase, **the standard computer forensics software used by law enforcement and corporate security departments.** [emphasis added]
>
> At the request of counsel for MassMutual, Mr. Bell . . . used Encase to search the hard drives of all personal computers assigned by MassMutual to the [relevant MassMutual employees] from 2002 to the present, the e-mail boxes of [those employees] and relevant files on a local area network on which human resources personnel can store documents electronically.

People v. Shinohara[141]

People v. Shinohara is an important case issued by an Illinois appellate court that validates EnCase software and its MD5 hash function. This case involved an unsuccessful challenge from the criminal defendant who contended that "the State failed to establish that the EnCase software program, which allegedly made an exact, bit-by-bit copy of the defendant's hard drive, was in proper working

139 127 S.Ct. 1141, 166 L.Ed.2d 893 (U.S. 2007).
140 Williams v Massachusetts Mutual Life Insurance Company. 474 F.Supp.2d 219 (D.Mass. 2007)
141 872 N.E.2d 498, 313 (Ill.App. 2007).

condition before he (the examiner) used it to conduct his forensic examination." Both the trial court and ultimately the appellate court rejected this argument and upheld the conviction.

There are several important aspects of this decision:

- The testimony of the trained computer forensics expert was sufficient to validate that the EnCase software was operating properly. This is consistent with several other decisions and reinforces the fact that testimony of a trained and qualified computer forensics expert is more than sufficient to validate the EnCase software.

- The defense unsuccessfully argued that because Illinois State Police computer forensics expert was not EnCE®-certified, he was not a qualified expert. The court noted that the expert was trained and supervised by an EnCE-certified superior. So, while obtaining EnCE certification is strongly advised and certainly provides strong weight toward being qualified as an expert, it is not mandatory. However, this case does illustrate that training is very important. (EnCE is the professional certification program that confers an "EnCase Certified Examiner" designation.)

- The legal standard utilized by the Court was whether the software was in proper working order. The Court relied on EnCase's "industry standard" MD5 hash value-verification function to establish that it worked properly during the course of the computer examination. According to the forensic analyst relied on by the Court: "the EnCase software has a computer industry standard built into it, known as MD-5 hash, which utilizes an algorithm to verify that the image it is taking of a hard drive is accurate. Application of this standard during the copying process reflected that the EnCase software was operating properly. Accordingly, we conclude that the State presented sufficient evidence to establish that the EnCase software was functioning properly when Bullock utilized it and ensured that the images presented at trial accurately portrayed the images on defendant's computer."

This published case is controlling authority in Illinois and persuasive authority for the rest of the United States.

State (Ohio) v. Heilman[142]

In *State v. Heilman,* the Ohio Court of Appeals affirmed the defendant's conviction on numerous sexual offenses with a minor and possession of child pornography based on evidence retrieved with EnCase software and other forensic tools. The prosecution's expert used EnCase software to examine the defendant's extensive home network, which consisted of several computer systems, thirty-eight hard drives, fifty-seven CDs, and 245 floppy diskettes. Using EnCase, the forensic expert was able to retrieve illegal pornographic images, which were both deleted and still active, incriminating web

142 State of Ohio v. Mark A. Heilman, 2006 WL 847120 (Ohio App. 2006)

searches, the duration of the defendant's use of the computer and his actions during those periods, and the user accounts and associated usage on each terminal.

The defendant explained the finding of child pornography on his computer by alleging that a virus had placed those files on his computer systems. Additionally, the defendant asserted that the fact that the computers were readily available to all the occupants of his house meant co-tenants could have been responsible for the child pornography. The prosecution's expert stated that the viruses were only present on a small segment of the networked computers and child pornography had been discovered on systems that were not infected. The expert testified that it was not plausible that these files were planted by malicious software. Furthermore, EnCase software was used to recover evidence that showed that the appellant's password-protected account was being used when the illicit actions took place. The Ohio court affirmed the defendant's conviction, which was based on evidence discovered with EnCase software.

Krumwiede v. Brighton Associates[143]

In *Krumwiede v. Brighton Associates*, the court rendered a default judgment against a party who had destroyed evidence and purposefully obstructed discovery. EnCase software was used by the defense to obtain evidence from the plaintiff's computer, and to establish the plaintiff's concealment of evidence.

Krumwiede had filed suit against Brighton, his previous employer, for back pay, intentional infliction of emotional distress, and violations of his employment agreement. Brighton then filed counterclaims for violations of confidentiality and non-compete agreements. Brighton sought to recover data from a laptop owned by Brighton, but in Krumwiede's possession.

After the Court-ordered production of the laptop, Brighton had its expert use EnCase software to examine the computer. Brighton's expert determined that immediately prior to surrendering his computer pursuant to the court order, Krumwiede had accessed over 13,000 files, had deleted numerous files, and had performed defragmentation routines. Furthermore, Krumwiede had employed USB storage devices and archiving utilities to backup files, and certain of those files were directly linked to Brighton based on keyword searches using EnCase software. Brighton's expert concluded that there were signs of purposeful destruction and concealment of evidence despite a preservation order from the court.

The court acknowledged that, "[a] default judgment…should only be employed in extreme situations where there is clear and convincing evidence of willfulness, bad faith or fault by the noncomplying party."[144] Based largely on Brighton's expert's report, the court found overwhelming evidence that Krumwiede acted in bad faith and awarded a default judgment in favor of Brighton on its counterclaims. Krumwiede was ordered to pay reasonable attorney fees and costs of the investigation. The court's judgment against Krumwiede based on evidence recovered with EnCase software highlights the role of EnCase software as an integral tool in investigating spoliation claims.

143 Charles A. Krumwiede v. Brighton Associates, L.L.C., 2006 WL 1308629, (N.D.Ill. 2006)
144 Id.

State (Ohio) v. Cook[145]

State v. Cook, an Ohio State Appeals Court decision, represents the first appellate decision that both validates and specifically addresses EnCase software. In *Cook*, the defendant appealed his conviction on twenty separate counts of possessing child pornography and designation as a sexual predator, challenging what he claimed to be "the lack of reliability of processes used to create two mirror images of the hard drive."[146] The Ohio appellate court addressed this argument by first describing how the law-enforcement investigator utilized EnCase software to make a forensic "mirror image" of the target drive. The court then noted that "[u]sing EnCase with the mirror image hard drive, [the investigator] generated a report hundreds of pages long, containing a complete history of everything on the computer's hard drive. Among the contents were over 14,000 pornographic pictures, covering a wide range of dates."[147] The court also specifically noted that the investigator was trained in the use of EnCase software. In upholding the validity of EnCase software, the Court stated:

> "In the present case, there is no doubt that the mirror image was an authentic copy of what was present on the computer's hard drive."[148]

The court cited Ohio Rule of Evidence 901(A) and 901(B), which are nearly identical to the corresponding federal rules, (and are discussed in length in Sections 1.1 and 2.1, respectively, of this text). The court found that Rule 901(A), which provides that authentication "as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims," governed the issue of authentication of the computer evidence. The court further noted that Rule 901(B)(9), which provides that "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result" is one way to establish authentication under 901(A). The court decision leaves no doubt that the copy was authentic and as evidence it cites the fact that the defense's expert did not even challenge the authenticity of the mirror image, and thus, the authentication requirements under Rule 901(A), were satisfied by the EnCase image.

State (Ohio) v. Morris

In this appellate case from Ohio, the original hard drive, which "belonged to a non-party . . . who used the computer in his business," was overwritten by the forensic investigator.[149] At trial, only the forensic image of the drive created by EnCase software was available. The court noted:

145 777 N.E.2d 882 (Ohio App. 2002)
146 Id. at 886.
147 Id.
148 777 N.E.2d at 887.
149 State v. Morris, 2005 WL 356801 (Ohio App. 9 Dist. Feb. 16, 2005).

> [T]he evidence in question was actually presented at trial in the form of a copy of the hard drive . . . In this case, [the forensic investigator] testified that the software utilized, Encase Version 3, takes the contents of the hard drive through a complex math equation and creates a 128 bit number known as a fingerprint… [The forensic investigator] went on to note that in the instant matter, the copy created by Encase was an exact copy of the original hard drive. Appellant has seemingly argued on appeal that, absent a software engineer verifying that Encase software does what it purports to do, this hard drive should not have been admitted. **This Court disagrees**.[150]

The court's decision: (i) validates the MD-5 hash process, and (ii) considers forensic disk images to be exact copies and admissible when the "original" is no longer available. This is important not merely in cases in which the forensic investigator has overwritten a hard drive, but for matters involving the collection of computer evidence using network-enabled computer forensic software, such as EnCase Enterprise software.

Taylor v. State

Taylor v. State[151], is another appellate decision that addresses EnCase software, although not to the same degree as *Cook* or *Williford*. *Taylor* involved several different issues on appeal, most of which did not involve EnCase software. The issue that did address EnCase software centered on whether the acquisition and verification MD5 hash readings documented in the EnCase Report for authentication purposes constituted hearsay. The court determined that because the acquisition and verification hash readings are generated by a computer analysis independent of any data input by a human, the information is not hearsay.[152] As a result, the court rejected the defendant's contention that the drive image was not authentic.

This ruling is significant as it provides that EnCase Evidence Files can potentially be authenticated at trial, even if the examiner who created the image is unavailable to testify. EnCase software generates an MD5 hash value of an acquired drive concurrent with acquisition in a secure, integrated, and automated manner, meaning that this critical authentication data is computer-generated and automatically documented. Other processes to generate and record an MD5 hash are not integrated or secure, thus requiring the manual recording and documentation of the readings, which, under *Taylor*, would be inadmissible hearsay if the examiner who acquired the drive was unavailable at trial, and, even if available, could subject the examiner to additional scrutiny.

150 Id. at 2 (emphasis added).

151 93 S.W.3d 487 (Tex. App. 2002)

152 Taylor v. State, supra, 93 S.W.3d 487, 507-08.

United States v. Strum[153]

In this case, the defendant Strum was indicted of one count of a felon being in possession of a firearm and one count of possession of child pornography. The opinion written by the United States District Court in Colorado reflects that the federal agents employed EnCase in the course of the computer forensics examination. Defendant Strum made a discovery motion to obtain copies of the EnCase Evidence Files made by the federal agents after they seized the defendant's computer. The Government opposed the motion on the grounds that such copying is prohibited under the Adam Walsh Child Protection and Safety Act of 2006 ("Walsh Act").

The court outlined and ultimately accepted the Government's alternative to providing copies of the Evidence Files:

> Agent Stoffregen affirmed that, since enactment of the Walsh Act, ICE no longer produces to defense counsel or defense experts bit-by-bit images of computer media containing child pornography. Instead, ICE Agents make the bit-by-bit images available for inspection in a private room designated for the purpose, provided that the inspector signs a stipulation promising not to copy any contraband depictions. Defense experts may use either a stand-alone computer provided by ICE or their own computers, which they can connect to the hard drive. Standard forensic software, such as EnCase, or a program called 'VM Ware,' facilitates the forensic analyses most commonly undertaken to verify that the bit-by-bit image is what it purports to be. In the unlikely event that defense experts do not have these software programs, ICE is able to provide them.

The district court denied the defendant's motion for production of copies of the EnCase Evidence Files.

United States v. Bhownath[154]

U.S. v. Bhownath is a federal software piracy prosecution brought in a United States District Court in Utah. According to the published opinion, the FBI used EnCase to conduct the computer forensics examination: "Agent Hubbert took the imaged copies and reviewed them on a viewing station using EnCase, a computer forensic tool widely used by computer forensic examiners. Agent Hubbert then ran a keyword search, looking for files and folders related to Infinite Mind and Snap Discount."

The EnCase-specific issues in *Bhownath* centered on Fourth Amendment concerns under the United States Constitution regarding whether the issued search warrant was rendered overbroad by virtue of utilizing the keyword searching capabilities in EnCase, which enabled the investigator to search every file on the seized computer in an automated fashion, as opposed to only manually

153 2007 WL 1453108, D.Colo., May 17, 2007

154 2007 WL 2570199 (D.Utah, 2007)

opening specific documents with file names suggestive of software piracy. The Court denied the defendants' motion to suppress evidence, finding that the evidence identified and recovered by EnCase was properly done without infringing upon the Fourth-Amendment rights of the defendant.

This case is discussed in detail in section 7.1, *infra*.

United States v. Shirazi

In *U.S. v. Shirazi*[155], federal law enforcement agents, in their affidavit filed with the court, specifically pointed to their use of EnCase to justify the issuance of a warrant to search and seize computers. The court noted that the "search was conducted with the aid of a file recovery program called EnCase, which enables a user to retrieve files that have been deleted but remain on a computer's media storage device such as a hard drive. While examining the desk top computer, FBI agents discovered files containing hundreds of stolen credit card numbers." During the search the officers inadvertently discovered child pornography. Following a warrant, the agents conducted a search with EnCase revealing several dozen instances of child pornography that the defendant had attempted to delete.[156]

Matthew Dickey v. Steris Corporation

One of the first known instances of a "serious" challenge to the use of EnCase software occurred in a civil litigation matter before the United States Federal District Court, Kansas, where at an April 14, 2000 pre-trial hearing, the court ruled that the testimony of an Ernst & Young expert regarding his computer forensic investigation based upon EnCase software would be allowed, overruling objections from the plaintiff. In *Matthew Dickey v. Steris Corporation*, the trial court overruled evidentiary objections to the introduction of EnCase-based evidence at an April 14, 2000 pre-trial hearing. Plaintiff Dickey brought a motion *in limine* seeking to exclude the testimony of an Ernst & Young expert, regarding the results of his computer forensic investigation based upon the use of EnCase software. The plaintiff's motion was based upon the report of his own expert, which consisted of a critique of the Ernst & Young report.

Steris Corporation ("Steris") successfully opposed Dickey's motion, clearing the way for the expert testimony based upon EnCase software. Steris brought its own motion to exclude the testimony of the plaintiff's expert. Among Steris's arguments was the contention that the plaintiff's expert was unqualified to provide an expert opinion about computer forensics as, among other reasons, she was admittedly unfamiliar with the EnCase software. The court denied both motions, finding that 1) the challenge to the EnCase process employed by the Ernst & Young expert was without merit, and 2) the testimony of the plaintiff's expert would not be excluded, although she could be questioned at trial regarding her unfamiliarity with EnCase software, which would be relevant to her credibility as a computer forensics expert.

155 2006 WL 1155945 (N.D.Ill.)

156 Id. at 8

State of Washington v. Leavell

On October 20, 2000 in a Washington State Superior Court, a contested hearing took place in the matter of *State of Washington v. Leavell*[157] where the defense brought an unsuccessful suppression motion to exclude from trial all computer evidence obtained through a forensic investigation utilizing EnCase software.

The defense brought its challenge on two grounds: 1) that the government's examiner could not establish a proper foundation for the evidence, asserting that EnCase software was essentially providing "expert testimony" and that the defense was unable to cross-examine the government witness in detail regarding how EnCase software works and how it was developed; and 2) that EnCase software should be subject to a *Frye*[158] analysis, which is a legal test employed by many courts in the United States to determine whether a scientific technique for obtaining, enhancing or analyzing evidence is generally accepted within the relevant scientific community as a valid process. (See §3 above.)

The court ruled that the government's trained computer examiner could provide a sufficient foundation for the evidence recovered by EnCase software, and that EnCase software met the *Frye* test as a process with general acceptance and widespread use in the industry.

On the issue of evidentiary foundational requirements, the court relied on the case of *State v. Hayden,*[159] which upheld the validity of enhanced digital imaging technology and the admissibility of evidence obtained through this process. The court noted that like enhanced digital imaging technology, EnCase software is merely a tool utilized by the State's examiner and is not providing expert "testimony." The court determined that the investigating officer who was trained in computer forensics could testify regarding the EnCase process.

On the related argument of the *Frye* analysis, the court similarly upheld the introduction of evidence obtained with EnCase software. The court determined that EnCase software was a widely used and commercially available software tool for recovering computer evidence, including deleted files, and that the investigating officer had conducted his own testing and successfully recovered deleted files on many other occasions. The defense based its *Frye* challenge in part on the theory that only Microsoft could completely and accurately recover deleted files, as the inner workings of the Windows operating system were proprietary.

The government countered by producing an affidavit from an internal computer forensic investigator at Microsoft who testified that his department used commercially available software for the forensic recovery of deleted files, and that EnCase software was one of their primary tools for this purpose. The court expressly took judicial notice of Microsoft's use of EnCase software, which served as one of the considerations in the court's ruling.

Finally, the court relied upon the case of *United States v. Scott-Emuakpor.*[160] The court in *Scott-Emuakpor* determined that the United States Secret Service agents who conducted the computer

157 Okanogan County Cause no. 00-1-0026-8.

158 Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

159 90 Wash.App. 100; 950 P.2d 1024 (Wash. App. 1998).

160 2000 WL 288443 (W.D.Mich. 2000).

forensic examination did not need to be qualified experts in computer science to present their findings and that the USSS agents could provide testimony to authenticate and introduce documents purportedly found on the defendant's computers.

People v. Rodriguez

On January 11 and 12, 2001, in Sonoma County, California Superior Court, a contested hearing took place in the matter of *People v. Rodriguez*[161] where the court subjected EnCase software to a lengthy pretrial evidentiary hearing to establish its foundation as a valid and accepted process to recover computer evidence for admission into court. The *Rodriguez* case involved recovered email messages from defendant Rodriguez's seized computer. Many of the emails sent by Rodriguez included his boasts of committing several armed burglaries and robberies. The emails were highly relevant to Rodriguez's intent and state of mind.

The defense brought its challenge on two grounds: 1) that EnCase software should be subject to a *Frye*[162] analysis, which is a legal test employed by many courts in the United States to determine whether a process for obtaining, enhancing, or analyzing scientific or technical evidence is generally accepted within the relevant scientific community as a valid process; and 2) that the EnCase Report itself should not be admitted into evidence. (The *Frye* test is employed in many state courts, while *Daubert*[163] is the standard in U.S. federal court. Many other countries with a common-law system also utilize standards with many similarities to a *Daubert* analysis for scientific evidence.)

Upon the conclusion of the hearing, the defense conceded that EnCase software was an "appropriate and accepted" methodology under the *Frye* test for recovering computer evidence.[164] After finally admitting that EnCase software represented a valid and accepted process, the defense then focused its attention on whether the EnCase Report itself should be admitted into evidence, under the grounds that the prosecution could not properly authenticate the document.

The court overruled the defense's objection and allowed the EnCase Report generated by the examiner into evidence. After the court's ruling, the trial proceeded and the jury ultimately returned a verdict convicting Rodriguez of robbery, burglary and assault with a deadly weapon.

The transcript features an extensive direct examination and a cross-examination of the computer forensic examiner, addressing in detail the factors related to authenticating the EnCase process under a *Frye* analysis. The prosecution testimony in the *Rodriguez* case is very similar to that of the mock trial transcript provided in Chapter 3, above. Among the findings presented in the hearing were that EnCase software was a widely used and commercially available software tool for recovering computer evidence--including deleted files--and that the investigating officer had conducted his own testing and successfully recovered deleted files on many other occasions. The extensive peer review and publication of the EnCase software was also emphasized. These points and the widespread acceptance

161 Sonoma County, California Superior Ct. no SCR28424.

162 Frye, supra, 293 F. 1013.

163 Daubert, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469.

164 People v. Rodriguez, transcript of January 11, 2001 hearing, p 88, ln 27.

of EnCase software in the industry were important factors that successfully authenticated the EnCase process under the *Frye* test.

The *Rodriguez* case represents another example of the courts subjecting EnCase software to a *Daubert/Frye*-type hearing, which is normally applied to determine the validity of scientific evidence.

United States v. Habershaw

In *United States v. Habershaw*[165], the court upheld the legality of a computer search by computer forensic expert David Papargiris over the defendant's objections. While not reflected in the court's published opinion, EnCase software was used by the experts for both the prosecution and the defense. The expert report submitted to the court by David Papargiris is included in full at the end of this chapter.

Habershaw involved a prosecution for possession of child pornography, where the defendant verbally agreed to have his computer searched. The first responder agents briefly (and, as contended by the defense, improperly) reviewed the defendant's computer, finding child pornography. The defendant subsequently signed a written consent form providing the police consent to search his computer and take "from the premises any property which they desired as evidence for criminal prosecution." The police then took the defendant's computer and some floppy disks into police custody. A few days later, the police obtained a search warrant to search the computer in its custody for material and information related to child pornography stored in the computer. Papargiris then conducted a computer forensics analysis of the hard drive, finding a great deal of incriminating evidence.

There are several compelling rulings and lessons in *Habershaw*, including the following:

1. The court rejected the defense's claims that a "sector-by-sector" search with computer forensic software exceeded the scope of the warrant. The court relied on the *United States v. Upham*[166] decision, which upheld a search where the government retrieved "deleted" computer files, and thus determined that the government could use any means to retrieve information from a computer so long as the information was within the scope of the warrant.
2. The EnCase Timeline feature proved to be important in this case. The opinion reflects intensive testimony regarding file time and date stamps, such as which files were accessed by the case agent, which files were accessed by the suspect before the case agent arrived, and when the computer was shut down for imaging when Mr. Papargiris arrived on the scene and provided expert assistance that proved pivotal. The expert report submitted to the court by Papargiris (provided in full at the end of this chapter) reflects that screen captures from the Timeline view were instrumental in providing important context to the sequence of events described at length in the opinion. Papargiris's report also features effective use of EnCase screen captures.
3. The actions of the case agent--who operated the target computer and accessed files in a live environment--were called into question by the defense's computer forensic expert, who

165 2001 WL 1867803 (D.Mass. May, 13, 2001)

166 168 F.3d 532, 537 (1st Cir. 1999).

claimed that evidence may have been planted by the case agent. Mr. Papargiris was able to show that while files were accessed during the time when the case agent was on the scene, but before Mr. Papargiris arrived, no files on the computer were created or modified during that time. Further, the Timeline showed no additional activity from the point when the computer was ultimately shut down for imaging by Papargiris. The Evidence File's integrated chain of custody feature was helpful in correlating the imaging of the computer to the cessation in activity on the Timeline.

4. This case reflects a growing trend of increased sophistication among defense experts. It is apparent that defense experts are not challenging accepted computer forensics software, but instead using computer forensic software to argue their case. In this case, the defense expert established that the computer was searched by the case agent before a written consent form was signed. However, the Court determined that the suspect had previously given verbal consent, and Mr. Papargiris was able to demonstrate that the files in question were accessed during this consent period. While the end result was favorable, this is an important example of how defense experts can impeach case agents who mishandle computer evidence.

State of Nebraska v. Nhouthakith

In 2001, EnCase software was used to recover evidence in a child exploitation case in Nebraska state court called *State v. Nhouthakith*.[167] The case involved a computer forensics examination by the Nebraska State Patrol that was conducted with EnCase software and that revealed computer graphic image files, whose contents included child pornography. EnCase software was subjected to an extensive *Daubert* hearing, in which the court weighed whether to accept the evidence recovered by EnCase software. The court held:

> That the technique of Acquisition, Authentication and Recovery of Computer Data specifically used in the Encase Software Forensic Tool is relevant in that it will assist the trier of fact to understand the evidence and to help determine a fact in issue and that it is reliable and valid because its methodology has been tested, has been subjected to peer review and publication, has a known or potential rate of error and has been generally accepted within the computer forensic community.[168]

Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.

In this civil case, the issue was not the acceptability of evidence gathered with EnCase software. Rather, the Magistrate Judge addressed the use of a wiping program, Evidence Eliminator, by the plaintiff.[169] This case highlights the disastrous results that can befall a litigant that uses a wiping program such as Evidence Eliminator. In this patent infringement case, the district court, in response to a discovery

167 Case No. CR01-13, District Court of Johnson County, Nebraska.

168 Journal Entry and Order, Nov. 6, 2001, by District Court Judge Daniel Bryan, Jr..

169 Kucala Enterprises, Ltd. v. Auto Wax Co., Inc., 2003 WL 21230605 (N.D.Ill., May 27, 2003).

request by the defendant, ordered the inspection of a computer used by the plaintiff. The defendant then hired an experienced forensic investigator to use EnCase software to create a forensic image and analyze the plaintiff's computer.

On February 28, 2003, the investigator imaged the plaintiff's computer. His analysis revealed that the plaintiff had employed Evidence Eliminator on his computer between midnight and 4 a.m. on February 28th to delete and overwrite more than 12,000 files, and that an additional 3,000 files had been deleted and overwritten three days earlier. In addressing the proprietary of the plaintiff's use of Evidence Eliminator, the Magistrate Judge stated, "Any reasonable person can deduce, if not from the name of the product itself, then by reading the website, that **Evidence Eliminator is a product used to circumvent discovery**. Especially telling is that the product claims to be able to defeat EnCase." (emphasis added)

The court described the plaintiff's actions as "egregious conduct" that was wholly unreasonable, and found the plaintiff at fault for not preserving evidence that it had a duty to maintain. As a result, the Magistrate Judge recommended to the district court that the plaintiff's case be dismissed with prejudice, and that the plaintiff be ordered to pay the defendant's attorney fees and costs incurred with respect to the issue of sanctions. Although the district court did not immediately dismiss the entirety of plaintiff's case, it did dismiss plaintiff's declaratory judgment claims, and left open the possibility of monetary sanctions.[170] In short, the *Kucala* case is an excellent example of the proposition that one of the surest ways to lose a case is to attempt to destroy relevant electronic evidence.

United States v. Greathouse[171]

The *Greathouse* case presents a new twist in computer forensic case law: rather than the typical situation in which the defense challenges the prosecution's use of a particular piece of software, in *Greathouse* the defense argued instead that the prosecution should have used EnCase software.

The *Greathouse* case involved information relayed from the German National Police to law-enforcement authorities in the U.S. in September 2000 regarding child pornography allegedly made available on the Internet by a computer user that went by the name "cyotee."[172] After tracking the user name through the internet service provider (ISP), the investigating agent determined that cyotee was located at a specific residence in Oregon. According to the ISP, the subscriber associated with the name cyotee was David Ihnen, the owner of the residence in question.

After further investigation over a period of months, including surveillance over a three-day period in September 2001, the investigating agent sought and obtained a search warrant on October 16, 2001.[173] Upon execution of the warrant the following day, law-enforcement officers discovered that there were five people living in the house, including Ihnen and defendant, and six computers networked together (five of which were in the den, and one of which was in defendant's bedroom).[174]

170 See Kucala Enterprises, Ltd. v. Auto Wax Co., Inc., 2003 WL 22433095 (N.D.Ill., Oct. 27, 2003).
171 297 F.Supp.2d 1264 (D.Or. Oct. 20, 2003).
172 Id. at 1267.
173 Id. at 1267-68.
174 Id. at 1268.

Two other computers were located in the den but not connected to the network. The execution of the warrant and the interviewing of the residents took place over a three- to four-hour time period.[175] According to the court:

> "[The investigating agent] explained that he decided to seize all of the computers and shut down the network because he could not tell which of the computers had the suspected child pornography and it would take several days to review and make this determination. [The investigating agent] further testified that he could see that the defendant's computer was hooked up to the network because of the presence of a network cable and a network card installed on the computer.
>
> At the hearing, defendant proffered testimony from . . . a computer forensic consultant . . . [who] explained that there is a computer preview program known as ENCASE that has been available for many years that makes it possible to quickly scan computers for certain information. [The expert] testified that, with ENCASE, a computer could be scanned for the presence of child pornography within just a few minutes. [The expert] also testified that there is a "port scan" that can be used to learn more about the nature of computer equipment. [The investigating agent] testified that he was aware of the ENCASE program, that he has this program available, but that he did not bring the program with him for this particular search."[176]

Later, forensic analysis revealed 166 suspect image files on defendant's computer, but none on the other computers in the residence.[177]

The court found that, when the German National Police contacted law enforcement authorities in the U.S., there was probable cause to believe that a computer located within the residence contained child pornography, and that "it was entirely reasonable for the agents to assume, based upon the evidence available, that they were investigating a single computer located in a single-family residence."[178] However, the court granted the defendant's motion to suppress the evidence based on staleness, noting that "the thirteen month delay in this case is simply too long."[179]

Although the basis of the court's decision was the staleness of the information supporting the warrant, the court went on in dicta to address what constitutes best practices in conducting searches in locations where multiple computers may well be present:

> Defendant also claims that the seizure of all eight computers was overly broad and he challenges, under *Franks,* [the investigating agent's] statement in the search warrant affidavit that the computers would need to be searched off-site by a forensics expert.

175 Id. at 1268-69.
176 Id. at 1269.
177 Id. at 1270.
178 Id. at 1271.
179 Id. at 1273.

> Defendant relies upon [his expert's] testimony regarding the ENCASE preview program.
>
> Numerous cases have upheld the wholesale seizure of computers and computer disks and records for later review for particular evidence as the only reasonable means of conducting a search. *See Hay,* 231 F.3d at 637 (agents justified in taking entire computer system off-site for proper analysis); *Lacy,* 119 F.3d at 746; *United States v. Upham* 168 F.3d 532, 534 (1st Cir.1999).
>
> However, I recognize that this may not always be true due to technological developments. In this case, I find that [the investigating agent] acted in reasonable reliance upon well-settled and clear Ninth Circuit authority upholding the right of investigating authorities to seize computers for later forensic analysis given that he had no way of knowing, prior to entry, that he would encounter eight computers instead of one. **Had there been any evidence that a number of suspect computers would be found on site, there may well be an obligation to use a program like ENCASE to more narrowly tailor the search and seizure.**[180] [emphasis added]

Thus, the *Greathouse* case, although decided on other grounds, puts investigators on notice that best practices require up-to-date tools, and that when sophisticated programs like EnCase software are available, investigators will be expected to use them.

State (Ohio) v. Anderson[181]

The *Anderson* case began with a law-enforcement investigation into the activities of Eugene Anderson, who lived in West Virginia but worked in Ohio for Marietta College.[182] The investigation ultimately led to search warrants for Anderson's residence and workplace where officers seized items that included computers and computer media.[183] As described by the court of appeals:

> "Trained forensic officers and analysts examined the computers and used an EnCase program to look at deleted files. Anderson's work computer had recently accessed a computer identified as "Caleb." Officers discovered that Caleb was a special computer server that only Anderson and a Robert Sandford could access. . . . Officers eventually located Caleb at Marietta College and disabled and seized it.
>
> . . . [T]he forensic officers continued to use EnCase and other methods to image or copy the computer hard drives, storage devices, and Caleb to recover deleted data. They

180 Id. at 1275 (emphasis added).
181 2004 WL 413273 (Ohio App. 4 Dist., Mar. 2, 2004).
182 Id. at 1.
183 Id. at 1.

found images of child pornography and evidence that Andersen used and maintained Caleb as a hidden server to store pictures, which included images of child pornography. These images depicted juveniles that were nude or engaged in sexual activity.

The computer examiners also found close to 8,000 Internet relay chat transcripts. One officer identified chats that Anderson had with young men that he had transported from West Virginia to Marietta College so that they could engage in sexual activity. . . . The chat logs further showed that Anderson used Caleb and helped Sandford set up and maintain it at Marietta College. In the chat logs, Anderson repeatedly identified himself, his position, his e-mail address and telephone numbers."[184]

Based largely on the computer forensics evidence, in the trial court the jury found Anderson guilty of 108 criminal offenses. Anderson appealed, arguing that the evidence produced at trial was insufficient to support the verdicts.[185] The court of appeals found that the convictions were supported by sufficient evidence, and were not against the manifest weight of evidence.[186]

NOTE: Please See Chapter 7 for a discussion of *United States v. Maali,* another case in which the forensic images comprised the only computer evidence in existence, as the original drives had been returned to the defendants.

United States v. Andrus[187]

Federal Immigration and Customs Enforcement (ICE) agents searched defendant's home computer at his father's residence using EnCase software. During the examination, EnCase bypassed the log-on user name and password and directly analyzed the contents of the computer hard drive. The defendant was ultimately convicted for possession of child pornography.

Defendant appealed the denial of a motion to suppress the evidence on the grounds that father did not voluntarily consent to the computer search, and that he did not have apparent authority to consent to the search. The Tenth Circuit affirmed the use of the evidence, determining that the use of EnCase, which bypassed the username and password, did not violate the defendant's Fourth Amendment rights.

The ICE agents visited the home of the defendant without a search warrant. The fifty-one year-old defendant lived with his ninety-year-old father. Defendant was not at home. The defendant's father, Dr. Andrus, allowed access to the defendant's unlocked bedroom, and consented to a search of the computer in the defendant's bedroom. An agent quickly connected his laptop to the defendant's

184 Id. at 2.
185 Id. at 3.
186 Id. at 20.
187 483 F.3d 711 (10th Cir.,2007)

computer utilizing the live preview function of EnCase, and began examining the contents of the defendant's computer hard drive. It took ten to fifteen minutes for the examiner to connect and configure his equipment and boot-up the computer to the EnCase boot disk before analyzing the computer. EnCase allowed direct access to the hard drive with no regard to whether a user name or password was needed for normal usage.

During the home examination, the agent used EnCase to search for .jpg files. He was able to see the pathname for the image and trace it to folders on the computer hard drive. The folders and file names indicated child pornography. The examiner estimated that it took five minutes to see the child pornography depictions. The examiner then stopped his search when the agents learned additional facts indicating that the computer belonged to the defendant and being told that the defendant was on his way home. The district court denied a motion to suppress the evidence gathered from the defendant's computer, and the Tenth Circuit affirmed the decision.

The primary issue was the expectation of privacy associated with a home computer in a third-party consent situation where no search warrant had been obtained. The Tenth Circuit observed that the privacy expectation in the computer data is analogous to cases involving suitcases or briefcases. Further, password-protected files have been analogized to a "locked footlocker inside the bedroom." Andrus, 483 F.3d 711, 718 (citing *Trulock v. Freech*, 275 F.3d 391, 403 (4th Cir. 2001)).

However, the court reasoned that the similarity of the computer hard-drive search to cases involving such physical evidence cases was limited. The issue of whether the owner of a suitcase or footlocker has indicated a subjective expectation of privacy turns on whether the item was physically locked. In cases of a computer "lock," the court observed that "a 'lock' on the data within a computer is not apparent from a visual inspection of the outside of the computer, especially when the computer is in the 'off' position prior to the search."[188] The difficulty of seeing such a "lock' on the data is "exacerbated" by forensic software, such as EnCase, which allowed user profiles and password protection to be bypassed.[189]

The determination of third-party consent turns on the officer's knowledge of any password protection on the computer and the physical location of the computer. In this case, the defendant's computer was located in a bedroom occupied by the homeowner's fifty-one-year-old son who cared for his ninety-year-old father. The father had unlimited access to the defendant's bedroom, and the officers did not inquire as to the father's actual use of the computer. The court concluded that the officer's belief in the father's authority to consent to the search of the computer was reasonable.

The court also noted that the issue of whether a password was actually in place on the computer was not relevant in this case, as the password would not have been obvious to the officers at the time they searched the computer. EnCase's software enabled analysis of the computer hard drive without initial determination of whether a user password existed on the computer. The court refused to take judicial notice that password protection is a standard feature of operating systems. The court commented in a footnote that if such judicial notice were taken, then the use of EnCase to override

188 Id. at 718

189 Id. at 719 n. 5

any password protection without indicating whether such protection exists would then be subject to question. "This, however, is not that case."[190]

A key point here was that EnCase was able to quickly analyze key files in the defendant's computer on-site and within a very short timeframe, underscoring the critical importance of the network preview function. Without it, the examination under the short "consent window" would have been impossible.

People v. Donath

In this Illinois case, EnCase software played a critical role in the conviction and sentencing of Howard Donath to 100 years' imprisonment for child pornography and predatory criminal sexual assault.[191] In a forensic investigation using EnCase software, Senior Special Agent Jarrod L. Winkle of the United States Customs Service found 224,376 images and video of child pornography on five computers, seven hard drives, 402 floppy disks, and 376 computer compact discs and other media seized from the defendant's home. According to the Appellate Court, "SSA Winkle had been involved with 150 forensic examination [sic] for child pornography but had never seen a case involving such an enormous amount of images."[192]

People v. Donath represents the longest sentence for child pornography in Illinois to date. According to Agent Winkle, "I exclusively use EnCase in all of my investigations. In this particular case, I was able to locate image files in which Donath was found to be molesting young girls. In another unrelated case, I found one of those files of a girl that Donath victimized that Donath had sent over the Internet. Donath is now serving a 100-year prison sentence, based on my investigation and on the items found during the forensic analysis."[193] The Appellate Court found that the trial court's imposition of a sentence of "30 years' imprisonment for each of three counts of predatory criminal sexual assault . . . and 10 years' imprisonment for child pornography . . . all sentences to run consecutively" was not an abuse of discretion, and upheld the sentence imposed.[194]

Carter v. State (Texas)[195]

The Texas Court of Appeals in *Carter v. State*, upheld the defendant's conviction of possession of child pornography and rejected Carter's argument that evidence collected using the EnCase software was insufficient because duration of possession was not established. Lt. George York of Kaufman County performed a forensic analysis of the computer using EnCase. York found Carter had saved child pornography onto his My Documents folder from his temporary Internet files. This contradicted

190 Id. at 722 n. 8.
191 People v. Donath, 827 N.E.2d 1001 (Ill.App. 1 Dist. 2005).
192 Id. at 1014.
193 E-mail correspondence from Senior Special Agent Jarrod Winkle, May 16, 2005.
194 People v. Donath, 827 N.E.2d at 1015.
195 2006 WL 3628889 (Tex.App.-Dallas 2006).

Carter's statement that he had deleted the pictures once he had noticed the pictures were depicting child pornography.

In addition, York found Carter had renamed the explicit filenames to less conspicuous ones. Using EnCase, York also did a word search analysis of "pedophile" and found Carter had done searches for such terms. York testified that, without software such as EnCase, they could not have retrieved such information. Based upon this computer forensic evidence, the Court found that the jury could have reasonably concluded that Carter knowingly and intentionally possessed the images for a sufficient duration of possession, and thereby concluded the evidence was legally and factually sufficient to support the conviction.

People v. Scolaro

In *Scolaro*[196], the defendant appealed a conviction for the possession of child pornography on the ground that the state failed to prove guilt beyond a reasonable doubt. The defendant rebutted evidence showing that 689 images found on his computer using Encase software did not prove he downloaded, saved, printed, or had control over the images.

Although the defendant presumably attempted to delete the images from the hard drive using a program called "Evidence Eliminator," the special agent recovered the images in a remote section of the defendant's hard drive titled "free space." The free-space repository automatically collects computer data or images when a user visits a website. As a result of EnCase's ability to locate the images, the Court found the defendant voluntarily sought the images by accessing the websites with his credit card and exercised control by having the ability to e-mail, copy, and print the images when they were saved in the free-space repository.

State (Minnesota) v. Levie

In another appellate case, this time in Minnesota, the Court addressed the defendant's argument that evidence of his Internet usage and the existence of an encryption program on his computer should have been excluded.[197] The Court explained that, prior to the start of the trial:

> [The defendant had] objected to the admission of a forensic report on the contents of his computer known as an EnCase Report . . . But the district determined that sections of the report were admissible, and stated, "[I]t is important for the State to be able to follow-up with that evidence to show . . . what the Defendant allegedly did, how he allegedly did it, and what [the author of the report] may have found."[198]

The Appellate Court affirmed the trial court's evidentiary rulings.

196 People v. Scolaro ,910 N.E.2d 126 (Ill.App. 1 Dist. 2009)
197 State v. Levie, 695 N.W.2d 619, 624 (Minn. App. 2005).
198 Id. at 622.

Liebert Corp. v. Mazur

In *Liebert Corp. v. Mazur*,[199] a manufacturer of computer network protection equipment and its exclusive reseller brought an action seeking to enjoin the reseller's former employees from using alleged trade secrets in a new competing business. The trial court denied the plaintiffs' motion for a preliminary injunction, and the plaintiffs appealed. A computer forensics investigation using EnCase software played a prominent role. The appellate court held that defendant misappropriated trade secrets by improper means. "We can infer from [Defendant's] spoliation of the evidence on the laptop that he destroyed evidence of misappropriation, leading us to believe [Defendant] acquired the [trade secrets] through improper means."[200] The court also granted plaintiffs a preliminary injunction based on the "real threat" that Defendant copied the trade secrets onto at least one CD and therefore had the ability to continue to use the trade secrets.

The evidence regarding defendant's spoliation of computer files and CD-burning activity was presented to the court through plaintiffs' expert witness, Lee Neubecker. Using EnCase software, "Neubecker made an exact copy of [defendant John] Mazur's hard drive and then performed extensive searches of the hard drive for any information related to [plaintiffs]."[201] According to the court, the results of Neubecker's investigation "made it more likely than not that Mazur successfully burned the CD."[202] Additionally, the computer forensics investigation revealed that Mazur implemented a "mass wave of deletion," including files containing trade secrets.[203] Moreover, "Neubecker discovered Mazur also purged his computer's application log sometime on February 9."[204]

One aspect of this case that stands out is the deference that the Appellate Court gave Neubecker's conclusions:

> Plaintiff's expert witness testified the information on the laptop indicated [defendant John] Mazur attempted and probably succeeded in copying the price books to a CD. Neubecker also described several scenarios in which information would remain in the "CD burning" folder after a successful burn. Mazur's questionable testimony was the only evidence disputing the expert's findings. Had plaintiffs been able to show Mazur successfully burned the CD, the trial court well may have reached a different outcome, which leads us to Mazur's destruction of the evidence on his laptop's hard drive. Although Mazur's deletion of all the [plaintiffs'] files was problematic, we find his decision to purge the application log particularly suspicious."
>
> Where a party has deliberately destroyed evidence, a trial court will indulge all reasonable presumptions against the party. Whether Mazur successfully made CD

199 Liebert Corp. v. Mazur, 827 N.E.2d 909 (Ill.App. 1 Dist., 2005).
200 Id.at 927.
201 Id. at 918.
202 Id. at 919.
203 Id..
204 Id.

> copies of the price books is a key issue in this case, and, for some unexplained reason, he deleted the application log which would have decisively answered the question. Because Mazur destroyed this crucial piece of evidence, we presume it would have showed he successfully copied the price books onto a CD.
>
> * * * * *
>
> Based on all the evidence presented at the hearing, we reject the trial court's finding on inevitable use.[205]

Porath v. State (Texas)

In this appellate case from Texas,[206] the defendant was charged with felony possession of child pornography. The court described the forensics investigation: "Nickie Drehel, a computer forensics officer, retrieved evidence from the two computers, diskettes, and compact disks. On the diskettes, Drehel found a large number of photographs, some of which appeared to be child pornography."[207] At a pre-trial hearing, Drehel, who used EnCase software in the investigation, "testified to the method utilized to retrieve the images from appellant's computer."[208] The court affirmed the trial court and the defendant's sentence of seven years' imprisonment.

Fridell v. State (Texas)

In this appellate case from Texas, the defendant appealed his conviction for possession of child pornography, arguing that the evidence was insufficient to support the conviction.[209] As in the *Kucala Enterprises* case discussed above, this case illustrates how the use of wiping utilities can backfire. The court described the situation as follows:

> "[Detective] Almond testified . . . that he used "Encase," a computer program that acquires data from a suspect's hard drive and analyzes the data without writing anything to the images obtained. Using this program on appellant's computer, the investigators recovered certain photographs, identified as State's exhibits 1-54. Almond also explained that a "wash" program had been used on the computer's hard drive during the early morning hours of June 19, 2003, and the images of State's exhibits 1-54 had been deleted from the computer but had been recovered during the investigation.
>
> * * * * *

205 Id. at 929.
206 Porath v. State, 148 S.W.3d 402 (Tex.App.-Houston [14 Dist.], 2004).
207 Id. at 406.
208 Id. at 415.
209 Fridell v. State, 2004 WL 2955227 (Tex. App. Dec. 22, 2004).

> The numerous photographs recovered, the extensive use of appellant's computer in searching for child pornography, and the appellant's attempts to erase material from the computer all show that appellant's possession of child pornography was knowing or intentional. We find that the evidence is legally sufficient to support appellant's conviction."[210]

United States v. Bass

In this Tenth Circuit case,[211] the FBI had learned that the defendant was a member of the "Candyman" Internet group. When the FBI, accompanied by a detective of the Enid Oklahoma Police Department, interviewed him, the defendant admitted that he had viewed child pornography on the Internet, and he stated that his computer, at some point in the past, had had a virus that saved such images.[212] The agents received consent to take the computer and conduct a forensic search. As described by the court: "[t]he Enid Police Department conducted the computer forensic search using two programs, "ENCASE" and "SNAGIT." ENCASE recovered over 2000 images of child pornography, and SNAGIT recovered 39 images . . ." In addition, wiping utilities were found. One of the main issues on appeal was whether the defendant had knowingly possessed child pornography. The presence – and admitted use by the defendant – of wiping utilities persuaded the court that "the jury here reasonably could have inferred that Bass knew child pornography was automatically saved to [the] computer based on evidence that Bass attempted to remove the images."[213]

United States v. Davis

This appellate case is of particular note to Guidance Software because the testifying expert, Jon Bair, has been an employee of Guidance Software since 2002. Prior to joining Guidance Software, he was a Special Agent with the U.S. Army Criminal Investigation Command. In this case heard by the U.S. Army Court of Appeals, the defendant had appealed his conviction on the basis that certain privileged testimony was admitted into evidence in error.[214] While the court ruled that the privileged testimony was indeed admitted in error, it nonetheless upheld the conviction because the computer forensic evidence, gathered using EnCase software, was so strong as to make the error harmless:

> Special Agent (SA) Jonathan Bair, U.S. Army Criminal Investigation Command (CID), examined the hard-drives and disks that he seized from appellant's home, and discovered deleted files containing thousands of images depicting what appeared to be children engaging in sexual activity. Special Agent Bair also discovered seven

210 Id. at 2-3.
211 United States v. Bass, 411 F.3d 1198 (10th Cir. 2005).
212 Id. at 1200.
213 Id. at 1202.
214 United States v. Davis, 61 M.J. 530 (Army Ct.Crim.App. 2005).

undeleted images of a similar nature on a floppy disk seized from the vicinity of appellant's home computer.

* * * * *

The government's case was very strong. The computer hard-drives and floppy disks seized with appellant's consent from his home contained thousands of images of child pornography, thus supporting the government's theory that appellant wrongfully possessed child pornography . . . The defense case was, by contrast, very weak. The crux of the defense was that these images had been unknowingly downloaded to appellant's computer and deleted upon discovery. The possibility of such innocent possession was severely undercut by the fact that images were found in a number of different drives and folders, including seven images that were found on a floppy disk that had to have been manually saved to that location.[215]

United States v. Long

In this Seventh Circuit case, the court described the search of the defendant's digital media as follows:

> "[The detectives' laptop] was equipped with EnCase diagnostic software. (The "EnCase Cybercrime Arsenal" package is sold by a company called Guidance Software to the law enforcement community;[216] it is described as a powerful search and diagnostic program. See http://www.guidancesoftware.com.) Using the EnCase software, the detectives searched the CDs and found movies and photos of child pornography on them. When Long's laptop was searched at a later date, the detectives found tens of thousands of images and over a hundred movies of child pornography on it as well."[217]

The court of appeals affirmed the district court's denial of Long's motion (made on the basis that the search exceed his consent) to suppress the evidence.

United States v. Houston[218]

Defendant moved to suppress all digital and physical evidence in connection with being charged with possession of child pornography. The investigator brought in to assist with creating and processing a forensic image of the defendant's computer used EnCase to search for keywords in emails sent and received by the defendant. The Magistrate Judge recommended to the District Court that Defendant's

215 Id. at 531, 537.

216 Although the Cybercrime Arsenal package is offered to law enforcement, EnCase software itself is available to the public at large.

217 United States v. Long, 425 F.3d 482, 484 (7th Cir. 2005).

218 754 F. Supp. 2d 1059 (D.S.D. 2010).

Motion to Suppress be denied. The District Court adopted the recommendation and the motion was denied.

Two-Way Media, LLC v. AT&T, Inc.[219]

Court notes deposition testimony of defendant's litigation manager stating that all of the evidence collected remotely from their New Jersey location was done using EnCase.

In re Hitachi TV Optical Block Cases[220]

In an interesting defensive use of forensic software, the court denied Plaintiffs' motion for sanctions because defendants had shown that (1) the files were not destroyed, (2) that the retrieved fragments more likely than not were already produced documents, and (3) that the three that were irretrievable were not relevant. Additionally, there was no evidence of intent of impede plaintiffs' access to evidence, and therefore, no evidence of bad faith. The defendant's forensic consultant used Encase, "the industry standard and most widely recognized computer forensic software platform", to recover deleted files from the hard drive. The court observed that Encase examines the space on the hard drive where the deleted files were stored, as recorded on the Master File Table.

United States v. Kuntz[221]

The defendant attempting to get the evidence of child pornography against him suppressed. The defendant asserted that the discovery materials he was provided with included references to a Dell computer he possessed, as well as references to a computer owned by another person. The defendant claimed he does not know this other person. The defendant contended that because the discovery was not clear as to which evidence related to him and which evidence was connected to the other individual, the evidence from the Dell computers should be suppressed. The Special Agent in Charge testified that he prepared an EnCase report which detailed the specific files and images found on defendant's computer depicting the sexual exploitation of minors. The motion to suppress was denied.

Brown v. Aud[222]

Court notes that evidence leading to the original conviction of the defendant was collected from a computer at his residence using EnCase. The investigator testified at trial that EnCase software allows reproduction of all files that have not been overwritten, including Internet files. In particular, he testified that "[Encase] created—it created the image, which is a—refer to as a mirror image, is an exact copy of everything that's on the hard drive; not only the data but everything else that's there. Maybe a file that was deleted at one time. It copies all of the data off of it"

219 636 F. Supp. 2d 527 (S.D. Tex. 2009).
220 2011 U.S. Dist. LEXIS 90882 (S.D. Cal. 2011).
221 2011 U.S. Dist. LEXIS 37893 (D.N.D. 2011).
222 868 F. Supp. 2d 608 (E.D. Mich. 2012).

Whitmore v. Cate[223]

Court find that an investigator in the case was provided with an exact copy of a hard drive created by EnCase, in order to permit him to examine the evidence without tampering with the original computer hard drive, which was later destroyed.

United States v. Soto[224]

The trial court denied the defendant's motion to suppress incriminating evidence on a laptop computer found in a car purchased by him. The appellate court noted trial testimony from a United States Secret Service Agent, who performed a computer forensics examination of the seized laptop, establishing that the Agent used EnCase to image the laptop's hard drive and perform his analysis.

United States v. Stanley[225]

Defendant appealed his convictions for possession of child pornography, arguing that the trial court erred in admitting expert testimony by the agent who conducted the forensic examination of his computer. Defendant's convictions were affirmed. The agent performing the forensic examination testified that she used EnCase to make a mirror image of the defendant's computer in order to examine its contents without risking damage to the original. The examination revealed that the defendant had downloaded and installed a peer-to-peer file sharing program called FrostWire. She was also able to determine that this program was used to search and download child pornography as well as to view, keep and share it.

United States v. Cotterman[226]

EnCase was used to collect evidence of possession of child pornography from a laptop seized at the Mexico-California border. In reversing a district court order suppressing the evidence, the Ninth Circuit sitting *en banc,* observed that "[Encase] copied, analyzed, and preserved the data stored on the hard drive and gave the examiner access to far more data, including password-protected, hidden or encrypted, and deleted files, than a manual user could access."[227]

NOTE: The above-listed cases are not an exhaustive list of EnCase references. To date, over 125 opinions from U.S. cases reference the use of EnCase software. Please See Chapter 2 for a Discussion of *Logan v. State*, a Court of Appeals of Indiana Decision involving EnCase Software, and Chapter

223 2012 U.S. Dist. LEXIS 130977 (S.D. Cal. 2012).
224 720 F.3d 51 (1st Cir. 2013).
225 2013 U.S. App. LEXIS 14643 (4th Cir. 2013).
226 709 F.3d 952 (9th Cir. 2013) (en banc).
227 Id. at 963 FN9.

7 for a Discussion of both *United States v. Riccardi*, a Tenth Circuit decision that involved EnCase software, and *United States v. Calimlim*, a federal case from Wisconsin involving EnCase software.

Other Jurisdictions

Regina v. Cox

In addition to the wealth of case law in the United States, the use of EnCase software has been widely accepted by courts in other common-law jurisdictions. For example, in 2003, a Canadian court addressed EnCase software in *Regina v. Cox*.[228] In that child pornography case, the Royal Canadian Mounted Police had used EnCase software to image and analyze three hard drives. On application by the defendant to compel the prosecution to turn over a copy of the EnCase software, the Court discussed how EnCase software is used, and ruled that the images and the forensic report produced by EnCase software were relevant evidence, but that the software itself was a tool used by experts, and not evidence.

Regina v. D.E.W.B.

In another Canadian case in Alberta Provincial Court called *R. v. D.E.W.B.*[229], police computer forensics investigators used EnCase software to preview and recover crucial evidence. The court explicitly accepted the reliability of EnCase software and its use in uncovering admissible evidence for a criminal trial.

The defendant in the case shared a home computer with his wife. His wife had inadvertently discovered child pornography on the computer, which she mentioned to certain Child Welfare authorities. The Child Welfare officials notified the Calgary Police, who obtained a search warrant. Detectives from the Technological Crimes Unit of the Calgary Police Service used EnCase software to examine the subject computer. There was conflicting testimony about whether the defendant actually informed the police investigators of the location of the child pornography, but in any event, the evidence was recovered and the defendant was charged with possession of child pornography.

The court noted that "the 'Encase' program allows the police to view what is on a computer without altering any of the date[sic] on the computer." The court further elaborated regarding EnCase software: "[o]ne of the things that the police were able to determine through the 'EnCase' program were the dates that the child pornography was placed in the computer's files . . . Those images were found in files created between August, 2001 and January, 2002."

Ultimately, the defendant was convicted of possession of child pornography. The *R. v. D.E.W.B.* case is important because it re-emphasizes that EnCase software is a reliable, widely available, and court-approved computer forensics tool.

---

228 2003 ABQB 212 (Mar. 7, 2003).

229 2003 ABPC 190 (Nov. 28, 2003).

Regina v. J.M.H.[230]

In this case, the Ontario Superior Court of Justice addressed the admissibility of a computer forensics report that had been prepared by a detective in the Ottawa Police Service using EnCase software. The defendant was alleged to have detained a child inside of his residence and to have shown adult pornography to the child on his computer.[231] Pursuant to a warrant, two computers were seized at the defendant's home, and a forensic analysis was undertaken to determine whether the computers had been used during the time the offense was allegedly committed.[232]

The court reviewed the qualifications of the computer forensics investigator, which included training described by the court as "Intermediate Encase Computer Forensic course."[233] The Crown asserted, and the court accepted, that scrutiny of expert evidence is based on four factors: (1) relevance, (2) necessity, (3) the absence of an exclusionary rule; and (4) a properly qualified expert.[234] The court held that the investigator was qualified to present digital evidence located on the defendant's computer.[235] The investigator's testimony established that one of the defendant's computers was in use during the time in question, and that the computer was used exclusively to surf pornographic sites.[236] The court held that "the evidence is material, relevant, compelling and reliable."[237]

Ler Wee Teang Anthony v. Public Prosecutor

In 2002, an appellate court in Singapore, in upholding a murder conviction, relied on evidence recovered through the use of EnCase software.[238] The Techno Forensic Branch of the Technology Crime Division of the Criminal Investigation Department of the Singapore Police had used EnCase software to retrieve a deleted file from one of the defendant's computers. The recovered file was quoted in detail by the court as evidence of the defendant's guilt.

State (N.C.T. of Delhi) v. Sandhu[239]

This extremely high profile case centered on the December 13, 2001, terrorist attack on the Parliament of India in which eight policemen, one civilian, and five terrorists were killed.[240] Mohammed Afzal's death sentence was upheld in the Supreme Court of India based in part on evidence, acquired using EnCase software, obtained from a laptop computer that had been seized from Afzal, who was charged with coordinating the attack. Using EnCase software, police recovered evidence showing that the

230 2003 O.J. No. 5513 (Dec. 5, 2003).
231 Id. at ¶ 3.
232 Id.
233 Id. at ¶ 14.
234 Id. at ¶ 7.
235 Id. at ¶ 15.
236 Id. at ¶ 20.
237 Id. at ¶ 65.
238 Ler Wee Teang Anthony v. Public Prosecutor, Court of Appeal, Criminal Appeal No. 27 of 2001 (April 19, 2002).
239 The Supreme Court's judgment can be found at http://judis.nic.in/supremecourt/qrydisp.asp?tfnm=27092
240 See, e.g., http://www.tribuneindia.com/2005/20050805/main1.htm

laptop had been used to make forged identity cards found on the bodies of the terrorists who were killed in the attack.[241]

Australian Cases

Peach v Bird [2006] NTSC 14 (Australia)

In *Peach v. Bird*, the appellant utilized evidence extracted with EnCase software to overturn the dismissal of a child pornography charge against the respondent. In September of 2005, Australian authorities charged Thomas Bird with the "simple defence" of possession of child pornography after investigators retrieved the digital remains of child pornography from his personal computer.

At trial, the prosecution offered the testimony of Detective Senior Constable Fausett. Fausett personally examined Bird's personal computer with the assistance of EnCase software. Based on his investigation with EnCase, Fausett testified that Bird had permanently deleted seventy image files from his computer. An "eraser program" was used to expunge the images; however, the names of the files were recoverable with EnCase software. Fausett cross-referenced the names of the image files with several child pornography sites, which were transcribed in a text document on Bird's hard drive. The detective discovered that one of the file names (8087053lg0.jpg) corresponded with a pornographic image found on one of the illegal websites. Bird admitted to transcribing URLs of the child pornography sites to the recovered text document, but denied ever visiting the sites.

Reasoning that "during night time surfing of the net looking at pornography sites and accessing adult chat rooms, [Bird] inadvertently downloaded this particular picture" the trial judge dismissed the charges against the defendant. The prosecution appealed the decision citing that the judge's decision was not based on evidence provided by either side. No evidence was presented that could be sourced for the inference that the images were accidentally downloaded to the defendant's computer. In fact, contrary testimony was provided by expert witnesses who stated that Bird must have made a concerted decision to download the images. Based on the expert testimony and the evidence provided by EnCase, the appellant court set aside the dismissal and ordered a retrial of the case.

Grant v. Marshall[242]

The *Grant* case involved a discovery matter in which the applicant, Grant, sought information concerning the identity of the author of e-mails who made allegations that Grant had engaged in corrupt activities. The Federal Court of Australia noted "that it may be possible, by examination of the hard drive of the computer in question, to obtain information that could assist in identifying the author of the e-mails.[243] The court specifically addressed the forensic imaging process as follows:

---

241 See http://www.chennaionline.com/colnews/newsitem.asp?NEWSID=%7B4A181E08-74B0-487D-910C-09C15658A43C%7D&CATEGORYNAME=NATIONAL

242 2003 WL 22407255 (Fed. Court), N1161 of 2003 (Sept. 19, 2003).

243 Id. at ¶ 4.

> Proper acquisition of computer evidence requires the use of non-task. Such software recovers, searches, authenticates and documents relevant electronic evidence without compromising the integrity of the original evidence. PricewaterhouseCoopers currently use "EnCase" software, **which is the industry standard**.
>
> * * * * *
>
> **The EnCase forensic image has an in-built audit trail with a sophisticated integrity validation process**.[244] [emphasis added]

The court ordered the Council of the Municipality of Mosman to "refrain from deleting, moving, erasing, altering, concealing or tampering with any document, whether electronic or otherwise" that is relevant to the issue in question.[245] In addition, the court ordered the Council of the Municipality of Mosman to provide Peter Chapman, a computer forensics investigator with PricewaterhouseCoopers, "with access to the hard drive . . . of the computer which is associated with IP address 203.111.117.212 for the purpose of enabling" a forensic investigation.[246]

Sony Music Entertainment (Australia) Ltd. v. Univ. of Tasmania, et al.

The Federal Court of Australia addressed EnCase software in *Sony Music Entertainment (Australia) Ltd. v. Univ. of Tasmania, et al.*,[247] The *Sony* case involved the use of file-sharing networks by university students for alleged copyright piracy, and a discovery dispute between the parties regarding the scope of information that should be supplied by three universities. The Federal Court of Australia allowed the computer forensics investigator hired by Sony to employ EnCase software to search the available digital evidence.

The court noted that if the computer forensics investigator agreed to certain confidentiality provisions, "then access could be given to all of the preserved records to search using the EnCase program." The court specifically found the use of EnCase software preferable to the discovery methods proposed by the universities, stating that "if the narrow search tools and methods proposed by the Universities . . . are used, then it is likely that there will be insufficient discovery."

244 Id. at Annexure A.
245 Id. at Order no. 3.
246 Id. at Order no. 4.
247 Fed. Court, NSW Dist., N128 of 2003 (May 30, 2003).

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA Criminal No. 01-10195-PBS

KEVIN HABERSHAW

REPORT OF GOVERNMENT EXPERT WITNESS
DETECTIVE DAVID C. PAPARGIRIS

I, David C. Papargiris do hereby state:

I am a detective with the Norwood Police Department in Norwood Massachusetts. I have been employed with the Norwood Police for 17 Years and have been assigned to the Bureau of Criminal Investigations for 4 years. I conduct all investigations into computer crime, Internet investigations as well as being a computer forensics examiner.

I have been working with personal computers for (8) years. I am a member of the United States Secret Service Electronic Crimes Task Force Boston Region, the High Technology Crime Investigation Association (HTCIA) and the Regional Electronic and Computer Crime Task Force located in Raynham, Massachusetts. I have received formal training on the processing of computer evidence and the science of computer forensics from HTCIA, United States Attorney Generals Office and the Internet Crimes Inc. I have also successfully completed the National White Collar Crime Centers Basic Data Recovery four and a half day school in Portland, Maine. I have completed the four day training course on Guidance Software Corporation's computer forensics software program," Encase". I have attended the Boston University's weeklong training on Windows NT titled Network Essentials. I have safely recovered evidentiary data from personal computers, during investigations involving fraud, identity fraud, hacking cases and crimes against children. I have testified in district court, grand juries and federal court on computer issues, along with the proper means of securing and processing computer evidence.

In preparing this brief, I conferred with court certified computer forensic expert, William C. Siebert, the Director of Technical Services for Guidance Software, maker of the computer forensic software, EnCase. A copy of his CV is attached at the end of this report.

I. Newsgroups:

USENET is a world-wide distributed discussion system. It consists of a set of "newsgroups" with names that are classified hierarchically by subject. "Articles" or "messages" are "posted" to these newsgroups by people on computers with the appropriate software -- these articles are then broadcast to other interconnected computer systems via a wide variety of networks. Usenet is available on a wide variety

of computer systems and networks, but the bulk of modern Usenet traffic is transported over either the Internet or UUCP.

USENET newsgroups consist of some 15,000+ topical entities which constitute an immense worldwide forum for discussion and discourse. These newsgroups actually pre-date the existence of the World Wide Web and are now an integral part of the "Internet experience". These forums for discussion range in subject from Ancient Art to Zen Buddhism, and within the "threaded" structure of each group emerges the true spirit of debate and a poignant example of freedom of speech. Though a few newsgroups are moderated (having a designated member of the group with oversight powers to keep the discussion on track,) most newsgroups are free forums, and may seem at times like free-for-alls, but taken as a whole, they provide a noble service in giving each and every user an equal voice.

Newsgroups can be compared to a bulletin board that you might see at a grocery store or on the wall at any college campus, except that imagine if after pinning a postcard to the bulletin board a duplicate postcard appeared on every bulletin board in every grocery store or college campus in the world within one hour.

It is true that Usenet originated in the United States, and the fastest growth in Usenet sites has been there. Nowadays, however, Usenet extends worldwide. The heaviest concentrations of Usenet sites outside the U.S. seem to be in Canada, Europe, Australia and Japan.

No person or group has authority over Usenet as a whole. No one controls who gets a news feed, which articles are propagated where, who can post articles, or anything else. There is no "Usenet Incorporated," nor is there a "Usenet User's Group." You're on your own.

Despite its most noble intent, the darkest side of the Internet will be found within a number of newsgroups. These are the pedophile newsgroups. Perhaps at one time, these forums functioned as discussion groups for people of similar, though no less frightening interests, that being the exploitation of children for the sexual gratification of the adults who control them. These newsgroups, as most pornographic newsgroups, are not moderated.

Granted, there are various activities organized by means of Usenet newsgroups. The newsgroup creation process is one such activity. But it would be a mistake to equate Usenet with the organized activities it makes possible. If they were to stop tomorrow, Usenet would go on without them.

Newsgroups are locations on the Internet that are accessed through a mail program such as Outlook Express. You have to set up your news account using information supplied to you by an Internet Service Provider (ISP); i.e. Mediaone.net, AT&T Roadrunner, Earthlink.net, etc. Your newsgroup section is different from your mail program that is also managed by your ISP. Your ISP has numerous servers one is a mail server and one is a news server, many customers never set up their news server and never go onto newsgroups at all.

This technology allows for the instantaneous electronic transmission of pictures over the Internet. These pictures are converted or encoded to a binary format and sent in a similar manner as a text message. The process is as simple as sending an email. Once uploaded, the encoded binary message appears within the newsgroup where it can be downloaded by any user and decoded back into its original form, and when this decoded format is accessed through an image viewer, it becomes a

photograph. I have witnessed for myself some of the images that have emerged from the pedophilia newsgroups. The computer picture format most often found on the newsgroup is jpegs.

II. What is a JPEG?

JPEG (pronounced "jay-peg") is a standardized image compression mechanism. JPEG stands for Joint Photographic Experts Group, the original name of the committee that wrote the standard.

JPEG is designed for compressing full-color or gray-scale images of natural, real-world scenes. It works well on photographs, naturalistic artwork, and similar material; not so well on lettering, simple cartoons, or line drawings. JPEG handles only still images, but there is a related standard called MPEG for motion pictures.

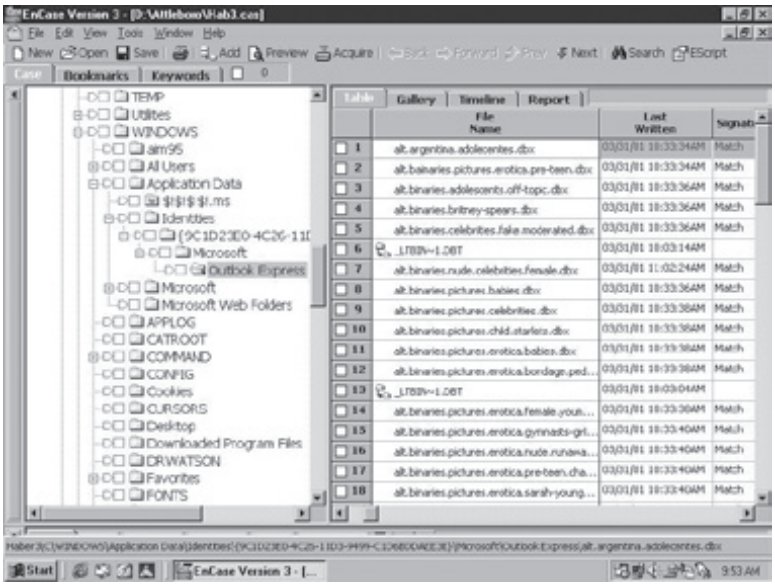
JPEG is "lossy," meaning that the decompressed image isn't quite the same as the one you started with. (There are lossless image compression algorithms, but JPEG achieves much greater compression than is possible with lossless methods.) JPEG is designed to exploit known limitations of the human eye, notably the fact that small color changes are perceived less accurately than small changes in brightness. Thus, JPEG is intended for compressing images that will be looked at by humans. If you plan to machine-analyze your images, the small errors introduced by JPEG may be a problem for you, even if they are invisible to the eye.

III. Continued Review of Kevin Habershaw's Computer

On February 15, 2002, as part of my research, I signed on to a news server on a computer which never had one assigned to it before. After setting up the account the first thing you are told is that the news server is going to get a list of newsgroups that are available on your ISP's news server. I received a list of 67,019 newsgroups. There are newsgroups available for just about any subject, as described above. After the list comes down into the window, you can scroll through the list or type in a keyword of what type of newsgroup you are looking for.

There are two ways to go to a newsgroup one way is to highlight the newsgroup and select GOTO and the other way is to select SUBSCRIBE. If you select GOTO, you are brought to that newsgroup and as much as three hundred messages could appear in the news window. If you double click on a message it could bring you to text or to a hyperlink to go to a web page or show you a graphic (photo) file. Once you exit the newsgroup it will ask you if you would like to SUBSCRIBE to the newsgroup.

If you select GOTO, or SUBSCRIBE to, in the newsgroup box a reference to that newsgroup is placed in your outlook express [sp] folder.



As you can see from this graphic, the left side of the windows indicates that I am in the Outlook Express folder. The right side of the window shows the items in that folder. The right side lists the newsgroups that were visited.

When an individual configures up their newsreader and either selects GOTO or SUBSCRIBE to a newsgroup, that information is stored on their hard drive. The computer forensic software, Encase [sp], allows an examiner to review the contents of a hard drive under investigation.

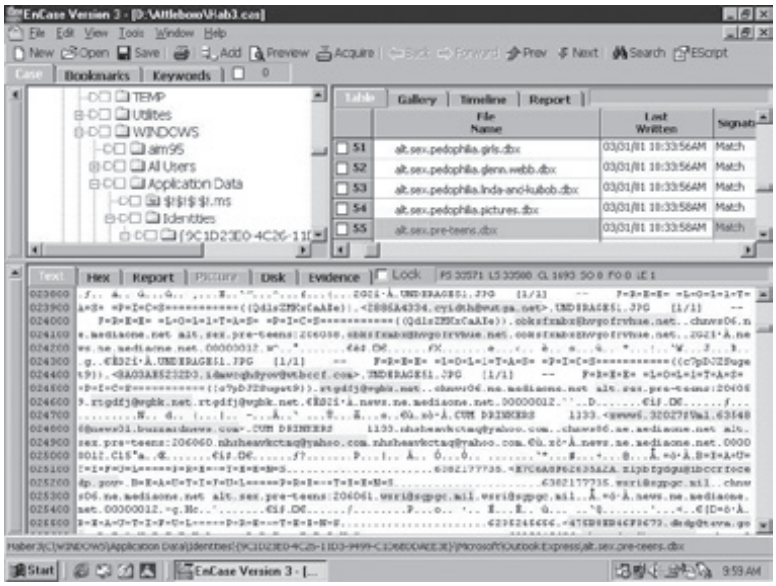
IV: Newsgroups on Kevin Habershaw's Computer

A review of the contents of Kevin Habershaw's Outlook Express folder shows those newsgroups of interest to him. The newsgroups included:

Alt.argentina.adolescents
Alt.bainaries.pictures.erotica.pre-teen
Alt.binaries.adolescents.off-topic
Alt.binaries.britney-spears
Alt.binaries.celebrities.fake.moderated
Alt.binaries.nude.celebrities.female
Alt.binaries.pictures.babies
Alt.binaries.pictures.celebrities
Alt.binaries.pictures.child.starlets
Alt.binaries.pictures.erotica.babies
Alt.binaries.pictures.erotica.bondage.ped
Alt.binaries.pictures.erotica.female.young
Alt.binaries.pictures.erotica.gymnasts-girl
Alt.binaries.pictures.erotica.nude.runaway
Alt.binaries.pictures.erotica.pre-teen.chatter
Alt.binaries.pictures.erotica.sara-young
Alt.binaries.pictures.girls
Alt.binaries.pictures.humor.babies
Alt.binaries.pictures.kids
Alt.binaries.pictures.olsen.twins
Alt.binaries.pictures.spice-girls
Alt.binaries.stories.sex
Alt.disgusting.stories.my-imagination
Alt.fan.britney-spears
Alt.fan.emma-bunton
Alt.fan.Melissa.j-hart

Alt.fan.olsen.twins
Alt.hipclone.kids.sexual-abstinence
Alt.idiot.pedophile.reb-ruster
Alt.idiot.pedophile.snoopy
Alt.no.advertising.files.images.sex.preteens
Alt.no.advertising.files.images.nude.preteens
Alt.Pedophiles
Alt.sex.children
Alt.sex.girls
Alt.sex.incest
Alt.sex.pedo.moderated
Alt.sex.pedophilia
Alt.sex.pedophilia.girls
Alt.sex.pedophilia.glen.webb
Alt.sex.pedophilia.Linda-and-kuibob
Alt.sex.pedophilia.pictures
Alt.sex.preteens
Alt.sex.stories.babies
Alt.sex.stories
Alt.sex.stories.incest
Alt.sex.stories.moderated
Alt.sex.stories.tg
Alt.sex.young
Alt.stories.erotic
Alt.stories.incest
Alt.Transformation.stories
Alt.transgendered
Alt.transgendered.Jeffrey-boyd
Alt.binaries.nude.celebrities.female
Pedo.binaries.pictures.erotica.children

Once you click on a newsgroup name, you can see the database of messages for the newsgroup, alt.sex.pre-teens for March 31st at 10:33:58 AM. These titles could lead you to text or a graphic file or a hyperlink (text that once clicked brings you to a web page) that had shown up in the newsgroup box. These references are left on a person's hard drive only if they have selected GOTO or SUBSCRIBE in their newsreader. Habershaw's Outlook Express folder showed that there were 61 references to newsgroups that he had visited. Alt.Sex.Pre-Teens, showed references to the terms like lolita, alt.sex and preteen, as did other newsgroups that had been accessed at 10:34 AM on the 31st of March. It was said that the term "preteen" did not come up during the keyword search under EnCase. The reason for this was because of the spelling in the newsgroup showed it as P=R=E=T=E=E=N.



Looking with in the lower box in EnCase it shows references to the newsgroup alt.sex.pre-teens. On the first line you can see a reference to underage51.jpg, which is an attached computer picture file available for downloading.

I also checked the timeline to see if in fact that the newsgroups were being updated every 30 minutes.

After checking the timeline, I could see that at 0930 hours on the 31st of March, two newsgroups were accessed. At 1002 Hours [sp], four newsgroups were accessed, and starting at 1033 hours forty-five different newsgroups were accessed. At 1101 hours 1 newsgroup was accessed. If the newsgroup were being checked automatically every thirty minutes, there would be the same amount of newsgroups accessed every thirty minutes, and this would show up in the timeline within Encase. Because different numbers of the newsgroups appear at different time intervals on the timeline, I do not believe that Habershaw's computer was automatically updating newsgroups every thirty minutes.

-- END OF REPORT --

7. Search and Seizure Issues and EnCase Software

§ 7.0 Overview

Issues related to the search and seizure of computer data constitute an area that has benefitted from the excellent research and writing of prosecutors and government attorneys. The Federal Guidelines on Searching and Seizing Computers, found at www.cybercrime.gov, is a must-read for every computer investigator. To distinguish, this Journal focuses on the more narrow search-and-seizure processes that are potentially impacted by the use of EnCase software. For example, the plain view doctrine is now more complex because EnCase software, by means of command-line utilities, allows forensic examiners to view, sort and manage many more files than previously possible. Important cases such as *United States v. Long* [248] specifically address this issue in the context of EnCase while providing important guidance.

The remote preview function of EnCase software also plays an important role in search-and-seizure issues. Many users report successful employment of the non-invasive EnCase remote preview feature in consent search situations. One reported decision, *United States v. Andrus*[249] directly illustrates this key benefit of EnCase software. (Please see Chapter 6 for a full discussion of *United States v. Andrus*.) Obviously, one is more likely to allow the search of one's computer if the preliminary exam can be done quickly and without "impounding" a favorite laptop. The feature is also very useful in increasingly common scenarios where the examiner is faced with numerous items of media and/or severe time constraints and needs to prioritize the media on the scene, or where a "blind" examination of media potentially containing other privileged documentation is required.

This chapter will focus on the areas of search-and-seizure law where EnCase software impacts many of the procedures and considerations addressed by current case law.

§ 7.1 EnCase-Specific Court Decisions Concerning Search and Seizure Issues

With the extensive use of EnCase in the field by the government, several courts have naturally addressed issues concerning the use of EnCase in the context of the Fourth and Fifth Amendments of the United States Constitution, which afford protections for citizens against unreasonable search and seizure and self-incrimination.

With its opinion in *United States v. Long*, the Seventh Circuit Court of Appeals issued what is to date the most important case directly addressing EnCase in the context of the Fourth Amendment.

In *United States v. Long*, the court rejected a defendant's assertion that the extensive and robust

248 United States v. Long, 425 F.3d 482 (7th Cir. 2005).

249 2007 WL 1207081 (10th Cir. Apr. 25, 2007).

functionality of EnCase meant that its use by law enforcement was prone to exceed constitutional bounds. The Court determined that law enforcement's use of EnCase did not exceed the scope of the voluntary consent provided by the defendant, despite the "powerful search" capabilities of EnCase. [250] The court described the search of the defendant's digital media as follows:

> "[The detective's laptop] was equipped with EnCase diagnostic software. (The 'EnCase Cybercrime Arsenal' package is sold by a company called Guidance Software to the law enforcement community; it is described as a powerful search and diagnostic program.) Using the EnCase software, the detectives searched the CDs and found movies and photos of child pornography on them. When Long's laptop was searched at a later date, the detectives found tens of thousands of images and over a hundred movies of child pornography on it as well." [251]

The Seventh Circuit affirmed the district court's denial of Long's motion (made on the basis that the search exceeded his consent) to suppress the evidence. In a key explanation of its decision, the court stated, "The fact that the EnCase search engine was sophisticated is of no importance. We agree with the district court's conclusion that Long "could not reasonably assert at this point that he didn't understand that [the police] were going to search any CDs that they found."

While *Long* involves the question of whether using the "powerful" search capabilities of EnCase exceeded the scope of the consent, a prosecutor should be able to extend this holding to analogous issues such as the "Plain View" doctrine and whether the scope of a warrant had been exceeded under a similar fact pattern.

Rosa v. Commonwealth [252] presents such a situation. The court held that a Virginia State computer crime investigator who used EnCase in an Internet crime investigation was entitled to open all files, including picture files, on a hard drive in a suspect's computer under a search warrant. The warrant authorized a search for computer and computer devices bearing information on conversations with the victim or conversations or files listing the suspect's screen name. Per the published opinion from the Virginia appellate court, "[the investigator] examined the computer using a program called EnCase, which is designed to recover any data located on a hard drive, whether it is an active computer file or a previously deleted file. After appellant's hard drive was copied, [the officer] performed keyword searches with specific words related to the terms on the warrant."[253]

The court recognized that EnCase:

> "[a]llowed a search of the contents of files as well as the names of files. Although (Officer) Deem testified that chat sessions would normally be saved as files with text extensions, he also opened files that did not have text extensions, such as picture or jpeg files, after completing the keyword search. He noted that it was common practice

250 425 F.3d at 482, 486-487.
251 Id. at 484.
252 628 S.E.2d 92, (VA App. 2006)
253 Id. at 93.

> to manually open picture files. The reason for doing this was that any text saved as a jpeg file would not be found by only conducting a word search, and it was possible to save a chat session as a jpeg file. Several chat sessions were in fact saved in jpeg files on appellant's computer. Deem stated that he '[c]ould not determine whether a particular jpeg file fell within the scope of the search warrant until he opened it to see if it contained relevant information.' While Deem was opening jpeg files, he viewed an image that he believed to be child pornography. He immediately stopped opening picture files and applied for and received a second warrant that allowed him to specifically search for sexually explicit pictures of children. Appellant had deleted the files containing child pornography from his computer, and they were visible only when Deem re-created them using the EnCase program."[254]

Thus, the court ruled that pictures obtained in this case were properly admitted:

> "After performing a keyword search, the officer glanced at the picture files to determine whether they fell within the scope of the search warrant. The officer testified that he commonly opened picture files when conducting a computer search, because any text saved in a picture file would not be found simply by using a word search. Indeed, a number of chat sessions were located in picture files on appellant's computer. Once the officer viewed the image he believed to be child pornography, he immediately obtained a second warrant. As a result the officer acted properly in opening files with various extensions in order to ascertain if they contained relevant material, and the trial court did not err in denying the motion to suppress." [255]

Finally, the *Rosa* court also rejected the argument that deleted files are entitled to additional protection, and held that the officer was entitled to examine all of appellant's files with EnCase, including the deleted ones, to determine whether they contained items that fell within the scope of the initial warrant. The court reasoned that the warrant authorized a search of all "electronic processing and storage devices, computer and computer devices, [and] external storage devices" and did not limit the search to any specific area of the computer. The officer, therefore, was permitted to look in any section of the computer that might contain the objects of the search, including deleted files that had been re-created using EnCase. [256]

Another case, which expressly followed the rationale adopted by the *Rosa* court, is *Russo v. State* [257]. In this capital murder case, the Texas appellate court noted that:

> Detective Roy Rector, a forensic computer examiner with the Austin Police Department, first made a copy of the computer's hard drive, which is protocol for forensic computer

254 Id. at 94.
255 Id at 97.
256 Id.
257 228 S.W.3d 779 (Tex App 2007).

> examination. Rector examined the computer with a program called 'Encase,' which is designed to recover any data located on a hard drive, whether it is an active computer file or a previously deleted file. Rector then performed some keyword searches on the hard drive copy…[258]

The original warrant authorized the examiner to search for information related to the victim, who was strangled, and her activity related to efforts to sell her home, which may have been related to her murder. In the course of the examination, the examiner recovered the defendant's Internet history files using EnCase, and came upon an Internet history entry indicating that the defendant had visited a website titled "necrobabes.com," which was later determined to be an asphyxiation-type pornographic web site. Once the detective came upon the website in question, he did not conduct any further search unrelated to the search authorized by the first warrant, but waited to proceed until he obtained a second warrant for a search related to asphyxia. Also, in searching for asphyxia-related material under the second warrant, the detective did not abandon the initial search.[259]

In examining these facts, the court found this case to be more like cases where the police, after uncovering material not covered by the warrant, halted the search of such material and obtained a new search warrant. The court cited *Rosa*: "In a search for tangible documents, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be searched . . . a lawful search extends "to the entire area in which the object of the search may be found." [260]

US. v. Long, Rosa v. Commonwealth and *Russo v. State*, are very important to government computer forensics professionals as they specifically apply the capabilities of the EnCase software to these important search-and-seizure rules and concepts. Further, the *Russo* court followed *Rosa*, specifically noting *Rosa*'s EnCase-specific application of the Plain View Doctrine.

United States v. Bhownath[261] is a federal software piracy prosecution brought in United States District Court, Utah. In *Bhownath,* the Federal Bureau of Investigation (FBI) successfully used EnCase to conduct its computer forensics examination. The opinion states: "Agent Hubbert took the imaged copies and reviewed them on a viewing station using EnCase, a computer forensic tool widely used by computer forensic examiners. Agent Hubbert then ran a keyword search, looking for files and folders related to (software piracy)." The search unveiled extensive evidence related to the suspected criminal activity. The EnCase-specific issues in *Bhownath* centered on whether the FBI exceeded the scope of the issued search warrant by virtue of utilizing EnCase's powerful keyword searching capabilities that enabled the investigator to search every file on the seized computer in an automated fashion.

The court denied the defendants' motion to suppress evidence, finding that the evidence identified and recovered by EnCase was done properly and did not exceed the scope of the warrant:

258 Id. at 800.
259 Id. at 790.
260 Id at 805.
261 2007 WL 2570199 (D.Utah,2007).

> "The warrant in this case allowed the agents to search all the data contained on Bhownath's computer. The court disagrees with Bhownath, however, that this is the digital era equivalent of rummaging. The agents must be allowed access to all files on a computer to search for files and folders relating to the case. The agents do so by searching all files for keywords. They then look at the files and folders that contain those keywords. The agents do not conduct a search by opening the first file, reading it, and then moving to the next. Searches of a computer are methodically done on an imaged hard drive. Bhownath's position would unnecessarily curtail the search for keywords in any file on the computer. The agents are not in a position to know what type of file or folder a defendant may use to store relevant information. If the court were to find the warrant facially overbroad, it would allow defendants to hide evidence of illegal conduct in unlikely places on their computer and escape the parameters of a warrant. Such a position is unworkable and unnecessarily limiting in the context of a computer search in a case such as this where a defendant is selling illegal products from a website associated with his home address and shipping products through an address associated with his home address."

The *Bhownath* decision is notable in that it supports the use of EnCase, which the court refers to as standard software "widely used by computer forensics examiners."

§ 7.2 Computer Files and the Plain View Doctrine

The Plain View Doctrine allows for seizure of evidence without a warrant where (1) the officer is in a lawful position to observe the evidence; (2) the object's incriminating nature is immediately apparent; and (3) the officer has a lawful right to access the object itself.[262] In the context of computer investigations, a "plain view" seizure of a computer file would likely only arise where officers lawfully observed a monitor attached to an operating computer displaying material evidencing criminal activity.

However, absent exigent circumstances, clear consent to search the computers themselves, routine border searches[263] or instances of a plain view display of criminal activity on a running monitor, courts have routinely excluded evidence obtained from warrantless searches of computer files.[264] The gray areas typically arise in more common situations where an officer lawfully searching computer files pursuant to a warrant comes upon evidence of criminal activity unrelated to that specified in the warrant. Recent judicial trends indicate that courts are affording special protection to electronic data stored on computers by narrowly construing the articulated terms of the warrant. In order to

262 Horton v. California, 496 U.S. 128, 134, 110 S.Ct. 2301, 2307, 110 L.Ed.2d 112 (1990).

263 United States v. Roberts, 86 F.Supp.2d 678 (S.D.Tex 2000) (Warrantless search by Customs agents of the defendant's computer and zip disks constituted a routine export search, valid under the Fourth Amendment). This holding is specifically limited to border or export searches.

264 United States v. Turner, 169 F.3d 84 (1st Cir. 1999) (Suppressing all evidence obtained from a warrantless search of suspect's computer files), See also, United States v. Barth, 26 F.Supp.2d 929, 935-936 (D.C. Tex. 1998).

understand the Plain View Doctrine in the context of computer files, the related issue of warrant particularity requirements must be understood.

The Fourth Amendment to the United States Constitution requires that all warrants particularly describe the place to be searched and the items to be seized. In order to pass constitutional muster, a warrant (1) must provide sufficiently specific information to guide the officer's judgment in selecting what to seize, and (2) the warrant's breadth must be sufficiently narrow to avoid seizure of purely unrelated items.[265] While it is relatively easy to draft warrants authorizing searches of physical evidence, "computers create a 'virtual' world where data exists 'in effect or essence though not in actual fact or form.'"[266] Ultimately, whether or not computer files containing information not included within the scope of the warrant can be searched often depends upon the specific language of the warrant. Thus, magistrates should ideally strike a careful balance between a warrant that is too overbroad and one that is so narrow as to prevent the search of all items relevant to the investigation.

However, due to a computer's ability to store vast amounts of information, the potential difficulty in accessing particular files in a computer, and the fact that the titles of many files do not satisfactorily indicate the substance of that file, it is often difficult to meet the constraints of the Fourth Amendment.[267]

Courts have generally upheld the search of all files contained within a computer where the warrant authorizes a broad search of computer equipment. In *United States v. Simpson*[268], the court found that where a warrant authorized the broad search of a suspect's computer, an additional warrant was not required for the individual computer files. The court noted that, at the time, there was no known authority providing that computer disks and files were closed containers separate from the computers themselves.[269]

In *United States v. Upham,*[270] the court held that the recovery of deleted files pursuant to a search warrant authorizing the seizure of "any and all computer software and hardware, . . . computer disks, disk drives . . . visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute]" was valid and did not exceed the scope of the warrant.[271] The court noted that, from a legal standpoint, the recovery of deleted files is "no different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note."[272]

In cases involving the investigation of child pornography, many courts have ruled that a warrant allowing seizure of a computer and all its associated printing, storage, and viewing devices is constitutional as the computer, applications, and various storage devices not only may contain

265 United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).
266 U.S. Department of Justice, Federal Guidelines for Searching and Seizing Computers (1994) Note 12, at 89.
267 United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998).
268 152 F.3d 1241 (10th Cir.1998).
269 United States v. Simpson, supra, 153 F.2d at 1248.
270 168 F.3d 532 (1st Cir. 1999).
271 United States v. Upham, supra, 168 F.3d at 535.
272 Id. at 537.

evidence of distribution of child pornography, but are also the instrumentalities of the crime.[273] In *United States v. Lacy,* the court allowed seizure of the suspect's entire computer system, hardware and software, because "the affidavit in this case established probable cause to believe Lacy's entire computer system was likely to evidence criminal activity." [274]

More recently, the Ninth Circuit Court of Appeals gutted its 2009 "Electronic Plain View" decision in *U.S. v. Comprehensive Drug Testing Case*. In a surprising u-turn, electronic search and seizure guidelines designed to protect Fourth Amendment privacy rights during court-authorized computer searches were nullified by the Ninth Circuit Court of Appeals. Instead, the judges urged "greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures."

The original 2009 decision offered detailed guidelines concerning the government's wholesale seizure of thousands of electronically stored information (ESI) relating to an anonymous drug testing program provided for in a collective bargaining agreement between Major League Baseball (MLB) owners and the MLB Players' Association. That decision was widely criticized for its lack of authority for the promulgated guidelines. The court recognized, "the process of segregating electronic data that is sizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." Segregating and redacting ESI to separate potentially relevant from irrelevant evidence is used every day in civil e-discovery and there is no reason why law enforcement cannot use similar protocols and procedures in conducting electronic searches pursuant to a warrant.

EnCase® Enterprise and EnCase® eDiscovery are good examples of technology available to both law enforcement and corporations that can be used to both effectively and economically separate the wheat from the chaff by enabling targeted investigations both on and off the network. Since technology evolves at a much quicker pace than the law, there is currently a wide gap between practice and principle. This court essentially showed a willingness to narrow the gap between forensic practice and legal principle by urging practitioners to use the latest technology and appropriate protocols to target only ESI subject to the search warrant and/or subpoena.

This case illustrates both the challenges faced by modern law enforcement in retrieving necessary information to pursue and prosecute wrongdoers, and the threat to the privacy of innocent parties from a vigorous criminal investigation.

---

273 See Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir.1997) (upholding seizure of computer and all files contained therein because probable cause supported seizure of computer as an instrumentality of the crime); United States v. Kimbrough, 69 F.3d 723, 727 (5th Cir 1995) (upholding warrant allowing seizure of "hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media-floppy disks, CD ROMs, tape systems and hard drive, other computer related operational equipment . . . used to visually depict a minor engaging in sexually explicit conduct"); United States v. Lamb, 945 F. Supp. 441, 457-58 (N.D.N.Y. 1996) (finding e-mail messages discussing the transport of child pornography to have a sufficient nexus to the crime and thus subject to seizure).

274 119 F.3d 742, 745 (9th Cir. 1997).

§ 7.3 United States v. Carey

The case of *United States v. Carey*[275] is a clear example of where narrowly drafted search warrants prevent any expansion of the search of computer media beyond the scope of that prescribed by the warrant. In *Carey*, officers investigating evidence of drug transactions obtained a warrant to search the defendant's computers. The subject warrant limited the search to the specific purpose of only searching defendant's computer files for "names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances."[276] The scope of the search was thus confined to evidence pertaining to drug trafficking.

After conducting a series of unsuccessful text string searches for files related to illegal drug activity, the investigating officer noticed other directories with files that he "was not familiar with," which turned out to be .jpg files.[277] Apparently unable to view the .jpg files with the forensic software utility he was using, the officer exported the files to floppy disks and then viewed them on another computer.[278] Upon opening the first file, the officer determined that it contained an image of child pornography. He then, by his own admission, abandoned the original search for evidence of narcotic transactions and instead searched for and seized evidence related to child pornography.[279] The court ruled the officer's actions exceeded the articulated scope of the warrant and thus violated the Fourth Amendment.

The government unsuccessfully argued that the Plain View Doctrine authorized the search of the child pornography files. The government asserted that "a computer search such as the one undertaken in this case is tantamount to looking for documents in a file cabinet, pursuant to a valid search warrant, and instead finding child pornography." The government further contended that "[j]ust as if officers had seized pornographic photographs from a file cabinet, seizure of the pornographic computer images was permissible because officers had a valid warrant, the pornographic images were in plain view, and the incriminating nature was readily apparent as the photographs depicted children under the age of twelve engaged in sexual acts."[280]

The warrant authorized the officer to search any file, according to the government, because "any file might well have contained information relating to drug crimes and the fact that some files might have appeared to have been graphics files would not necessarily preclude them from containing such information."[281] At oral argument, the government expounded on the filing cabinet theory, arguing that the situation "is similar to an officer having a warrant to search a file cabinet containing many drawers. Although each drawer is labeled, he had to open a drawer to find out whether the label was misleading and the drawer contained the objects of the search."[282]

---

275 172 F.3d 1268 (10th Cir. 1999).
276 United States v. Carey, supra, 172 F.3d at 1272-1273.
277 Id., at 1271.
278 Id.
279 Id.
280 Id. at 1272.
281 Id.
282 Id. at 1274.

The court rejected the government's argument that the files were in plain view, finding that "it (was) the contents of the files and not the files themselves which were seized." The court also noted that the pornographic images "were in closed files and thus not in plain view."[283] By this language, the *Carey* court seems to imply that file folders evidencing criminal conduct outside the scope of the search warrant may be seized, but the actual file contents may not be searched absent a supplemental warrant. The court also rejected the file cabinet analogy, noting that "[t]his is not a case in which ambiguously labeled files were contained in the hard drive directory. It is not a case in which the officers had to open each file drawer before discovering its contents. Even if we employ the file cabinet theory, the testimony of (the officer) makes the analogy inapposite because he stated he knew, or at least had probable cause to know, each drawer was properly labeled and its contents were clearly described in the label."[284] The court further noted that "because this case involves images stored in a computer, the file cabinet analogy may be inadequate. 'Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information.' Relying on analogies to closed containers or file cabinets may lead courts to oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage."[285]

The *Carey* court, seizing the opportunity for discussion in an unsettled area of the law, then proposed in dicta that courts addressing this issue in future "acknowledge computers often contain 'intermingled documents.' Under this approach, law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. The magistrate should then require officers to specify in a warrant which types of files are sought."[286]

In support of its proposal, the court invokes a *Harvard Law Review* notation, which theorizes that, where a warrant "seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records sought. Where relying on the type of computer files fails to narrow the scope of the search sufficiently, the magistrate should review the search methods proposed by the investigating officers."[287] The court further opines that with "the computers and data in their custody, law enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory. In this case, (the officers) did list files on the directory and also performed a key word search, but they did not use

283 Id. at 1273.
284 Id. at 1275.
285 Id. (citations omitted)
286 Id.
287 Id., citing, Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 104 (1994).

the information gained to limit their search to items specified in the warrant, nor did they obtain a new warrant authorizing a search for child pornography."

However, notwithstanding its extensive comments on the topic and its rejection of the filing cabinet analogy advocated by the government, the court ultimately stated that it did not reach its decision on the applicability of the Plain View Doctrine.[288] Instead, the court expressly bases its ruling upon the testimony of the investigating officer who conceded that he intentionally abandoned his search for evidence of drug trafficking and began opening the .jpg files with the intent to search for files containing erotic depictions of minors. Under such circumstances, the court noted, "[w]e cannot say the contents of each of those files were inadvertently discovered."[289] The court indicated throughout the opinion that had the investigating officer obtained a supplemental warrant after viewing the first file containing child pornography, such a supplemental warrant and authorized search would have been proper. The court also implies that had the officer come across the various items of child pornography inadvertently while continuing his search for drug-related information, the Plain View Doctrine would have been applicable. Unlike the majority opinion, concurring opinion is less than subtle on this point, noting that "if the record showed that (the officer) had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, I think a different result would have been required."[290]

§ 7.4 Post-*Carey* Case Law

Several courts have issued published decisions involving the search and seizure of computer media that feature a discussion of *Carey*, while others courts have addressed the Plain View Doctrine in the context of forensic searches of computer files, but without a discussion of *Carey*. These decisions provide some indications as to the impact of the *Carey* decision.

NOTE: Please Refer to section 7.1 above for a detailed discussion of cases addressing EnCase in this specific context.

In *United States v. Gray,*[291] FBI agents executed a search warrant at the home of a suspected computer hacker and seized four computers belonging to defendant, which were taken back to the FBI's offices. The warrant authorized the FBI to search the defendant's computer files for evidence of computer hacking activity, including stolen computer files and utilities enabling unauthorized access to protected computer systems.

After imaging the four computer drives onto magneto-optical disks, the FBI Computer Analysis

288 The court notes: "Although the question of what constitutes 'plain view' in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others, we do not need to reach it here." Carey, 172 F.3d at 1273.

289 Id.

290 Concurring opinion of Judge Baldock, Carey, 172 F.3d at 1277.

291 78 F.Supp.2d 524 (E.D.Va. 1999).

Response Team (CART) agent created a series of CD-ROMs from the disk images to allow the case agents to view the information in readable form. While the information was being copied onto the CD-ROMs, the agent, pursuant to routine CART practice, opened and looked briefly at each of the files contained in the directories and subdirectories being copied to look for the materials listed in the search warrant in the hope that they might facilitate the case agent's search.[292] To accomplish this, the CART agent utilized the CompuPic program to display thumbnail views of the text and graphical image files contained in each directory. In the course of this action, the CART agent came across and opened a subdirectory entitled "Teen" that contained numerous files with ".jpg" extensions.[293] While the agent noted that the files in that subdirectory appeared to contain images of child pornography, he continued his original search pursuant to the warrant.

Thereafter, the agent saw another subdirectory entitled "Tiny Teen," causing the agent to wonder if child pornography resided in that subdirectory.[294] The CART agent testified that he then opened the "Tiny Teen" subdirectory not because he believed it might contain child pornography, which it did, but rather "because it was the next subdirectory listed and he was opening all of the subdirectories as part of his routine search for the items listed in the warrant."[295] Upon determining that the "Tiny Teen" subdirectory did apparently contain child pornography, the CART agent ceased his search and obtained a second warrant authorizing a search of defendant's computer files for child pornography. The search pursuant to the supplemental warrant revealed additional images of child pornography, which, along with the images that triggered the application for the warrant, the defendant moved to suppress.[296]

In upholding the original search and supplemental warrant as lawful, the court noted that:

> Although care must be taken to ensure a computer search is not overbroad, searches of computer records 'are no less constitutional than searches of physical records, where innocuous documents may be scanned to ascertain their relevancy.' It follows, then, that (the agent's) search of the 'Teen' and 'Tiny Teen' subdirectories was not beyond the scope of the search warrant. In searching for the items listed in the warrant, (the CART agent) was entitled to examine all of defendant's files to determine whether they contained items that fell within the scope of the warrant. In the course of doing so, he inadvertently discovered evidence of child pornography, which was clearly incriminating on its face. [297]

The *Gray* court found *United States v. Carey* to be distinguishable, finding that the CART agent never abandoned his original search: "he was not commencing a new search when he opened the 'Teen' and 'Tiny Teen' subdirectories, rather, he was continuing his systematic search . . . without

292 United States v. Gray, supra, 78 F.Supp.2d at 526.
293 Id. at 527.
294 Id.
295 Id.
296 Id. at 528.
297 Id. at 529, citing United States v. Hunter, supra, 13 F.Supp.2d at 584.

regard to file names or suffixes because he was aware that the materials that were the subject of the warrant could be hidden anywhere in defendant's files."[298] The *Gray* court was also not persuaded by the defense's argument that the CART agent knew the "Teen" and "Tiny Teen" subdirectories did not contain documents or other files related to hacker activity when he searched them because many of the files had ".jpg" extensions, indicating a picture file, and none of the materials covered by the warrant were believed to be pictures. In a strong affirmation of standard practice by many examiners, the court noted that the CART agent "would have been remiss not to search files with a '.jpg' suffix simply because such files are generally pictures files," based upon his experience that computer hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories.[299]

In *United States v. Scott,*[300] Secret Service agents conducting a counterfeit securities investigation obtained a warrant authorizing the search of the suspect's residence and seizure of items that constituted "evidence of criminal offenses, the fruits of crime, and the instrumentalities of criminal offenses."[301] Although the initial warrant did not specifically provide for the seizure of the computer files and equipment, the court held the seizure of two computers was proper as the officers had probable cause to believe the computers were being used as an instrumentality of criminal offenses, and thus the officers acted within the scope of the warrant.[302]

In the course of examining the seized computers for information relating to the bank fraud investigation, the investigating agent conducted what the court described as "a 'text string' mirror-image search of the computers' hard drives."[303] The investigating agent used EnCase for this process and his overall computer investigation.[304] The text string search resulted in numerous hits that, in conjunction with other independent information, led the agents to believe that the defendants may have been involved in additional crimes involving bank and tax fraud. On that basis, the agents sought and obtained a supplemental warrant authorizing the search of the computers for evidence of the additional crimes, which the court ultimately found to be supported by adequate probable cause.[305]

In *Wisconsin v. Schroeder,*[306] detectives conducting an investigation of online harassment and disorderly conduct were issued a search warrant to enter defendant Schroeder's residence and seize his computer and related items in order to search for evidence of his having posted the Internet messages. Upon seizing the computer system, Schroeder indicated to the officers that there was child pornography on his computer. The computer was then sent to the state crime lab for analysis, where the officer who served the warrant informed the computer lab examiners that child pornography might

298 United States v. Gray, supra, 78 F.Supp.2d at 530.

299 Id. at 529.

300 83 F.Supp.2d 187 (D.Mass 2000).

301 United States v. Scott, supra, 183 F.Supp.2d at 195.

302 Id. at 196.

303 Id. at 197.

304 Although the opinion does not reflect the type of software utilized, the EnCase Legal Journal confirmed with the investigating agent identified in the opinion that EnCase was used for the investigation. (March 28, 2000 telephone interview of USSS Special Agent Bruce Rittenour).

305 United States v. Scott, supra, 183 F.Supp.2d at 197-198.

306 2000 WL 675942, Wisconsin Supreme Court Decision.

be residing on the computer. In their search for evidence of online harassment, the lab examiners did find some pornographic pictures of children, at which point they stopped their search and sought a second search warrant to provide authority to search for child pornography on Schroeder's computer. Upon being issued the second warrant, the state crime lab examiners resumed the search and found more illicit pictures of minors, as well as evidence of the online harassment.

Schroeder sought to suppress the evidence of child pornography, asserting that the crime lab's initial discovery of the images did not legitimately fall under the Plain View Doctrine exception and thus the supplemental warrant represented "fruit of the poisonous tree." Schroeder contended that when the crime lab analyst first began to search the computer for evidence of harassment, he was also actively looking for child pornography, even though there was no warrant for him to do so. Schroeder noted that, after being told that there might be child pornography on the computer, the crime lab analyst opened files that had names suggestive of child pornography and thus was "verifying" that the files did contain child pornography. According to Schroeder, "This additional step of opening and reviewing the folder to verify it contained child porn makes the search illegal."

The lab analyst testified, however, that when he searches a computer he systematically examines user-created files regardless of their names, in the event that a file has been renamed in order to conceal its contents. While systematically opening all user-created files, the lab analyst opened one containing images that he considered child pornography. At that point, he stopped his search and proceeded to obtain a supplemental warrant. He did not resume his search and find the rest of the contraband until after the issuance of the second search warrant. Thus, his initial discovery of child pornography occurred when he opened a file and saw a nude picture of a child appear on his monitor. Finding that the Plain View Doctrine did apply, the court noted "this was no different than an investigator opening a drawer while searching for drugs and seeing a nude picture of a child on top of a pile of socks."

The *Schroeder* court placed heavy reliance on *United States v. Gray*, and, like the *Gray* court, distinguished *United States v. Carey*. The *Schroeder* court noted, "[i]n *Gray*, as in the present case, the investigator stopped searching and obtained a second warrant. There, as here, the continued search for child pornography was authorized by the second warrant."

The Ninth Circuit has also declined to adopt the *Carey* reasoning. In *United States v. Rossby* [307], the defendant had given his consent to a "complete search" of his office.[308] While conducting a "complete search," the police included defendant's computers in the search. The Ninth Circuit stated that "[t]he district court did not clearly err in holding that [the defendant's] consent to search his office reasonably included consent to examine the contents of his laptop computers.[309] The Ninth Circuit was not persuaded by the defendant's reliance on *Carey* and noted that "even in the Tenth Circuit, *Carey* has been limited to its facts."[310]

In *United States v. Balon*[311], the Second Circuit addressed the technological problem caused by the

307 81 Fed. Appx. 109 (9th Cir. 2003).
308 Id. at 110.
309 Id.
310 Id.
311 384 F.3d 38, 41 (2nd Cir. 2004).

Carey analysis. The defendant argued that the supervised release condition authorizing the monitoring of "all data" on his computer was overbroad and that the probation officer should be limited to reviewing "only those actions or files that might indicate introduction of child pornography onto the computer."[312] The three-judge panel of the Second Circuit took a dim view of this line of reasoning:

> [I]f a computer user loads contraband data onto a computer, it would seem easy to label the files containing the data in innocuous ways, say, by disguising the file as a "word" or "excel" document and changing its filename to "communication to attorney" or "tax return info." To insulate the file from examination, the user need only change the letters at the end of the filename. It appears, therefore, that unless the probation officer is allowed to search these documents, a user could store huge amounts of illicit data on the computer without anyone being allowed to view it."[313]

One court that followed the *Carey* decision was a trial court in New York State in the case of *People v. Carratu*.[314] The defendant in *Carratu* was the focus of an investigation into criminal possession of illegal cable television access devices. The warrants in the case authorized searches for "devices capable of defeating the security and encryption system of a cable television operator… records relating to the purchase, sale, and transportation of such devices… as well as computers and computer diskettes used in connection with the illegal activity."[315] The court described the forensic examination as follows:

> The initial procedure was to make a copy of the hard drive for each of the systems. . . . Then the directory for each of the hard drives was displayed, and the folders for each hard drive were listed alphabetically. Finally, the detective opened each folder and examined each user-generated file to determine whether it contained evidence pertaining to the illegal cable box operation. . . . In a folder labeled "Fake I.D." on the Sony hard drive, the detective observed image files of driver's licenses, social security cards, inspection stickers, and registration certificates.[316]

The *Carratu* court closely followed the reasoning of *Carey*. The *Carratu* court held that folders that are "ambiguously labeled" may be opened by an investigator searching for evidence of a specific crime.[317] However, with respect to folders that are not "ambiguously labeled," the court reached a different conclusion:

> The court notes that the "Fake I.D." folder was not ambiguously labeled. To the contrary, the name of the folder clearly indicated that it likely contained false identification

312 Id.
313 Id. at 48.
314 194 Misc.2d 595, 755 N.Y.S.2d 800 (2003).
315 194 Misc.2d at 599, 755 N.Y.S.2d at 804.
316 194 Misc.2d at 602, 755 N.Y.S.2d at 806.
317 194 Misc.2d at 605, 755 N.Y.S.2d at 808.

> documents rather than documents or records concerning the sale of illegal cable boxes. . . . Thus, from mere inspection of the folder name [the detective] had probable cause to seek a further warrant authorizing a search of the Sony computer for evidence of possession of forged instruments. And, since the file extension names on the files within the Fake I.D. folder indicated that they likely contained images, they appeared not to contain the type of text files which were akin to the items sought by the warrant.[318]

In suppressing the evidence of false identification documents, the *Carratu* court did not even consider the ease with which files could be purposefully named anything at all, or that file extensions can be easily changed. Under the reasoning of the *Carratu* court, all a criminal would have to do to hide text documents is to name his folders something innocuous like "Family Photos" and change the file extensions to .gif or .jpg, and the evidence would be suppressible.

In *Frasier v. State*,[319] an appellate court in Indiana again distinguished *Carey*. In *Frasier*, the affidavit in support of a search warrant application set forth evidence related to marijuana possession and child pornography.[320] Based upon the affidavit, the judge issued a search warrant that directed the police to enter the defendant's home and search for marijuana-related materials and equipment; the judge specifically struck out from the draft affidavit the words "pornographic images depicting persons believed to be children."

When the police executed the warrant, a detective noticed an icon labeled "Smoke" on the desktop of a personal computer located in a bedroom. The detective opened the file, and noticed that it contained drug-related materials. The detective then began opening documents listed in the "Documents" menu of the computer's "Start" menu. The first document opened contained an image the detective believed to be child pornography. The detective opened a few other files, which also appeared to contain child pornography. A warrant was then sought and obtained to search for evidence of child pornography on the computer.

In addressing the defendant's objection to the introduction of the evidence of child pornography, the *Frasier* court held that the Plain View Doctrine applied, and it specifically discussed *Carey* in great detail:

> The situation in *Carey* was similar to the one before us: the police had a warrant to search the defendant's computer for documentary evidence pertaining to the sale and distribution of controlled substances.
>
> * * *
>
> [The *Carey* court stated that] "the question of what constitutes 'plain view' in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others, *we do not need to reach it here.*" . . . [T]he essential

318 194 Misc.2d at 605, 755 N.Y.S.2d at 808.

319 794 N.E.2d 449 (Ind. App. 2003).

320 794 N.E.2d 449, 452-54.

> holding of the *Carey* court was that the plain view exception was inapplicable because the officer expected to find the files. . . [A]ccording to the *Carey* court, the fact that the document was closed cannot be the touchstone of whether the plain view doctrine is applicable; rather, it is whether the discovery was inadvertent.
>
> * * *
>
> We have our own concerns with the approach . . . suggested by the *Carey* court, which implies that the police must rely upon the label given to a file to determine its contents. A computer image file is not exactly the same as a physical photograph. . . . The image file must be "opened," i.e., read and interpreted by some program in order to render its contents into a humanly perceptible form, i.e., an image on the computer monitor. In this sense, a computer image file is akin to a photograph sealed in an envelope or folder. And the name given to the file is like a label stuck onto the envelope or folder. Although such a label might say "Tax Records," the photograph inside could be of a nude child. Likewise, a computer image file containing child pornography could easily be named "tax_records.xls," in an attempt to hide its actual contents. . . . An officer searching for one type of record on a computer should not be forced to rely upon the name given to a file, which might very well hide its actual contents. In order to find out what is contained in the file, it must necessarily be "opened" in some way to ascertain its contents.

In *People v. Pacifico B.*[321], an unpublished California decision, the court distinguished *Carey*. In the *Pacifico B.* case, the warrant authorized a search for photographs of the victim. The computer forensics investigator "was informed of the scope of the warrant, and was given a photograph of [the victim] so that he could recognize her. [He] opened all of the files on the hard drives, including files with the extension 'JPG' . . . [He] did not encounter any photographs of [the victim] but did see photographs of other children that were pornographic in nature. . . No supplemental warrant was acquired."[322] The defense, relying on *Carey* and *United States v. Turner* (cited above in Section 7.1) sought to have the defendant's conviction reversed. The *Pacifico B.* court rejected the defense's arguments, and noted that:

> "[T]he warrant in this case specified that a search be conducted for images of the victim. [The investigator] was thus acting within the scope of the warrant in opening the JPG files on defendant's hard drives to look for such images. And having properly opened those files pursuant to the warrant, the child pornography images [the investigator] ultimately encountered were appropriately characterized as being in plain view.[323]

321 2004 WL 1427013 (Cal. Ct. of Appeal, June 25, 2004).
322 Id. at 5.
323 Id. at 6.

Although the *Pacifico B.* case does not carry precedential value, those drafting search warrants may want to keep the court's reasoning in mind.

United States v. Hill[324] is a case from federal district court in California that does not specifically refer to *Carey*, but that clearly rejects the reasoning of the *Carey* court. The government expert in *Hill* conducted "a comprehensive computer analysis using 'EnCase' forensic software," and discovered over 1,000 images of child pornography on two zip disks.[325] The defendant argued that the search warrant relied upon was overbroad "because it placed no limitations on the forensic examination of the [zip] disks that were seized."[326] The court refused to limit the investigator's search of computer files:

> Defendant also argues that the warrant was overbroad because it did not define a "search methodology." He claims that the search should have been limited to certain files that are more likely to be associated with child pornography, such as those with a ".jpg" suffix (which usually identifies files containing images) or those containing the word "sex" or other key words.
>
> Defendant's proposed search methodology is unreasonable. "Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent." *United States v. Hunter,* 13 F.Supp.2d 574, 583 (D.Vt.1998). Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.
>
> Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled "flour" or "talcum powder." There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it. The ease with which child pornography images can be disguised--whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated--forecloses defendant's proposed search methodology.[327]

In *United States v. Maali*,[328] defendants filed a motion to suppress evidence seized pursuant to a federal investigation into their employment and harboring of aliens and tax evasion. One objection lodged by defendants was that the government should have included a computer search strategy in its affidavit to obtain the warrant as recommended in a Department of Justice computer search manual.

---

324 322 F.Supp.2d 1081 (C.D. Cal. 2004).

325 Id. at 1091.

326 Id. at 1084.

327 Id. at 1090-91.

328 United States v. Maali, 346 F. Supp. 2d 1226 (M.D. Fla., 2004).

The court held: "The better practice would have been to follow the DOJ guidelines in developing a search strategy and presenting that strategy to the magistrate judge, and the failure to do so is troubling. However, the lack of a detailed offsite search strategy does not render the warrants [sp] computer search provisions insufficiently particular, and the computer search provisions otherwise satisfy the Fourth Amendment."[329]

Defendants also challenged the manner in which the computer hard drives were seized and copied. "The seized computer hard drives were copied or "mirrored" and the hard drives were returned to the defendants approximately one week after the searches."[330] Citing *United States v. Hill*, the court held the seizure of hard-drives permissible because the affidavit supporting the warrant explained the necessity of an off-site search of the hard drives. "[S]ome aspects of a computer search necessarily require a controlled environment and special techniques."[331]

As for the manner in which the hard drives were searched, the FBI computer analyst in the case compiled all "data records" from the eighty-three computer hard drives onto a master hard drive, "culling down" the search by eliminating all "program files." Defendants argued that this "culling down" was insufficiently particular and the agent should have limited the search to specific data files. The court disagreed, holding "the computer search has not been shown to be constitutionally infirm. . . it has been recognized that seizure of superfluous computer files is virtually inevitable."[332]

Additionally, defendants argued that investigators should have retained records of the text string searches that they ran. Disagreeing, the Court held: "[a]s to the failure of the searchers to keep records of the text string searches that they ran, while the maintenance of a search log seems feasible and not terribly burdensome to the searchers, the lack of such a record does not in and of itself render the search unconstitutional, at least in the face of testimony from the agents that the text string searches that were run pertained to the issues and entities described in the warrant."[333]

In *State v. Bolsinger*,[334] an appellate case from Iowa, the defendant argued that the search of his computer hard drive went beyond the scope of the warrant. The trial court had rejected this argument, stating:

> The actual search of the computer was not overbroad. There was testimony by the officer that did the search that he uses a special software system that enables him to do keyword searches of the entire system. That software then pulls up all fields that have hits of that keyword in them and allows the officer to view a small section of the file. Several words before and after the keyword come up to allow the officer to see the context in which the word is being used. From there the officer is able to make a determination whether to open the file or not. In addition to seeing the context of the word, the software tells him what type of computer file it is in. This too gives him

329 Id. at 1247.
330 Id. at 1236.
331 Id. at 1264.
332 Id. at 1265.
333 Id.
334 State v. Bolsinger, 2005 WL 756767 (Iowa App. Mar. 31, 2005).

> information in order to determine whether that file is within the bounds of the search warrant. The officer did not look at everything on the hard drive. Rather, the search was narrow in focus due to the utilization of the software system and professional judgment of the officer after viewing the word or words in context.[335]

Due in part to the "comprehensive safeguards taken by the police to limit their search of Bolsinger's computer to the items specified in the warrant," the Court of Appeals of Iowa affirmed the trial court.[336]

The Tenth Circuit itself has narrowly interpreted *Carey*, or sought to avoid its application, on at least two occasions. First, in *United States v. Riccardi*,[337] the defendant argued that the warrant that had authorized the search of his computer did not comply with the particularity requirement of *Carey*. Indeed, the warrant was remarkably vague: it authorized the "seizure" of Riccardi's computer and the search of "all electronic and magnetic media stored within such devices."[338] When the investigating officer conducted his forensic examination of the computer using EnCase software, he found thumbnail images of child pornography.[339] Apparently aware of Tenth Circuit precedent, however, the officer then suspended the search in order to review the search warrant language. After a prosecutor assured the officer's supervisor that the child pornography found on the computer would be covered by the warrant, the officer continued the search. The court held that because the "warrant in this case was not limited to any particular files, or to any particular federal crime," it lacked the specificity required by *Carey* and its progeny.[340] However, the court found that the good-faith exception applied:

> Even if the court finds the warrant to be facially invalid – as was the case here – it "must also review the text of the warrant and the circumstances of the search to ascertain whether the agents might have reasonably presumed it to be valid."
>
> The officers remained within the terms of the warrant as well as the affidavit, and did not conduct a "fishing expedition" beyond the scope of the authorized investigation. They did not search for, or seize, any materials for which probable cause had not been shown. By consulting the prosecutor, they showed their good faith in compliance with constitutional requirements. Nor do we think the defect in the warrant was so flagrant or obvious that "the executing officers [could] not reasonably presume it to be valid."[341]

As a result, the court upheld the defendant's conviction.

---

335 Id. at 6.

336 Id.

337 United States v. Riccardi, 405 F.3d 852 (10th Cir. April 19, 2005).

338 Id. at 858.

339 Id. The use of EnCase software was confirmed by Special Agent David Finch in a telephone conversation with Gregg Smolar of Guidance Software, Inc. on June 15, 2005.

340 Id. at 862-63.

341 Id. at 863-64.

In another Tenth Circuit case, *United States v. Brooks*,[342] an FBI agent had conducted a search of the defendant's computer at the defendant's house and with the defendant's consent. Upon locating several contraband images, the agent shut down the computer and seized it, and subsequently obtained a warrant authorizing a forensic search of the defendant's three computers and other media; this search was conducted at a police laboratory.[343] The defendant moved to suppress the evidence discovered during the forensic search, arguing that the warrant for the search was not specific enough, in that it did not describe a specific search methodology. The court disagreed, reasoning as follows:

> At the outset, we disagree with Brooks that the government was required to describe its specific search methodology. This court has never required warrants to contain a particularized computer search strategy. We have simply held that officers must describe with particularity the *objects of their search*. . . .
>
> The question of whether the nature of computer forensic searches lends itself to predetermined search protocols is a difficult one. Given the numerous ways information is stored on a computer, openly and sureptiously [sp], a search can be as much an art as a science. . . . [C]ourts will look to (1) the object of the search, (2) the types of files that may reasonably contain these objects, and (3) whether officers actually expand the scope of the search upon locating evidence of a different crime.[344]

The court went on to explain that *Carey* does not "stand for the proposition that a warrant is per se overbroad if it does not describe a specific search methodology."[345]

The defendant also made a second argument concerning the warrant, arguing that it was overbroad because its language (authorizing a search of the computers "for evidence of child pornography," and then identifying the things to be searched as including "correspondence, including printed or handwritten letters, electronic text files, emails and instant messages") did not explicitly instruct the officers to look solely for those text files containing child pornography.[346] The court rejected the argument, noting that "although the language of the warrant may, on first glance, authorize a broad, unchanneled search through Brooks' document files, as a whole, its language more naturally instructs officers to search those files only for evidence *related to child pornography*."[347]

In a federal case from the Eastern District of Wisconsin called *United States v. Calimlim*, the warrant, perhaps written with *Carey* in mind, specified detailed search methodologies to be used on any computers seized, including "[s]canning storage areas for deliberately hidden files [and] performing key word searches in electronic storage areas to determine whether occurrence of language

342 United States v. Brooks, 2005 WL 2767185 (10th Cir. Oct. 26, 2005).
343 Id. at 2.
344 Id. at 5 [Internal citations omitted; emphasis in original].
345 Id.
346 Id. at 6.
347 Id. [Emphasis in original].

contained in such storage areas exist that pertain to the subject matter of the investigation."[348] The court noted that one agent used EnCase software (and another forensic tool) and the other "utilized EnCase software to perform key word searches of the data in each computer."[349] The Magistrate Judge agreed that the keywords used by the agents demonstrated a reasonable effort to limit the search to items identified in the warrant.[350]

§ 7.5 Post-*Carey* Practice

In synopsis, *Carey* provides that an investigator may not manually search through individual files in a concerted effort to obtain information outside a warrant's articulated scope. While not addressing *Carey*, the *United States v. Scott* decision provides an indication that text string searches performed across an entire hard drive or other form of media would not subject the examiner to questions of exceeding the scope of a warrant, as long as such text searches were generally within the course of the investigation delineated by the warrant. The *Calimlim* case reached a similar result.

By logical extension, results from aggregate hash file analysis, signature mismatch analysis and other automated functions featured in EnCase software would provide a means for investigators to justifiably seek supplemental warrants to broaden searches for evidence of additional criminal activity. At the same time, investigators employing such practices would arguably be better insulated from charges that they conducted an unauthorized review of individual files to obtain probable cause for the supplemental warrant.

EnCase software features several automated features, such as the categorization of the hash value of each file in a case, which can help identify suspect files. EnCase software also features a capability providing for an unlimited number of executable macros and filters, and an automated picture gallery displaying all known graphical images in a case. As these functions will presumably be enacted as a routine practice in the course of computer investigations, supplemental warrants based upon information obtained from the aggregate outputs of these automated processes would be within the scope of the Fourth Amendment. See *United States v. Gray,*[351] (software providing thumbnail views of all files in a directory properly utilized as standard FBI CART practice).

The *Carey* court proposed that in future investigations, computer examiners should be required to "engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents." The court noted that law enforcement computer investigators "can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of

348 United States v. Calimlim, 2005 WL 2922193 at 17 (E.D.Wis. Nov. 4, 2005).

349 Id. at n. 4.

350 Id. at 17.

351 Supra, 78 F.Supp.2d at 526.

each file stored in the memory." If the courts were to adopt such a "file sorting" requirement, EnCase software provides an excellent mechanism to comply with various computer file-sorting instructions from a magistrate.

Though *Carey* has not been overruled, the post-*Carey* case law (including *Frasier* and *Hill*) reveals that most judges are becoming more nuanced in their understanding of how computer evidence can be stored and how to best search for it while respecting legitimate privacy interests. Furthermore, there are many cases that distinguish the *Carey* holding, and the Tenth Circuit itself has narrowly construed it. Others cases such as *Hill* have rejected its reasoning while not mentioning it by name.

An example of a post-*Carey* decision is *United States v. Farlow*.[352] While searching defendant's computer for a non-pornographic image of a bodybuilder that was sent to a detective posing as a minor, a police officer executing a warrant discovered images of child pornography on defendant's computer using EnCase. Based on the images retrieved by EnCase, the officer obtained a search warrant authorizing a search for images of child pornography. Defendant argued that the officer should have limited his initial search to the bodybuilder image. Defendant did not offer any evidence contradicting the officer's declarations that the only reasonable way to locate most copies of an image was to use a visual search, that tracking the hash mark of the bodybuilder image would not have located the bodybuilder image, and that the officer's search method was the narrowest search reasonably likely to obtain the bodybuilder image. Defendant was unable to cross-examine the examining officer but nevertheless attempted to claim the nature of EnCase program and its ability to find images matching a particular hash would have prevented the officer from finding the child pornography. The court rejected the defendant's assertions under the plain view doctrine.

Another example is *State v. Bizewski*,[353] where the court determined that photos containing child pornography found on a suspect's laptop were admissible under the plain view doctrine where the investigating officer found the images while using Gallery View in EnCase. Citing to the difficult nature of locating image files with SHA value, the opined that using the Gallery View was within the scope of the search warrant and the officer had probable cause to do so.

Certainly investigators located in the Tenth Circuit should be aware of the *Carey* holding and conform their actions to it, and investigators in New York State should be cognizant of the *Carratu* case (although *Carratu* is not binding precedent). At this point, the courts are moving away from the *Carey* holding and recognizing that search warrants exercised to discover computer-based evidence should proceed in light of the realities of the virtual world rather than the realities of the physical world.

§ 7.6 Business Disruption Caused by the Seizure of Computers

One of the problems with seizing computers in the field for later forensic analysis is the extensive disruption caused to the party from whom the computers are seized, which can be particularly acute in the case of a business. In many instances, the computers from which evidence is gathered belong

352 2009 U.S. Dist. LEXIS 112623 (D. Me. 2009).

353 2013 Conn. Super. LEXIS 809 (Sup. Ct. Conn. 2013).

to a third party that has not been charged with a crime. [*See, e.g.*, *State (Ohio) v. Morris*, discussed above in Chapter 6, in which law enforcement returned the original hard drive, which "belonged to a non-party . . . who used the computer in his business."][354] In these situations, law enforcement needs to be able to acquire the data in the field, so as not to unnecessarily burden innocent parties. In *Airtrans, Inc. v. Mead*,[355], the Sixth Circuit Court of Appeals addressed a claim by plaintiff that "[d]uring execution of the warrant, the agents seized records and disabled company computers, leaving AirTrans effectively unable to operate. . . After the search, AirTrans filed a § 1983 action against the defendants seeking compensation for its business losses."[356] In that case, AirTrans was the target of a criminal investigation, and the Court of Appeals found that there was no constitutional violation.

Nevertheless, it would have been far easier for the government to collect the computer data on site, thereby obviating any claim of harm by plaintiff. As in the *Morris* and *Maali* cases (discussed above in Section 7.3), the forensic image could readily serve the government's investigative purposes. The case of *State v. Kaminski*[357] represents a common misperception among law enforcement personnel and judges concerning the investigation of a computer system. In applying for a warrant to search the defendant's residence, the affiants stated to the court "that to retrieve data from a computer system it is necessary for the entire system to be seized and submitted to a computer specialist for examination and analysis in a laboratory setting."[358] With modern technology, this is no longer necessary.

354 State v. Morris, 2005 WL 356801 (Ohio App. 9 Dist. Feb. 16, 2005).

355 Airtrans, Inc. v. Mead, 389 F.3d 594 (6th Cir. 2004).

356 Id. at 596-97.

357 State v. Kaminski, 2005 WL 1155112 (Conn.Super., Apr. 25, 2005).

358 Id.

8. Complying with Discovery Requirements in Criminal Cases When Utilizing the EnCase Process

§ 8.0 Overview

One of the questions prosecutors and examiners routinely face in the field is how to comply with discovery requirements when the prosecution's computer evidence is contained within an EnCase image. This is a somewhat difficult issue because of the nature of computer evidence. Printing out the data contained on a 10-gigabyte hard drive would result in a stack of paper approximately 300 meters tall. Even worse, this data will be compromised unless properly handled with computer forensic software because the act of printing can change the contents of the hard drive. The question then becomes, what is required to produce relevant and sound computer evidence in the course of discovery?

There are several models for producing electronic evidence in the course of discovery that are employed by prosecutors and attorneys. Each has its own strengths and weaknesses, and the applicable statutes and discovery rules of the particular jurisdiction and preferences and discretion of the individual judge often determine which of the following models are most suitable.

§ 8.1 Production of Entire EnCase Images

Many attorneys choose to produce exact copies of the EnCase Evidence File, which is a complete physical image of an acquired drive. Often the prosecution will also produce the Case File, which contains the bookmarks, text-string searches, various notes and comments of the investigator, as well as other information. As much of the data contained within the Case File, such as the examiner's bookmarks and notations, could be considered work product, it is within the discretion of the prosecutor to produce such evidence.

Many prosecutors in the US inform the defense that it should retain an expert who is familiar with EnCase software. As EnCase software and computer forensics have become standard, experts in the private sector, as well as federal and state public defenders' offices, increasingly use EnCase software. As such, producing an exact copy of the EnCase Evidence File is becoming more feasible as the practice of computer forensics expands.

The advantage of this approach is that it ensures the defense cannot tamper with the evidence--at least without detection--and weakens any claim that the prosecution withheld evidence. For these reasons, this method of discovery is the most desirable. The disadvantage of this approach is that many defendants and their counsel still lack the expertise or means to purchase and utilize the EnCase software, although as noted above, this is less and less frequently the case.

§ 8.2 Production of Restored Drives

Another option is to provide a restored hard drive, which is a complete bootable clone of the original seized drive. EnCase software includes a feature that allows the examiner to easily restore an EnCase image to a separate drive. EnCase software will restore the seized drive onto a separate drive and verify the copy by a 128-bit, MD5 hash, which will match that of the original evidence, even if different sized media is utilized in the process. After receiving the discovery, the defense's retained expert can examine the evidence.

The advantage of this approach is that it provides the entirety of the evidence in a manner that is widely and readily accessible. However, the disadvantage of this approach is that deleted, temporary and buffer files, as well as key metadata, are not viewable by simply booting the cloned drive. Also, once the defense boots the cloned drive, much of the evidence would change, including date stamps and writes to the swap file.

As a result, the defense may attempt to introduce--not necessarily intentionally--evidence that is not an accurate reflection of the data originally seized. Of course, with the MD5 hash of the restored drive recorded, the prosecution would be able to detect any such changes made by the defense, so this drawback is mitigated by the technology itself.

§ 8.3 Production of Exported Files

Some prosecutors provide selected exported files and other information from the Evidence File, along with printouts of that information. Production of these files and blocks of selected data is achieved by transferring the information to a CD-ROM disk in a format that is easily viewable by counsel. The EnCase Report may also be produced. This option provides the exact information that the prosecution intends to introduce at trial in a convenient and easy to read format.

By providing the electronic evidence on CD-ROM disks, the defense cannot tamper with the selected portions of the original evidence. Disadvantages of this process include potential claims that the production was too narrow and that potentially exculpatory documents were omitted. Many courts tend to prefer that document productions be comprehensive, as opposed to more limited productions that may not contain all relevant data.

§ 8.4 Supervised Examination

Where the defense has retained an expert, another option is to permit the defense expert to access, under the supervision of the investigating officer and/or a special master, an image of the original drives so that the expert can conduct a proper and non-invasive investigation. Ideally, the expert would utilize EnCase software to conduct the exam, but may be permitted access to the original drives or a properly restored clone for re-imaging with other non-invasive tools.

Section 4.4 summarizes a New Hampshire Federal District Court case where the prosecution offered to allow the defense supervised access to a copy of the EnCase Evidence File, which contained images of child pornography. However, the defense contended that it required access to the original

computer systems in question so that they could operate those computers and examine them in their native environment, and filed a formal written request for a court order allowing such unfettered access to the "original" computer evidence. The government filed a successful objection to the request, asserting that the "mirror image" created by the special agent is the proper way to preserve the original evidence. The government asserted that merely turning on the computer, as the defense requested, will change the state of the evidence by altering critical date stamps and potentially overwriting existing files and information.

The court ruled that the defense could only have access to the original computer systems if their expert created a proper forensic image under the supervision of the special agent. The defense was barred from booting the original computer systems to their native operating systems.

§ 8.5 Production of EnCase Evidence Files to Defense Experts

A number of courts have required that the prosecution provide copies of EnCase evidence files to the defense. This approach is highly controversial in cases in which the computer evidence consists of contraband, such as child pornography, and in such cases the prosecution typically argues for the type of supervised examination described above in Section 8.4.

United States v. Hill,[359] a case from federal district court in California (described above in Chapter 7), is illustrative. In that case, the court held that the government had to provide copies of the EnCase evidence files to the defense, reasoning as follows:

> The government intends to introduce into evidence "over 1,000 images of child pornography and/or child erotica," which it discovered on two 100 megabyte zip diskettes taken from defendant's home. The government's expert discovered the images through a comprehensive forensic computer analysis using "Encase" forensic software. Defendant wishes to obtain two "mirror image" copies of the computer media analyzed by the government's expert to allow his own expert to conduct a forensic analysis and his counsel to prepare his defense. The government opposes producing these items, offering instead to permit the defense to view the media in an FBI office and to conduct its analysis in the government's lab.
>
> * * * * *
>
> The court concludes that defendant will be seriously prejudiced if his expert and counsel do not have copies of the materials. Defense counsel has represented that he will have to conduct an in-depth analysis of the storage media in order to explore whether and when the various images were viewed, how and when the images were downloaded and other issues relevant to both guilt and sentencing. The court is persuaded that counsel cannot be expected to provide defendant with competent

359 322 F.Supp.2d 1081 (C.D. Cal. 2004).

representation unless counsel and his expert have ready access to the materials that will be the heart of the government's case.

The government's proposed alternative--permitting the defense expert to analyze the media in the government's lab at scheduled times, in the presence of a government agent--is inadequate. The defense expert needs to use his own tools in his own lab. And, he cannot be expected to complete his entire forensic analysis in one visit to the FBI lab. It took defense counsel between two and three hours to quickly scroll through the 2,300 images in the Encase report, so it is likely to take the expert much longer than that to conduct a thorough analysis. Defendant's expert is located in another state, and requiring him to travel repeatedly between his office and the government's lab--and obtain permission each time he does so--is unreasonably burdensome. Moreover, not only does defendant's expert need to view the images, his lawyer also needs repeated access to the evidence in preparing for trial.

There is no indication that defendant's counsel or expert cannot be trusted with the material. The expert is a former government agent who has a safe in his office and has undertaken to abide by any conditions the court places on his possession of the materials. He has experience in dealing with child pornography and takes precautions to ensure that contamination doesn't occur, including using the Encase software and fully "wiping" the forensic computers on which he examines the images. Defense counsel is a respected member of the bar of this court and that of the Ninth Circuit. The court has every confidence that he can be trusted with access to these materials.[360]

The reasoning of the *Hill* court was explicitly followed in *United States v. Frabizio*,[361] in which the defendant "moved for production of an image of the hard drive, as well as all 'Encase' files."[362] The government refused to produce any images it believed to be child pornography, but it did make those images available for inspection at an FBI facility. The court rejected the government's approach; instead it adopted the same approach used by the *Hill* court, and noted that "there is no reason to think that defense counsel or her expert cannot be trusted to abide by the proposed protective order. It cannot be said—at least credibly—that the only defense counsel and experts to be trusted are those who were formerly employed by the government."[363]

In an unpublished opinion in *State of Minnesota v. Kandel*, a Minnesota appellate court affirmed the dismissal of a case because the prosecution had refused to turn over a forensic image of the defendant's hard drive, which the prosecution asserted contained child pornography.[364] Defense counsel had specifically requested a "forensically sound Image Copy of the hard-drive of the computer

360 Id. at 1091, 1092-93.
361 2004 WL 2397346 (D. Mass. Oct. 27, 2004).
362 Id. at 1.
363 Id. at 3.
364 State of Minnesota v. Kandel, 2004 WL 1774781 (Minn.App. Aug. 10, 2004).

containing the alleged pornographic images, and all digital storage media including but not limited to Zip Discs, Jaz Discs, CD Rom, Tapes, Floppy Discs and any other storage media."[365] The prosecution "asserted its ongoing refusal to allow respondent to access the allegedly pornographic images, arguing that [among other things] federal law prohibits the dissemination of the images, even to defense counsel or respondent's expert."[366] The trial court dismissed the case because of the prosecution's recalcitrance, a decision that was upheld by the appellate court.

United States v. Alexander[367] is another case in which the court ordered the production of a duplicate forensic image of a hard drive containing contraband to a defense expert. The court dismissed the prosecution's concern regarding further dissemination of contraband, relying "on the efficacy of its orders to protect the public from further disclosure of the images."[368]

In the consolidation of two Tennessee child pornography prosecutions, *State v. Butler*,[369] "[c]ounsel for both defendants filed motions for discovery, including requests that the state provide them with copies of the computer hard drives and 'other computer materials' for their independent examination and review. The state refused, offering to make the material available for examination by defense counsel and defense computer experts at the sheriff's department, but contending that it would constitute a violation of the sexual exploitation statute for the material to be removed from the custody and control of the sheriff's department."[370]

The Court of Criminal Appeals of Tennessee held that the State was required to provide the defense with copies of the alleged pornographic materials, and that "so long as it occurs in the context of the prosecution or defense under the statute," dissemination would not constitute a violation.[371] At the trial court, one of the defendants had argued that the state should be required to turn over the original hard drive, rather than a forensic image of the hard drive, alleging that "computer programs in existence did not create true mirror images."[372] The trial court rejected this argument, "requiring the State to provide Allen's counsel with a mirror image copy of the computer hard drive rather than the actual hard drive itself."[373]

§ 8.6 Discovery Referee in Civil Litigation Matters

Chapter 9 includes a discussion of a well-designed protocol proscribed by a Federal District Court for the discovery by computer forensic experts of electronic evidence contained on opponents' hard drives. In *Simon Property Group v. mySimon, Inc.*,[374] the court issued an order appointing a computer forensics expert as an Officer of the court, enabling the expert to conduct the exam under court

365 Id. at 1.
366 Id. at 2.
367 2004 WL 2095701 (E.D. Mich. Sept. 14, 2004)
368 Id. at 10.
369 State v. Butler, 2005 WL 735080 (Tenn.Crim.App. Mar 30, 2005).
370 Id. at 1.
371 Id. at 11.
372 Id. at 2.
373 Id. at 3.
374 194 F.R.D. 639 (S.D. Ind. 2000).

supervision as a neutral special master. By serving in such capacity, any attorney-client or other privileges would remain intact during the course of the neutral experts' examination, with the producing party afforded full opportunity to lodge objections to the production of evidence identified during the course of the examination. This particular special master model may be appropriate in some criminal cases as well, particularly those involving seizure of computers from law firms or other businesses with sensitive material.

§ 8.7 Federal Rules of Civil Procedure's Electronically Stored Information Amendments in a Criminal Context

In some cases, the court must engage in a lengthier discovery process than that typically associated with a criminal prosecution. Unfortunately, criminal procedure is yet to develop rules accounting for voluminous amounts of electronically stored information (ESI). Thus one court, in *United States v. O'Keefe*[375], adopted the then recently enacted amendments to the Federal Rules of Civil Procedure (FRCP) for use in the criminal context.

In *O'Keefe*, the government charged the defendant with taking bribes to expedite visa applications for employees of a co-defendant's company, and the defense took the position that the visa applications processed by the defendant were no more expedited than a normally expedited visa application, where bribes were not given. To prove this argument, the defense requested the government produce various documents, many of which were stored electronically, relating to the expedited visa process at various American consulates throughout Canada and Mexico. However, the government's production fell short of the information the defendant sought, and thus Magistrate Judge John M. Facciola was called upon to decide a discovery dispute not unlike many seen in the civil arena.

In *O'Keefe*, the parties disagreed over many issues typical to a civil discovery dispute involving ESI: form of production, relevance, scope of the production, search terms used, and storage of electronic information. Judge Facciola called on the FRCP to decide the proper course of action: "In criminal cases, there is unfortunately no rule to which the courts can look for guidance in determining whether the production of documents by the government has been in a form or format that is appropriate. This may be because the 'big paper' case is the exception rather than the rule in criminal cases. Notwithstanding the fact, Rule 34 of the Federal Rules of Civil Procedure speak[s] specifically to the form of production. The Federal Rules of Civil Procedure in their present form are the product of nearly seventy years of use and have been consistently amended by advisory committees consisting of judges, practitioners, and distinguished academics to meet perceived deficiencies. It is foolish to disregard them merely because this is a criminal case, particularly where, as is the case here, it is far better to use these rules than to reinvent the wheel when the production of documents in criminal and civil cases raises the same problem."[376] This is a significant decision because it provides guidance to the more than 4,000 Department of Justice federal prosecutors, and defense counsel, on how a court might handle ESI in the criminal area."

375 537 F. Supp. 2d 14 (D.D.C. 2008)

376 United States v. O'Keefe, 537 F. Supp. 2d 14, 18-19 (D.D.C. 2008).

9. Civil E-Discovery

§ 9.0 Overview

Electronic discovery has become a standard part of the litigation process, fostered by a growing awareness among counsel and the bench that nearly all evidence is digital. "Rules 26(b) and 34 of the Federal Rules of Civil Procedure instruct that computer-stored information is discoverable under the same rules that pertain to tangible, written materials."[377] The vast majority of documentation now exists in electronic form and in most cases is non-numeric.

The changes to the Federal Rules of Civil Procedure relating to ESI were made in 2006. Yet, more than seven years later, it is perhaps perplexing to see that organizations are still being sanctioned for not appropriately handling their ESI for litigation and investigations. Particularly for more recent cases, a few common themes continue to arise:

- Importance of a timely and documented legal hold notice process
- Self-collection – Still a bad idea (*NDLO v. ICE)*
- Failure to preserve ESI from reasonably accessible data sources (*Apple v. Samsung*)
- Lack of coordination of production of ESI across multiple cases (*Delta / Airtran Baggage Fee Antitrust Litigation)*
- Continuing efforts to streamline ESI review (*Da Silva Moore, Kleen Products* Cases)

These cases will be discussed in further detail in this chapter.

The difficulty in maintaining compliance with legal standards for e-discovery in civil cases is not simply a lack of attention to these issues, but the constant vigilance that is needed to keep up with the changes in technologies for the data sources as well as the methods to acquire and process such data. This chapter will provide an overview of a number of different issues that should be addressed in putting together a defensible process for ESI.

§ 9.1 E-Discovery – A Mandated and Routine Process

The Federal Rules of Civil Procedure (FRCP) specifically address the unique challenges of electronic discovery. The 2006 Amendments modified the existing rules in a manner intended to further highlight the importance of and provide a more established framework regarding electronic discovery. To

377 Rowe Entm't, Inc. v. The William Morris Agency, No. 98 Civ. 8272(RPP), 2002 WL 975713 at *3 (S.D.N.Y. May 9, 2002).

comply with these rules, large organizations and their counsel have to undergo significant procedural and operational changes.

The amendments to the Federal Rules of Civil Procedure have had a significant impact in e-discovery. According to the *Georgia Daily Report*, the "[r]esults of a[n] . . . online poll of executives conducted by Deloitte Financial Advisory Services portray the growing volume of electronic data in corporations as a virtual litigation disaster waiting to happen." Almost 40 percent of executives responding to the survey expressed concern that "data volumes in their organizations are increasing in size and becoming unmanageable." Furthermore, "17.5 percent of executives [said] their companies are not ready to handle complex discovery requests," and almost "12 percent of companies surveyed have no policy in place to provide clear guidance for the IT department and other employees on document retention and destruction." The Daily Report noted that the concern is caused by "a Federal Rules of Civil Procedure amendment requiring companies to have the ability to quickly access electronically stored information in the event of litigation."[378]

The projected impact of the amendments involved both intangible effects and more concrete operational changes. From a historical standpoint, the Federal Rules of Civil Procedure are not regularly amended, and when they are, the entire legal profession, including the judiciary, is attuned to the changes. And while e-discovery has always fallen under the general purview of the current discovery rules, the amended rules specifically address e-discovery and provide standardized terminology and a clear framework.

For instance, Rule 34 defines computer-based information and other digitally stored data as "Electronically Stored Information" (ESI). The ESI definition had already permeated the nomenclature of key judges and legal pundits, but now it is enshrined in the statute.

Consistent and uniform terminology and framework should result in a more consistent and uniform approach by the courts to ESI discovery. The FRCP Amendments send a clear message of standardization and the inevitability of ESI discovery. Everyone is on notice, and there is no longer any uncertainty regarding the overall importance of ESI. As such, e-discovery is now an integral part of all federal civil litigation.

In terms of more specific operational impact, a consistent theme throughout the amended rules is one of a de facto requirement for large organizations to adopt a systemized internal process to address inevitable ESI discovery. This theme of systemization is centered on three key elements of the amendments:

1. The early attention requirements
2. The native file production requirement for ESI
3. The "safe harbor" rule for when data is deleted in the normal course of business.

One of the most important aspects of the FRCP is that they direct attention to electronic discovery issues early in the litigation process. For instance, the amended rules require that relevant electronic evidence be identified, preserved and disclosed at the initial outset of the litigation. As noted by

378 http://www.law.com/jsp/ihc/PubArticleIHC.jsp?id=1202423760005&rss=newswire (last accessed on May 20, 2009).

the Judicial Conference in their September 2005 comments to the amendments: "The proposed amendments to Rule 16, Rule 26(a) and (f), and Form 35 present a framework for the parties and the court to give early attention to issues relating to electronic discovery, including the frequently-recurring problems of the preservation of the evidence…"

The preservation element is particularly critical. Courts are increasingly holding parties to a stricter standard concerning the preservation of ESI, and the amendments and their corresponding comments strongly emphasize the importance of the duty to properly preserve ESI. The comments to Rule 26(f) note "[t]he volume and dynamic nature of electronically stored information may complicate preservation obligations . . . failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes."

Under these guidelines, parties must convene (per Rule 26(f)) to discuss the preservation and production of ESI. At the subsequent Rule 16 case management conference, which is usually held within weeks of the filing of the lawsuit, counsel must be prepared to discuss the ESI preservation already undertaken in the case, including details of the executed litigation hold. An influential 2007 manual written for the Federal Judiciary underscores the importance of these early meetings:

> "All too often, attorneys view their obligation to 'meet and confer' under Federal Rule of Civil Procedure 26(f) as a perfunctory exercise. When ESI is involved, judges should insist that a meaningful Rule 26(f) conference take place and that a meaningful discovery plan be submitted." [379]

Thus, litigants face an even greater likelihood of court sanctions if they fail to properly preserve relevant ESI at the outset of the litigation. It is no surprise, then, that the cases post-amendment underscore the need for a defensible e-discovery preservation and collection capability. In these important decisions, courts are carefully scrutinizing efforts undertaken to execute litigation holds and collections in the context of motions to compel and for sanctions.

For instance, in *Tomlinson v. El Paso Corp.*[380], the courts made it clear that the e-discovery process is the company's responsibility. In *Tomlinson* the pension plan participants sought production of electronic pension plan records from the defendant employer. The defendant maintained it could not produce the data because it was in the possession of a third-party plan record-keeper. The plaintiffs argued that the defendant had a duty under the Employment Retirement Income Security Act (ERISA) to maintain the data for inspection or examination. The court concluded that it was the defendant's responsibility. The court held the data was in the defendant's possession, custody or control within the meaning of Fed. R. Civ. P 26(a)(1)(B) and subsequently ordered production of the requested

379 Additional amendments to the FRCP relating to e-discovery currently are being considered. One is a proposed change to Rule 26(f) which would add a requirement of "proportionality" to the definition of the scope of discovery. Another proposed amendment is to Rule 37(e), the former "safe harbor" provision, which inserts "substantial prejudice based on wilful conduct or bad faith" as a prerequisite for sanctions relating to the preservation of discoverable information. The new rules, if accepted and promulgated, would take effect on or after December 1, 2014. A copy of the proposed rules can be obtained at http://www.uscourts.gov/RulesAndPolicies/rules/proposed-amendments.aspx.

380 245 F.R.D. 474 (D.Colo. 2007)

documents.[381] This rule makes it clear that an organization cannot "turn a blind eye" regarding their e-discovery responsibilities.

In *Z4 Technologies, Inc. v. Microsoft Corp.*[382], Microsoft was not aware or knowingly failed to disclose the existence of a database. They also were not able to produce an email during discovery. Microsoft was sued by Z4 Technologies for patent infringement and was ordered by a federal judge in Texas to pay enhanced damages of $25 million plus almost $2 million in attorney fees for failure to comply with these two requests.

In *Kelly v. Montgomery Lynch & Assoc.*[383], the plaintiff filed a motion to compel discovery necessary to support a motion for class certification. The defendant claimed the discovery request was unduly burdensome because the filing system was not maintained in a searchable format. Finding the defendant did not make a reasonable inquiry into the discovery request apart from claiming an undue burden, the court ordered the defendant to comply with the plaintiff's narrowly tailored discovery request.

In re NTL, Inc. Securities Litigation[384], the court imposed severe sanctions, including adverse inference instructions, attorney fees and costs, upon discovering the defendant and related entity lacked a defensible process to preserve and collect ESI. Upon reviewing the steps taken to preserve and collect ESI after litigation commenced, the Court determined that the named defendant was grossly negligent because "[t]he evidence, in fact, [showed] no adequate litigation hold existed..." Although the defendant had circulated two document-hold memoranda, the court faulted the adequacy of the overall process, noting that many employees never received the memoranda and that no concerted effort to collect the relevant ESI took place.

In *Star Direct Telecom, Inc. v. Global Crossing Bandwidth, Inc.,* No. 05-CV-6734T (W.D.N.Y. Mar. 22, 2012 the court, granted, in part, plaintiff US Telesis Inc.'s Motion for Spoliation Sanctions holding that the defendant failed to preserve the email and computers of key custodians after the commencement of litigation. Plaintiff US Telesis moved for spoliation sanctions arguing that the defendant had an obligation to preserve and not destroy emails from 2004. The defendant countered that it was not under a duty to preserve until the complaint was filed in December 2005. The defendant argued that they could not have anticipated litigation earlier based on the plaintiff's grievances, particularly where in the same time period the defendant received 2,218 billing disputes and only the plaintiff's case resulted in litigation. Similarly, in 2006, the defendant had more than 1,600 billing disputes and only two customers initiated litigation. Finding that the defendant's conduct was grossly negligent, the court still awarded only monetary sanctions in the absence of bad faith or a showing by the plaintiff of prejudice.

As these case examples illustrate, litigants face a much higher likelihood of court sanctions if they fail to properly preserve relevant ESI from the outset of the litigation.

In order to properly identify, preserve and disclose relevant ESI, large companies are establishing

381 Id. at 477.

382 507 F.3d 1340 (6th Cir. 2007).

383 No. 1:07-CV-919, 2007 WL 4412572 (N.D. Ohio Dec. 13, 2007).

384 244 F.R.D. 179 (S.D.N.Y. 2007).

highly operational and systemized processes to address ESI requirements as standard litigation practice with each case, in place of a more reactive and ad hoc approach. The traditional "wait and see" approach to e-discovery–where companies and their counsel often defer addressing ESI until its production is demanded by their opponent–results in a disjointed approach to ESI categorized by hurried outsourcing or other non-systemized collection and preservation efforts that greatly increased cost and risk. However, such practices are no longer sustainable under the amendments to the FRCP. Courts will only accept as reasonable an integrated, systemized, and efficient internal process, which routinely identifies and preserves relevant ESI at the outset of litigation.

As previously mentioned, the second key "systemization" element of the FRCP Amendments involves the provisions for the production of ESI. Rule 34(b) provides a procedure for specifying and objecting to the form of production of ESI. Under subsections 34(b)(ii) and 34(b)(iii), if the requesting party does not specify the form of production, the default form for producing electronically stored information is that form "in which it is ordinarily maintained [or] reasonably usable." It is widely expected that most requesting parties will designate that ESI be produced in its native file format, which is generally how ESI is ordinarily maintained and is generally the most usable format.

Additionally, requesting parties will also require under Rule 34(b) that the production of ESI be in a format with its applicable metadata intact. Numerous decisions hold that file metadata contained within ESI must also be preserved and produced.[385] When ESI discovery is outsourced and not systemized, it is difficult to properly preserve and produce ESI in its native format with its metadata intact.

Outside consultants that handle their client's ESI will typically process the data in several stages to filter, de-duplicate, and format the ESI for attorney review. Such processing is necessitated by an inefficient and non-systemized collection and preservation process that results in significant over-collection. In addition to being expensive, this processing often results in the loss of metadata and the conversion from native format to an image or .PDF format. An internal and systemized process can better preserve and produce ESI in its native format by utilizing enterprise technologies that enable more efficient and targeted data collection, as well as review tools that support native file review and production.

Finally, the "safe harbor" rules are also a key "systemization" element of the FRCP. Subsection 37(e) states, in full, "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system." The Advisory Committee Notes explain that ordinary computer use necessarily involves routine alteration and deletion of information for reasons unrelated to litigation.

The overall theme is that courts are unwilling to overlook discovery abuses. Given the proper facts, courts will impose sanctions, including monetary, adverse inference sanctions, and even default

385 See Nova Measuring Instruments Ltd. v. Nanometrics, Inc., 417 F. Supp. 2d 1121 (N.D. Cal. 2006); In re Verisign Inc. Sec. Litig., No. C 02-02270 JW, 2004 WL 2445243 at *1 (N.D. Cal. March 10, 2004) (upholding discovery orders requiring production of documents in native format with metadata as not clearly erroneous: "'[t]he electronic version must include metadata as well as be searchable'"). See also In re Honeywell Int'l, Inc. Sec. Litig., 230 F.R.D. 293, 296 (S.D.N.Y. 2003).

judgment. Therefore, the best advice for corporations and their counsel is to remain observant in preserving electronic information and addressing e-discovery issues. Parties should have a clear understanding of the "safe harbor" protection and make an objective and recurring analysis of whether their policies allow them to take advantage of Rule 37(e).

For instance, the court in *Doe v. Norwalk Community College*[386] refused to allow the defendant to claim the protections of Rule 37(f) because it failed to suspend its deletion policy upon notice of litigation. Another court refused protection in *In re Krause*[387] because the hard drive wiping was not discontinued once the duty to preserve attached. The court in *Oklahoma ex. rel. Edmondson* went so far as to warn the parties to be "very cautious in relying upon any 'safe harbor' doctrine as described in new Rule 37(e)." [388]

In order for a party to establish that the deletion of ESI resulted from the routine and good-faith operation of their electronic information system, the party must be able to demonstrate the existence of an established, well-documented and systemized electronic records management process. This process must be effectively tied into the party's litigation readiness plans, so that litigation holds are effectively executed.

Again, this is impossible without a well-planned and established system-wide process. As with each of the three elements of the new rules discussed above, the more established and systemized the process to preserve, collect and delete ESI, the more reasonable and defendable the process will be found by the court.

For instance, *Williams v. Taser International, Inc.,*[389] shows that, the threshold for a bad faith determination is very low. The court previously found that defendant's privilege log was inadequate. As a result, the defendant was ordered to provide a privilege log that met the requirements of Rule 26(b)(5)(A) and was warned that failure to comply would result in the waiver of any claim of privilege. According to the court, defendant's privilege log--submitted following the order--remained inadequate.

The court recognized that a large number of documents had to be reviewed by defendant, but held that the time taken to provide an adequate privilege log was unjustified. The court noted that defendant was involved in other litigation with similar issues and likely had previously reviewed at least some of the documents. The court concluded that defendant's delay rose to the level of bad faith and warranted the sanction of waiver of privilege claims. Defendant thus was ordered to provide plaintiffs with all documents listed on the privilege log.

To address these challenges and the reality of the new framework, large companies are looking to bring much of their e-discovery processes in house. A common new hire at *Fortune* 500 legal departments is a deputy general counsel exclusively dedicated to e-discovery and records management. His or her mission is to get the organization's e-discovery and records management process in order, reduce risk, and reduce costs.

For large organizations, e-discovery costs and associated risks are spiraling out of control. With a

386 248 F.R.D. 372 (D. Conn. 2007).

387 367 B.R. 740 (Bankr. D. Kan. 2007).

388 Oklahoma, ex rel. Edmondson, No. 05-CV-329-GKF-SAJ, 2007 WL 1498973 at *6 (N.D. Okla. May 17, 2007).

389 247 F.R.D. 694 (N.D. Ga. 2008).

process that is largely outsourced, a major corporation can expect to incur tens of millions of dollars in out-of-pocket costs annually, mostly in the form of outside consultant fees to collect and process data. Beyond the significant expense of a non-systemized e-discovery process, a global and systemized approach enables not only cost savings, but also an improved ability to comply with the amended federal rules.

The traditional and non-systemized approach to electronic evidence discovery involves a highly manual process to gather immense sums of data and then load that data onto a system that allows for searching and processing. This approach results in ever-increasing costs as the volume of data within a corporation grows. For instance, without enterprise computer investigation technology, collecting files from hundreds or even thousands of computers distributed across multiple locations must be performed manually. With no means to prioritize and filter out irrelevant data, the collection is overbroad, and a great deal of irrelevant data is aggregated into a central database where it is then finally processed and searched. In addition, metadata is lost in the process and files are migrated into non-native formats.

By providing for effective, customized, and manageable system-wide searches of distributed workstations and servers throughout the global enterprise; a more targeted and presumptively relevant data set is returned to a centralized location in an automated fashion. Additionally, this technology enables the live and remote analysis and collection of evidence over a network from centralized locations in a sound and non-invasive manner, and thus does not disrupt operations. This capability greatly reduces risk by providing a highly defensible process and reducing many of the pains and liabilities associated with a broken e-discovery process.

Establishing a defensible process is a critical element of compliance as opposing counsel are now routinely seeking to capitalize on the e-discovery struggles of large corporations. Claimant's lawyers in particular seek to distract the defense with "litigation within a litigation" allegations of spoliation or lack of due diligence in complying with e-discovery requests. Plaintiffs seek to gain a significant advantage by obtaining evidentiary sanctions, petitioning the court for an order allowing their own experts to investigate the corporate defendants' systems, or otherwise driving up the cost of litigation by forcing costly and overbroad computer evidence investigations. With the new framework provided by the FRCP amendments, these tactics will only increase.

An established enterprise investigation capability can be a powerful shield against these tactics, as the supporting software is built upon the same processes and technology as that relied upon by top law-enforcement agencies for their computer investigations. (See, e.g., *Sanders v. State*[390], [Court notes that "EnCase is the field standard for computer forensics investigation."]) Such a solid foundation of credibility and reliability provides a highly defensible and diligent process to establish compliance and confidence with the courts in e-discovery matters. In light of the new federal rules' clear and consistent emphasis on the importance of properly preserving and identifying relevant ESI, large organizations can ill-afford not to have such a scalable, systemized–and thus defensible–process in place.

390 191 S.W.3d 272 (Tex. App. 2006).

§ 9.2 Sanctions

The following are some of the more notable cases involving both the imposition of sanctions and the denial of sanctions. (*See also, Real eDiscovery, Winter 2010 - Ediscovery Spoliation Sanction Milestone; and Real eDiscovery, Fall 2010 - Reduce Risk by 80 Percent.)*

Harkabi v. Sandisk Corp.[391]

In *Sandisk*, a dispute arose between the plaintiffs and Sandisk regarding the implantation of plaintiffs' technology in two Sandisk products. The plaintiffs sought proof of their involvement in the technology by obtaining their company laptops and e-mails. To that end, plaintiffs issued a preservation letter to Sandisk. In response, Sandisk in-house counsel issued a do-not-destroy memo to preserve the plaintiffs' laptops.

Although Sandisk did technically follow the preservation request, when they switched their e-mail server some of the e-mails were not preserved because the preservation instructions were for current employees only. The court held Sandisk to a higher standard of care by reasoning that:

> Sandisk [is] a global business that champions itself a leader in electronic data storage. Its size and cutting edge technology raised an expectation of competence in maintaining its own electronic records. The concatenation of omissions and missteps at Sandisk reveal a lack of attention to detail that has worked a hardship on the plaintiffs and delayed this litigation.

The court noted that failing to preserve the laptops was "at a minimum" negligent and indicated that an adverse inference is appropriate. For "prolonged delay" in producing relevant e-mails, the Court denied terminating sanctions but ordered monetary sanctions in the amount of $150,000.

Victor Stanley, Inc. v. Creative Pipe, Inc.[392]

This decision followed an early decision in *Victor Stanley, Inc. v. Creative Pipe, Inc.*[393] The case is attracting significant attention because of its finding of civil contempt on the part of the defendants. Judge Grimm ordered the defendants' president to be imprisoned for up to two years, unless and until he pays plaintiffs' fees and costs relating to the motions for spoliation of evidence. However, on defendants' appeal, the district court judge declined to adopt the Magistrate Judge's order regarding incarceration:

> [T]he court does not find it appropriate to Order Defendant Pappas incarcerated for future possible failure to comply with his obligation to make payment of an amount

391 275 F.R.D. 414 (S.D.N.Y. 2010).
392 269 F.R.D. 497 (D. Md. 2010).
393 250 F.R.D. 251 (D. Md. 2008).

> to be determined in the course of further proceedings. Certainly, if Defendant Pappas should fail to comply with a specific payment order, the Court may issue an order requiring him to show cause why he should not be held in civil contempt for failure to comply with that payment order. Also, under appropriate circumstances, criminal contempt proceedings might be considered.[394]

The district court upheld the Magistrate Judge's order and recommendations in all other respects, however, and ordered defendants to pay plaintiff Victor Stanley, Inc. $337,796.37 as a sanction for their bad-faith spoliation.

This opinion echoes the continuing frustration of the courts for parties not doing the right thing when they have a lawsuit: preserve ESI.

Judge Grimm is dumbfounded to find yet another case where a party fails to implement a litigation hold on key data sources and fails to take any reasonable measures to preserve data. *Slip op.* at 13-14. Moreover, the key bad actor for the defendant was found to have deleted nearly ten thousand files *during* the discovery stay. *Id.* at 24. Judge Grimm observes that the culmination of bad acts and omissions relating to preservation of ESI "constitute the single most egregious example of spoliation that I have encountered in any case that I have handled or an any case described in the legion of spoliation cases I have read in nearly fourteen years on the bench." *Id.* at 34.

What is clear from Judge Grimm's opinion, as well as the recent Sedona Conference® emphasis on proportionality, is that the courts are not looking for organizations to "boil the ocean" and completely revamp their entire IT systems and architecture in order to respond to discovery requests. Judge Grimm echoes the frequent refrain that the preservation duty "pertains only to relevant documents" and is "neither absolute, nor intended to cripple organizations." *Id.* at 49-50. The court's view of whether preservation conduct is acceptable in a case depends on what is *reasonable* and whether what was done (or not done) was *proportional* to the case.

The patented Optimized Distributed Search ("ODS") capability in EnCase eDiscovery helps in demonstrating a defensible and cost-effective preservation process: collect and preserve *only* what is relevant to a lawsuit from reasonably accessible data sources (laptops, desktops, servers, ECM repositories) *when* you need it. There is no need to index or archive your entire IT environment.

EnCase eDiscovery's First Pass Review capability also enhances another important step in the ESI preservation process: assessing the accuracy and validity of selected search terms. Designed for legal department, this interface allows non-technical personnel to get granular analytics on the specific impact of search terms on a data set. This functionality is key to demonstrating a defensible process, as Judge Grimm observes that "failure to assess the accuracy and validity of selected search terms also could be negligence." *Id.* at 64 (citations and internal quotations omitted).

394 06-cv-02662 (MJG) [Dkt. 397] (D. Md. November 1, 2010).

Green v. McClendon[395]

This case concerns the duty of defendant and their attorneys to preserve ESI. It highlights the fact that attorneys must always be prepared to identify, preserve, and search for ESI. Attorneys must take the necessary steps to educate themselves about their clients' electronic data systems, regardless of whether their client is a large corporation or an individual.

Regarding the scope of the obligation to both a litigant and to counsel, the court stated:

> "Once a 'litigation hold' is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed 'on hold' . . . ." *Id.* Then, "[c]ounsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched." *Id.*

Addressing culpability, the court found that the defendant *and her counsel* had been "at least negligent" in failing to implement a litigation hold, properly search for documents, and supplement discovery responses.

The court reasoned:

> "The preservation obligation runs first to counsel, who has 'a duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing its destruction.' "*In re NTL, Inc. Securities Litigation,* 244 F.R .D. 179, 197-98 (S.D.N.Y.2007) (quoting Chan, 2005 WL 1925579, at *6); *see also Fayemi v. Hambrecht and Ouist, Inc.,* 174 F.R.D. 319, 326 (S.D.N.Y.1997). Moreover, this responsibility is "heightened in this age of electronic discovery." *Qualcomm Inc. v. Broadcom Corp.,* 05 Civ.1958-B, 2008 WL 66932, at *9 (S.D.Cal. Jan. 7, 2008), *vacated in part on other grounds,* 2008 WL 638108 (S.D.Cal. March 5, 2008)."[396]

The court determined an adverse inference was not appropriate; however, finding that the defendant and counsel violated their duty to preserve evidence, the court authorized additional discovery and awarded plaintiff his costs, including attorney's fees, to be paid by the defendant and her counsel.

Qualcomm Inc. v. Broadcom Corp

Despite what she characterized as a "massive discovery failure," United States Magistrate Judge for the Southern District of California, Barbara L. Major, declined to impose sanctions on outside counsel absent evidence of bad faith in *Qualcomm Inc. v. Broadcom Corp.*[397]

The case has a relatively long history. On January 7, 2008, the trial court found that plaintiff Qualcomm Incorporated ("Qualcomm") intentionally withheld tens of thousands of documents that

395 262 F.R.D. 284 (S.D.N.Y. 2009).

396 Id. at 290.

397 No. 05CV1958-B (BLM), 2010 WL 1336937 (S.D. Cal. Apr. 2, 2010).

defendant Broadcom Corporation ("Broadcom") had requested in discovery. The court also found that six attorneys assisted Qualcomm in withholding the critical documents by failing to conduct a reasonable inquiry into the adequacy of Qualcomm's document production and by ignoring the "warning signs" that the search was inadequate. The court awarded defendant all of its attorney fees and costs in the litigation totaling $8.5 million. The attorneys were ordered to forward the court's order to the State Bar of California for investigation, and to participate in a Case Review and Enforcement of Discovery Obligations program to create a case management protocol to serve as a model in the future.

Qualcomm did not appeal the $8.5 million sanction imposed against it; however, the Qualcomm attorneys filed objections to the sanctions order with the trial judge. On March 5, 2008, the sanctions order was vacated and remanded, finding that the sanctioned attorneys had a due process right to defend themselves and "should 'not be prevented from defending their conduct by the attorney-client privilege . . .'" of plaintiff and its employees and representatives.[398] The sanctioned attorneys were provided with an opportunity to conduct discovery and to present new facts.

After considering all of the new facts, Magistrate Judge Major declined to sanction any of the attorneys. According to Judge Major, "there still is no doubt in this Court's mind that this massive discovery failure resulted from significant mistakes, oversights, and miscommunication on the part of both outside counsel and Qualcomm employee ... However, it also revealed that the Responding Attorneys made significant efforts to comply with their discovery obligations."[399]

She characterized the fundamental problem in the case as an *incredible breakdown in communication*: "The lack of meaningful communication permeated all of the relationships (amongst Qualcomm employees {including between Qualcomm engineers and in-house legal staff}, between Qualcomm employees and outside legal counsel, and amongst outside counsel) and contributed to all of the other failures."[400]

Judge Major also noted that one of the most significant failures on the part of the Qualcomm attorneys was their lack of familiarity with and understanding of Qualcomm's IT infrastructure:

> "Moreover, outside counsel did not obtain sufficient information from any source to understand how Qualcomm's computer system is organized: where emails are stored, how often and to what location laptops and personal computers are backed up, whether, when and under what circumstances data from laptops are copied into repositories, what type of information is contained within the various databases and repositories, what records are maintained regarding the search for, and collection of, documents for litigation, etc. Finally, no attorney took supervisory responsibility for verifying that the necessary discovery had been conducted (including ensuring that all of the correct locations, servers, databases, repositories, and computers were correctly searched for potentially relevant documents) and that the resulting discovery

398 Id. at *1.
399 Id. at *2.
400 Id.

> supported the important legal arguments, claims, and defenses being presented to the court. These fundamental failures led to the discovery violations."[401]

Judge Major noted that she had the inherent power to impose sanctions on attorneys who engage in abusive litigation practices, but that sanctions may only be imposed under the court's inherent authority *upon a finding that the attorney acted in bad faith*.[402] And so, while she acknowledged that the evidence presented at the remand proceedings established that "significant errors" were made by Qualcomm attorneys, Judge Major found that there was insufficient evidence to prove that any of them had engaged in the "requisite bad faith" to impose sanctions.[403]

In re A&M Fla. Props. II, LLC[404]

In this case, Chief Bankruptcy Judge Arthur Gonzalez was asked to impose sanctions pursuant to Federal Rule of Civil Procedure 37(d) for intentional obstruction of the discovery process.

The case concerned e-mail communications evidencing the fact that GFI Acquisition (GFI), a subsidiary of A&M Florida Properties LLC, had received copies of promissory notes. Although the defendant was certain that plaintiffs should be in possession of such e-mails, they were not produced. However, late in the case, relevant e-mails were located after a forensic examination and countless attempts to locate the relevant e-mails.

The court noted: "[h]ad Nash fulfilled his obligation to familiarize himself with GFI's policies earlier, the forensic searches and subsequent motions would have been unnecessary. The Court finds that monetary sanctions are appropriate here and orders GFI and its counsel to reimburse American Federated its half of the cost of the forensic searches. GFI and its counsel are also ordered to reimburse American Federated for the costs associated with bringing the motion for sanctions and the motion to compel."[405]

To be sure, the court considered imposing terminating sanctions (dismissal with prejudice), but concluded that the lack of intentional destruction of evidence/failure to obey court orders meant that "dismissal would be unjustly harsh here, especially considering that American Federated eventually acquired the documents it sought all along. To obtain an adverse inference instruction for the late production of evidence, the moving party must establish that:

> "(i) the party having control over the evidence had an obligation to timely produce it; (ii) the party that did not timely produce the evidence acted with a "culpable state of mind"; and (iii) the tardily produced evidence is "relevant" to the party's claim or

401 Id.
402 Id. at *6.
403 Id. at *7.
404 No. 09-15173 (AJG), 2010 WL 1418861 (Bankr. S.D.N.Y. Apr. 7, 2010).
405 Id. at *7.

defense "such that a reasonable trier of fact could find that it would support that claim or defense.""[406]

In the end, the defendant was able to obtain the desired e-mails and there was no evidence of bad faith on the part of GFI's counsel. The producing party simply did not understand the technical depths to which electronic discovery can sometimes go. The court did not find any intent to block American Federated from gaining possession of the discovered messages.

Bray & Gillespie Mgmt., LLC v. Lexington Ins. Co.[407]

Even though United States District Court Judge for the Middle District of Florida, Mary S. Scriven, chose not to impose the "excessive remedy" of dismissing the plaintiff's *entire* amended complaint (which was the recommendation of the Magistrate Judge), she did dismiss with prejudice the plaintiff's claims for damages arising from or related to any alleged interruption of business in *Bray & Gillespie Mgmt., LLC v. Lexington Ins. Co.*

Plaintiff was seeking coverage from the defendant insurer for business interruption losses resulting from three hurricane strikes that took place on the plaintiff's hotel resort property. Defendant sought discovery that would show that the hotel had re-opened after the second hurricane and that the plaintiffs only lost business due to the third hurricane. During the deposition of the defendant's expert, plaintiff first disclosed the existence of certain "room folios" that might be used to contest the defendant's expert's theory. The room folios were compilations of data from various points of sale in and around the property documenting a guest's stay and use of the hotel facilities, and could be used to confirm revenue figures reported by plaintiff prior to the third hurricane.

Upon reviewing the defendant's expert report and noting discrepancies in the folio information, the plaintiff claimed it realized that additional folios had to have been generated. The plaintiff undertook a subsequent search for folios and discovered hard copies of additional folios in boxes of files that had been sent to storage but that had never been searched. Based upon this, the Magistrate Judge sanctioned the plaintiff for the late production, and held the plaintiff and two of its outside counsel jointly and severally liable for defendant's costs, including attorney and expert fees.

Plaintiff explained that the discrepancy in the production was a result of the computerized accounts management system and filing software it used at the resort, although the court noted that explanation did not fully account for all of the gaps in production. Plaintiff's substitute counsel, however, called the software provider of the system used to capture and produce room folios and learned that (1) despite threats of dismissal by the court, plaintiff had never previously consulted its software provider to attempt to retrieve the archived documents, and (2) the archived files were likely retrievable with minimal effort and expense and could likely render all room folios available for review for the relevant time period.

Judge Scriven noted that a finding of bad faith or willfulness is necessary to impose the most

406 Id. at *6.

407 No. 6:07-cv-0222-Orl-35KRS, 2010 WL 55595 (M.D. Fla. Jan. 5, 2010).

"severe sanction" of default or dismissal. Not only did she find that the plaintiff had, in fact, acted willfully and in bad faith, but Judge Scriven also found that the plaintiff "evidenced a pattern of inexcusable disregard for the authority of this Court and the larger civil discovery process."[408] Despite that, however, Judge Scriven found that, "dismissal of Plaintiff's entire Amended Complaint, as recommended by the Magistrate Judge, would be an excessive remedy."[409]

First, she found unpersuasive defendant's contention that plaintiff's failure to produce the Treasure Island room folios prevented defendant from interviewing persons who could describe the condition of the resort and the room rented at the time of that person's stay. Second, the deliberate misconduct was only related to the production of room folios.

Accordingly, Judge Scriven dismissed with prejudice all claims against defendant for damages arising from or related to any alleged interruption of business at the resort property caused by the second hurricane; however, plaintiff's claims for other damages, including for reimbursement of property damage allegedly caused to the resort property by the second hurricane, remained for trial. Further, she imposed sanctions in the amount of $75,000.00, which was also meant to serve as a partial reimbursement to the defendant for expenses incurred in pursuit of its motion for sanctions and the full production and use of all room folios.[410]

Green v. Blitz U.S.A., Inc.

The withholding of relevant ESI by a defendant resulted in civil contempt sanctions, mandatory disclosure in other lawsuits, the possibility of a $500,000 sanction, as well as the general ire of United States District Court Judge T. John Ward in *Green v. Blitz U.S.A., Inc.*, 2011 US DIST. LEXIS 20353 (E.D. Tex., March 1, 2011).

In 2007, Plaintiff Rene Green ("Green") brought a products liability lawsuit against Defendant Blitz U.S.A., Inc. ("Blitz"). At the conclusion of the evidence and before the jury returned a verdict, the parties entered into a high-low settlement agreement. The jury returned a unanimous verdict against the plaintiffs, resulting in a settlement figure at the low end of the high-low range; the case was closed on November 10, 2008.

Counsel for the plaintiff in the *Green* case, however, was also counsel in a related case in the Western District of Texas, where Blitz was also the defendant. Through discovery in the other case, and nearly a year after the trial in the *Green* case, counsel learned of documents that were not produced by Blitz in the *Green* case and promptly filed a motion in February of 2010. Green argued that Blitz failed to produce certain documents and also failed to preserve documents.

It was eventually revealed that Blitz had a single employee, Larry Chrisco ("Chrisco"), who from 2004 until 2007 was solely responsible for searching and collecting relevant documents in the ongoing litigation against Blitz. Chrisco, however, never instituted a litigation hold of documents, did

408 Id. at *5.
409 Id.
410 Id. at *6.

any electronic word searches for e-mails, talked with the IT department regarding how to search for electronic documents, and even admitted that "I am about as computer literate--illiterate as they get."

But this was not the end of Blitz's discovery abuses. As outlined by Judge Ward:

> . . . Blitz made little, if any, effort to discharge its electronic discovery obligations. But Blitz also failed to preserve its electronic documents. Far from instituting a litigation hold on relevant electronic documents, Blitz actually asked its employees to routinely delete electronic documents. From 2004 through 2007, Blitz's IT department head, Paul Hale, routinely sent emails to all Blitz employees instructing them and encouraging them to delete email…
>
> . . . Paul Hale admits that when he sent these multiple emails telling employees to delete their email, the employees were not told to retain email relevant to ongoing litigation. Additionally, during the Feb. 1, 2011 Show Cause Hearing, Larry Chrisco admitted that he never communicated any type of "litigation hold" request to the employees at Blitz…
>
> Finally, to make matters worse, Blitz rotated its backup tapes every two weeks during this time period -- at such time the old backup tapes are permanently deleted -- so the deleted emails by the employees are permanently lost. Because of this systematic destruction of potentially relevant documents, it will never be known how much prejudice against the plaintiff was actually caused by Blitz's failure to preserve documents. The Court holds that Blitz's failure to preserve is sanctionable under the Court's inherent powers.

The Court denied Plaintiff's Motion to Re-Open the Case, but ordered Blitz to pay $250,000.00 in civil contempt sanctions to Green. The Court ordered "that Blitz has thirty (30) days from the date of the Memorandum Opinion & Order to furnish a copy of this Memorandum Opinion & Order to every Plaintiff in every lawsuit it has had proceeding against it, or is currently proceeding against it, for the past two years."

The Court issued an additional $500,000.00 sanction that will be tolled for 30 days from the date of the Memorandum Opinion and Order. According to Judge Ward, "At the end of that time period, if Blitz has certified with the Court that it has complied with the Court's order, the $500,000.00 sanction will be extinguished." To top it all off, Judge Ward ordered that, "for the next five years, Blitz is ordered that in every new lawsuit it participates in as a party, whether plaintiff, defendant, or in another official capacity, it must file a copy of this Memorandum Opinion and Order with its first pleading or filing in that particular court." The Court expressed no opinion as to the manner in which a particular court may use or not use such copy.

The number of cases addressing claims for sanctions based on failure to preserve ESI continue to grow. Some examples include:

Beck v. Test Masters Educ. Servs., Inc.[411]

In this D.C. Consumer Protection Procedures Act case, the defendant revealed in opposition to a motion to compel that it had accidentally lost or destroyed emails. Although the destruction allegedly did not occur in bad faith, the court awarded sanctions in the form of an adverse inference instruction. On defendant's motion to vacate the order, the court held that an adverse inference was appropriate even absent bad faith in part because the defendant "failed to make any serious effort to recover the data" after e-mails were deleted and a computer crashed, and such a "lackadaisical response constitutes a conscious disregard of . . . preservation obligations." (Internal quotations omitted). However, the court modified its prior order on a mandatory adverse inference instruction to make the instruction a permissive one because it found defendant's destruction was not intentional. The court also awarded plaintiff its costs and fees in making the sanctions motion under Rule 37(b).

EEOC v. JP Morgan Chase Bank, N.A.[412]

The EEOC moved for spoliation sanctions in this Title VII litigation after defendant destroyed ESI that it was on notice to preserve. Defendant's asserted that the destruction was due to routine deletion of electronic records and should not be sanctioned. The court granted plaintiff's motion to the extent of ordering a permissive adverse inference.

EEOC v. Ventura Corp. Ltd.[413]

Plaintiff moved for sanctions in this employment discrimination case, alleging destruction of email accounts and other deletion of data in a data migration after reasonable anticipation of potential litigation. Court awarded an adverse inference instruction and excluded parts of defendants' testimony where the defendant destroyed e-mail accounts and made large-scale changes to computer systems, including a software program migration, after being put on notice of the litigation hold.

Micron Tech., Inc. v. Rambus, Inc.[414]

In this patent infringement case, the district court dismissed claims against Micron due to Rambus' spoliation of evidence. On appeal, the Federal Circuit upheld the factual findings of spoliation, but vacated and remanded for a further explanation by the district court of why such a severe sanction was necessary. On remand, the district considered lesser sanctions, but ultimately held that the only appropriate sanction was to hold the patents-in-suit unenforceable against Micron.

In support of this holding, the court focused on (1) facts showing Rambus' document retention policy was adopted as a litigation plan; (2) facts showing the policy was executed selectively; (3) facts

411 2013 WL 772879, 2013 U.S. Dist. LEXIS 28716 (D.D.C Mar. 1, 2013).
412 2013 WL 765593 (S.D. Ohio, Feb. 28, 2013).
413 2013 WL 550550 (D.P.R. Feb. 12, 2013).
414 917 F.Supp.2d 300 (D.Del. Jan. 2, 2013).

showing Rambus knew its policy was improper; and (4) Rambus' litigation misconduct. Specifically, Rambus hired Joel Karp, who met with litigation attorneys to design the policy. Karp created the policy specifically to "develop a licensing and litigation strategy." Karp even called the policy "'necessary to prepare for the upcoming battle' in the context of Rambus' licensing and litigation strategies" in meetings with the Board of Directors. Moreover, against the advice of outside counsel, Karp encouraged employees "to 'look for things to keep' that would help Rambus prove its case . . . [and] expunge documents questioning the patentability of Rambus inventions." Karp "tried to keep [the policy] quiet" to hide it from outside counsel, by, inter alia, insisting that employee questions be face to face. In an internal memorandum about the litigation, Karp proposed a "shredding party" to expunge documents that might raise questions about the validity of Rambus' patents.

In light of Rambus' conduct, the district court noted: "Rambus' destruction of evidence was of the worst type: intentional, widespread, advantage-seeking, and concealed."

Northington v. H&M Int'l[415]

Circuit court affirmed an adverse inference instruction where the defendant moved its e-mail system to another vendor and key witness's e-mail account were deemed inactive and deleted.

Pillay v. Millard Refrigerated Services, Inc.[416]

In this wrongful termination suit, the court awarded an adverse inference sanction where a company's software automatically overwrote data related to plaintiff's job performance and necessary for plaintiff's case. Although the deletion was routine and in accordance with the company's ordinary retention policy, the court awarded sanctions because the defendant had notice of its duty to preserve and took no affirmative steps to prevent the automatic deletion. Plaintiff's counsel sent a demand letter and filed charges with the EEOC providing notice to defendant, and defendant's general counsel did nothing to prevent the automatic deletion. Further, the court found severe prejudice to the plaintiff from the deletion. Accordingly, the court held that the defendant had acted in bad faith or recklessly and granted plaintiff's motion for an adverse inference instruction.

§ 9.3 The Defensibility of an In-House Process and the 30(b)(6) Witness

In addition to considerable cost savings, establishing a systemized and consistent e-discovery process reduces business disruption and mitigates risk by enhancing compliance. As noted above, the "early attention" requirements of the amended FRCP mandate that organizations identify, preserve and collect relevant ESI at or near the outset of a litigation matter. A systemic process executed with plugged-in enterprise tools, run by a well-trained internal team familiar with the organization's IT infrastructure and that works alongside corporate legal, is well-suited to meet these requirements.

415 2013 WL 1150215 (7th Cir. Mar. 21 2013).
416 2013 WL 2251727 (N.D. Ill. May 22, 2013).

For these reasons, an in-house capability with a trained staff armed with best-practices technology is not only highly defensible, but is optimal for large organizations.

In fact, recent case law fully supports the defensibility of organizations handling e-discovery internally where best practices are employed. In addressing the issue of best practices concerning the searching and analysis of computer evidence, the *Zubulake v.* Court advised counsel to work closely with corporate IT to develop a process for identifying relevant sources of computer data and execute on preserving, collecting and searching that data.[417]

In *Williams v. Massachusetts Mutual Life Insurance Company*, the court found that the e-discovery investigation performed by internal IT security personnel at Massachusetts Mutual was proper and competent. Notably, Mass Mutual relied upon the testimony of its Chief Information Security Officer (CISO) regarding the thoroughness and competency of the investigation to establish a defendable process using best-practices technology and to defeat the plaintiff's highly charged motion to compel further discovery.[418]

Conversely, in *Residential Funding Corp. v. DeGeorge Fin. Corp.*, the court found it unreasonable for Residential to continue to retain an e-discovery service provider who was unfamiliar with the client's data storage systems. Residential's e-discovery provider professed to the court that "technical problems" prevented the timely and cost-effective retrieval of sought computer data. [419] One of the many benefits of an established and internalized process is that the key details of the organization's IT systems are accounted for, the network and key ESI storage locations are mapped, and the procedures to rapidly preserve and collect relevant ESI are in place in advance of the next case.

This is not to say that e-discovery service providers are not an important part of the process. Many consultants help to design efficient and systemized processes, which are in turn implemented by IT. Consultants can also effectively augment company staff for larger engagements, as well as routine overflow. Outsourcing is also usually a good option for mid-sized companies with lighter litigation volume. To be sure, an untrained, ill-equipped, and unprepared internal IT team may be the worst of all options. However, with the right technology, people, training, and well-defined procedures, an internalized process will be the most effective option for large organizations.

It is important to defend the steps a corporate defendant or plaintiff took to identify, preserve, collect, and produce documents relevant to the litigation. This requires detailed inquiry into a corporation's information management and retrieval systems in order to ensure that discovery was diligently completed in good faith. The target of this inquiry is the 30(b)(6) witness.

The deposition of the 30(b)(6) witness can be a nightmare for the unprepared because the court places a significant burden on companies to save potentially relevant ESI and other data when they face the threat of litigation. When a party has failed to produce any meaningful documents in response to a discovery request or appears to be uncooperative, the need for and relevance of this witness becomes that much more important.

The 30(b)(6) deponent is often the most important witness called to testify regarding electronic

417 Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004).

418 Williams v. Mass. Mut. Life Ins. Co., 226 F.R.D. 144, 146 (D. Mass. 2005).

419 Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 103 (2d. Cir. Conn. 2002).

discovery. Federal Rules of Civil Procedure 30(b)(6) requires a noticed organization to designate one or more persons to testify on its behalf regarding the subject matter identified in the areas of inquiry. Depending upon the facts of the case and the size of the corporation, these areas of inquiry can be extensive. The bottom line is that the testimony of this witness will bind the company and may be used for any purpose.

That witness not only has a duty to be knowledgeable on the subject matter of the inquiry, but also on subjects the entity should reasonably know as well. Once designated as the so-called "voice of the corporation," producing an unprepared witness is tantamount to a failure to appear, sanctionable under rule 37(d). Many companies have lost the confidence of the court and discovery because of producing an unprepared witness. An ineffective witness will open up Pandora's box and will cause defense counsel to start chasing ghosts instead of focusing on the merits of the case.

This witness is often called to testify on the steps the corporation took to find and produce responsive documents in order to ensure discovery was diligently completed in good faith. When called to provide sworn testimony on information management, document retention, and e-discovery issues, the witness must be prepared to testify on such topics as location of ESI, access to ESI, the way it is maintained, and how the data was preserved for the subject litigation.

Since the topics can cover a large number of areas of expertise--including qualifications and organizational structure, information systems, software and e-mail, records management, alternative sources of electronic information, legacy systems, backup and restoration procedures, production of ESI in other lawsuits--it may take more than one witness to give meaningful testimony, especially for large corporations.

An effective, repeatable and defendable e-discovery response plan requires an organization to proactively anticipate the type of discovery that could be initiated and develop an offensive strategy that employs both technology and human resources. Having the right witness(es) and investing in defensible technology has always been the lynchpin to the overall successful implementation of any litigation readiness plan.

Having the right people to tell the corporate e-discovery story is just as important as having the technology to identify, preserve, collect and process the ESI. A company needs both defendable technology and knowledgeable witnesses to respond to an e-discovery request. To that end, e-discovery has made the 30(b)(6) witness an invaluable tool for the requesting and responding parties.

§ 9.3.1 Employing a Reasonable and Defensible Process

A common thread throughout all aspects of e-discovery compliance is that a responding party must be able to convince the court that its electronic discovery process is thorough and reasonable under the circumstances. It is black-letter law that a party must take reasonable steps to preserve potentially relevant evidence when faced with pending litigation.

When discussing electronic data, many commentators have noted that a litigant must suspend its normal document retention practices, which may call for the intentional deletion of electronic data (or paper documents, for that matter) as part of the normal course of business. The court in *Zubulake* stated:

> The scope of a party's preservation obligation can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents.[420]

Unlike paper documents, however, a company that uses computers "destroys" electronic data, *whether or not it ceases the intentional deletion of files*. A computer will overwrite deleted files as part of its ordinary operation. Indeed, the simple act of turning on a computer can alter hundreds of files, including changing the metadata associated with files. As a result, the suspension of a party's document-retention policies will not suspend the "destruction" of electronic data. Indeed, when it comes to electronic data, a party should take immediate steps to *preserve* data that is potentially relevant to the litigation. In other words, a litigant must take affirmative steps to preserve electronic data that may be relevant to pending litigation.

Of course, it is not reasonable to assume that a litigant will stop using computers in the context of its business solely in order to preserve potentially relevant information. In the past, at the outset of litigation a litigant would often send an e-mail to employees, notifying them of the pending litigation. As highlighted above, however, this does not satisfy the litigant's preservation obligations; "[I]n short, it is *not* sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information."[421]

Fortunately, however, with the advent of EnCase Enterprise, technology is readily available to efficiently search and preserve electronic data contained on workstations, servers, and other types of computer systems, with minimal disruption to the litigant's business operations. For example, if a litigant becomes aware that litigation is likely to be commenced against it, it can use its network-enabled computer forensics capability to search its workstations and servers in order to identify the drives on which information regarding that vendor is located. Thus, a litigant can, at the outset of litigation, significantly narrow the scope of the universe of potentially relevant data, thereby saving time and money, while concretely meeting its preservation obligations.

By properly executing a litigation hold to preserve relevant electronic files, workstations or servers, a litigant can better defend any subsequent charges of spoliation of evidence (which arise frequently in the context of electronic evidence). Indeed, a litigant may be able to continue to operate its automatic deletion systems, provided it has first preserved the potentially relevant data.

An illustration of this point is *Peskoff v. Farber*,[422] in which the court heavily scrutinized the ESI preservation, search, and collection efforts employed by the defendant at the outset of the case. Finding an "explicit" duty under the new FRCP amendments to utilize reasonable efforts to search available electronic systems for potentially relevant ESI, the court faulted the defendant's prior effort as inadequate and insufficiently documented, and ordered the defendant to conduct a further search. Notably, the court scheduled a future hearing to review the adequacy of the ordered new search:

420 Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

421 Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004).

422 Peskoff v. Farber, 240 F.R.D. 26 (D.D.C. 2007).

> Once the search is completed . . . Defendant must also file a statement under oath by the person who conducts the search, explaining how the search was conducted, of which electronic depositories, and how it was designed to produce and did in fact produce all of the emails I have just described. I must insist that the person performing the search have the competence and skill to do so comprehensively. An evidentiary hearing will then be held, at which I expect the person who made the attestation to testify and explain how he or she conducted the search, his or her qualifications to conduct the search, and why I should find the search was adequate.[423]

Similarly, in *Wachtel v. Health Net, Inc*.,[424] the court found that "Health Net's process for responding to discovery requests was utterly inadequate . . . Health Net relied on the specified business people within the company to search and turn over whatever documents they thought were responsive, without verifying that the searches were sufficient."[425]

The court made clear that having a paralegal merely email preservation notifications is insufficient, noting that, "[d]espite the document hold, thousands of employees' emails failed to be searched." The court found that, "even when [defendant's] employees could search their emails, their searches were sporadic rather than systemic."[426] The court, concluding that these failings constituted bad faith, imposed harsh evidentiary and monetary sanctions.

In *Bd. of Regents of the Univ. of Nebraska v. BASF Corp.*[427], the defendant moved to impose sanctions against the plaintiff for violation of an earlier court order compelling document production. The defendant's request included full compliance by continued search and production of employee files, certification of full compliance by plaintiff, reproduction of witnesses for deposition, as well as reasonable fees and expenses. The record revealed that the plaintiff continued to produce documents after discovery deadline. Additionally, the plaintiff produced 6,000 pages following the deposition of the plaintiff's witnesses.[428] The plaintiff's witness did not receive a litigation-hold notice; rather, he was encouraged to review and eliminate as many files as he could.

The court determined that this, while not willful, was far from diligent. The court held that as the litigation was pending at the time of the destruction, bad faith was not required for sanctions and ordered the plaintiff to pay for all costs and expenses associated in re-deposing witnesses and the filing of this motion.[429] This shows how imperative it is to have an in-house research process to prevent these adverse effects.

In the *In re Seroquel* litigation, the plaintiffs urged the court to impose sanctions on the defendant for failing to timely comply with discovery obligations.[430] The plaintiffs pointed to a number of

423 Id. at 31.
424 Wachtel v. Health Net, Inc., 239 F.R.D. 81 (D.N.J . 2006).
425 Id. at 92.
426 Id. at 103.
427 No. 4:04CV3356, 2007 WL 3342423 (D. Neb. Nov. 5, 2007).
428 Id. at *3.
429 Id. at *5.
430 In re Seroquel Prods. Liab. Litig., 244 F.R.D. 650 (M.D. Fla. 2007).

instances where the defendant failed to produce documents in an accessible or useable format, in addition to missing many deadlines.

While the court found two of those instances to be excusably negligent, the other behavior warranted sanctions. The court was displeased with the defendant's failure to discuss keyword search terms with the plaintiffs, failure to include page breaks between documents it did produce, failure to produce usable single-page .TIFF documents, omission of attachments and relevant emails, and purposeful sluggishness in making an effective production.[431] The court stayed the determination of which sanctions to impose to allow the plaintiffs an opportunity to present evidence as to their damages or prejudice. The quote search offered by EnCase eDiscovery with keyword update for the user's preview would eliminate these errors by the defendant. It is no longer difficult to search and share information that formerly was difficult to display.

In contrast, a recent case that highlights the benefits of employing a defensible process is *Williams v. Massachusetts Mutual Life Insurance Company*,[432] in which the plaintiff alleged the existence of an email that "'spelled out' a policy or practice by MassMutual of using disciplinary actions as a pretext for terminating minority employees."[433] When MassMutual did not produce the email, plaintiff filed a motion seeking "to have the court appoint a 'neutral' forensic computer expert to inspect Defendants' computer hard drives and/or electronics communication system in an attempt to recover the . . . e-mail message which he claims exists."[434]

In refusing to order what the court described as "an intrusion into an opposing party's information system," the Court noted that MassMutual had already performed its own computer forensics search-and-collection effort in response to the litigation.[435] The affidavit that MassMutual had submitted in support of its response to plaintiff's motion stated in part as follows:

1. Robert Bell is a member of the team of information security professionals [at MassMutual]... Mr. Bell has performed over seventy-five (75) investigations using EnCase, the standard computer forensics software used by law enforcement and corporate security departments.

2. At the request of counsel for MassMutual, Mr. Bell . . . used EnCase to search the hard drives of all personal computers assigned by MassMutual to the [relevant MassMutual employees] from 2002 to the present, the e-mail boxes of [those employees] and relevant files on a local area network on which human resources personnel can store documents electronically.[436]

431 Id. at 663-65.
432 Williams v. Mass. Mut. Life Ins. Co., 226 F.R.D. 144,(D. Mass. 2005).
433 Id. at 145.
434 Id.
435 Id. at 146.
436 Affidavit of Bruce Bonsall, available electronically on the PACER system (http://pacer.psc.uscourts.gov).

In contrast to the responding party's position in the *MassMutual* case, the defendant in *Mudron v. Brown & Brown, Inc.*[437] found itself in the unenviable position of being forced to allow the plaintiff's computer forensic expert to access the defendant's computers.

The plaintiff "filed a motion for discovery sanctions and other relief alleging that he has been consistently denied electronic data."[438] The court ordered that the defendant, who had presumably not conducted a computer forensic examination itself, had to allow plaintiff's computer forensic expert to access defendant's "computer drives to obtain forensic images."[439]

The 2005 high-profile case between Morgan Stanley and Ron Perelman concerning the sale of Sunbeam to Coleman[440] graphically illustrates the perils of failing to employ a defensible electronic data collection and preservation approach. In this fraud case, Morgan Stanley collected electronic documents using software it had developed in-house, with dire consequences:

> [A Morgan Stanley employee] reported that ... she and her team had *discovered that a flaw in the software they had written* had prevented [Morgan Stanley] from locating all responsive e-mail attachments. [She also] reported that [Morgan Stanley] discovered... that the date-range searches for e-mail users who had a Lotus Notes platform were flawed, so there were at least 7,000 additional e-mail messages that appeared to fall within the scope of [existing orders]...[441]

The judge viewed Morgan Stanley's failures as intentional. As described on the front page of the *Wall Street Journal*:

> As a result of what she described as Morgan Stanley's "bad faith" actions, Judge Elizabeth Maass made an extraordinary legal decision: She told the jury it should simply assume the firm helped defraud Mr. Perelman.
>
> * * * * *
>
> Morgan Stanley is in serious trouble because of the way it mishandled an increasingly critical matter for companies: handing over email and other documents in legal battles. Lawsuits these days require companies to comb through electronic archives and are sometimes won or lost based on how the litigants perform these tasks.[442]

---

437 Mudron v. Brown & Brown, Inc., No. 03 C 8708, 2005 WL 645927 (N.D. Ill. Mar. 17, 2005).

438 Id. at *4.

439 Id. See also, Electrolux Home Prods., Inc. v. Whitesell Corp., No. 3:05-MC-017, 2006 WL 355453 (S.D. Ohio Feb. 15, 2006)(holding similar to Mudron).

440 Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., No. CA 03-5045 AI, 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005).

441 Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., No. 502003CA005045XXOCAI, 2005 WL 679071 at 4 (Fla. Cir. Ct. Mar. 1, 2005).

442 Susanne Craig, "How Morgan Stanley Botched a Big Case by Fumbling Emails," Wall Street Journal, May 16, 2005.

This decision was reversed on appeal.[443] However, the lesson of the *Morgan Stanley* case remains: using a "black-bag" approach that cannot be explained to the court and the other side–and hasn't been thoroughly tested or vetted in court–is unacceptable and unwise.

Another decision illustrating the importance of a defensible process, *Residential Funding Corp. vs. DeGeorge Financial,*[444] is a significant case in the area of computer evidence discovery. Residential Funding Corp (Residential) attempted to stave off its opponent's discovery request for production of computer evidence by citing the prohibitive expense and technical difficulties involved in producing the requested emails and other computer documents. Residential's own expert professed to the court that "technical problems" prevented the timely and cost-effective retrieval of sought computer data.[445]

The court, however, had no patience for Residential's obstruction, characterizing its conduct as "purposeful sluggishness," and dropped a judicial bombshell by further commenting that it was unreasonable for Residential to continue to employ the services of its electronic discovery expert, who admitted difficulty in getting the job done. The court granted DeGeorge's expert access to Residential's network, including desktops and backup tapes, and imposed harsh monetary sanctions, as well as allowing the trial court to impose evidentiary sanctions against Residential for its bad-faith conduct.[446]

The *Residential* decision clearly illustrates that the alleged burden of computer evidence discovery is no longer a shield to compliance, and that permitting computer evidence to be destroyed can lead to sanctions or the drawing of an adverse inference. A federal magistrate judge noted, in a class-action sexual harassment case, that the defendant:

> "…had a duty to preserve the computer hard drives, e-mail accounts, and internet records of anyone who left the company who had been accused (formally or informally) of sexual harassment or misconduct. Or, if this were cost prohibitive, it could have searched the computer for sexually inappropriate or otherwise offensive material before destroying the other data it contained and reusing the computer."[447]

Thus, courts are now assuming that the technical means are available to litigants to engage in systemized computer evidence preservation, retrieval, and analysis. For example, the court in the *Residential Funding* case had no patience for the "purposeful sluggishness" of Residential's e-discovery compliance efforts. Similarly, in *In re Search of: 3817 W. West End,* the Court highlighted the growing lack of judicial patience for unprepared or incompetent e-discovery "experts":

> When the Court raised the possibility of limiting the search to certain time periods, one of the government representatives stated that such a limitation would not be helpful since the file directory only shows when a document was last saved. The Court then asked the government technical expert whether that problem could not

443 Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co. Inc., 973 So. 2d 1120 (Fla. Dec. 12, 2007)

444 Residential Funding Corp. v. DeGeorge Fin. Corp.,306 F.3d 99 (2d Cir. Conn. 2002).

445 Id. at 103.

446 Id. at 113.

447 Wiginton v. CB Richard Ellis, 2003 WL 22439865 at *5 (N.D. Ill. Oct. 27, 2003).

> be overcome by examining the "metadata" in the computer files, which would show not only the date a document was last saved, but also when the document was first created and (often times) the changes in the documents from the original draft to the final revision. The government technical expert made no response, leaving the Court with the firm impression that he was not familiar with a term that we would expect a computer expert to know.[448]

In another case, the court ordered an examination of hard drives and even suggested specific search terms and time parameters.[449] Several other courts have similarly issued decisions requiring expedient and full compliance with computer evidence discovery requests.[450]

Moreover, courts continue to severely punish litigants who fail to preserve and/or alter computer evidence when a lawsuit is pending. *Metropolitan Opera Association v. Local 100, Hotel Employees & Restaurant Employees International Union,*[451] is one in a line of unequivocal cases that impose harsh penalties upon parties who fail to preserve computer evidence. In *Metropolitan Opera*, the court, in effect, ordered a case-ending finding of liability as a litigation penalty after determining that the defendants improperly destroyed computer evidence in bad faith.[452]

Indeed, as these cases and the *Kucala* case [453](see Chapter 6) reveal, courts are increasingly likely to enter a judgment in favor of the other party based upon the failure to preserve evidence while litigation is pending, whether that failure is attributable to the party, the party's expert, negligence, or intentional conduct.

In perhaps the most notable case to discuss the failure of a party to employ a reasonable e-discovery process, *Qualcomm Inc. v. Broadcom Corp.,*[454] the court ordered the plaintiff, Qualcomm, to pay over $9 million in attorney's fees and costs to Broadcom due to Qualcomm's total failure to provide relevant information during discovery. In addition, the court ruled that Qualcomm's two patents were unenforceable, and also referred six of Qualcomm's attorneys to the State Bar for their conduct during the discovery proceedings.[455]

At issue in the case was whether Qualcomm had participated in an industry group called the Joint Video Team, ("JVT"), prior to 2003; if Qualcomm had participated in JVT, they were barred from

448 In re Search of: 3817 W. West End, 321 F.Supp.2d 953 at n.1 (internal citations and quotations omitted).

449 United States v. Andreozzi, 60 M.J. 727, 747 (A.C.C.A. 2004), in which the Court's Order specified that "the computer hard drives of Captain Travis . . . will be examined . . . Suggested examination time parameter should include from 1 April 1998 to 10 June 1998. Suggested examination terms are 'andreozzi' and 'enlisted,' or 'andreaozzi' and 'forum.'"

450 Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645 (D. Minn. 2002); Tulip Computers Int'l B.V. v. Dell Computer Corp., 52 Fed. R. Serv. 3d 1420 (D. Del. 2002).

451 212 F.R.D. 178 (S.D.N.Y. 2003).

452 Id. at 231.

453 Kucala Enters. v. Auto Wax Co., 56 Fed. R. Serv. 3d (N.D. Ill. 2003).

454 539 F.Supp.2d 1214 (S.D. Cal. 2007).

455 GC California, June 2008, "Hard Lessons: What in-house counsel should learn from Qualcomm's e-discovery disaster." (Summary of Qualcomm, Inc. v. Broadcom Corp., and Qualcomm's e-discovery fiasco which resulted in paying over $9 million to Broadcom in attorney fees; also features lessons in-house counsel can take from the case.)

enforcing the very patents upon which they were now suing Broadcom, but if they had not participated in the JVT group, Qualcomm could enforce their patents against Broadcom.[456]

Broadcom contended that Qualcomm was an active participant in the JVT prior to the release of the H.264 video standard (a video standard related to the two patents Qualcomm sought to enforce), which would have made Qualcomm's two patents unenforceable. Qualcomm, on the other hand, adamantly asserted that they did not participate in the JVT until after the H.264 standard was released, in 2003. Broadcom sought discovery of ESI and documents related to "JVT," "H.264," and an e-mail list server used by the JVT, "avc_ce." Qualcomm asserted numerous times to opposing counsel, the Magistrate Judge, the District Judge, and the jury that there were no documents proving Qualcomm's participation in JVT prior to 2003; in fact, Qualcomm submitted an expert declaration, signed by both inside and outside counsel, confirming the absence of any corporate records relating to Qualcomm's participation in JVT prior to 2003.[457]

Unfortunately for Qualcomm and its attorneys, there were numerous documents linking Qualcomm to JVT prior to 2003. In fact, there were over 46,000 documents and e-mails linking Qualcomm to JVT as early as January 2002.[458] Evidence presented at the sanctions hearing failed to reveal that Qualcomm had even used basic search terms, like "JVT" and "H.264," in its search for relevant documents.[459] Further, Qualcomm and its attorneys fought aggressively over virtually every discovery request by Broadcom: Qualcomm argued phrases like "participation and/or involvement" and "standard" were vague and overly burdensome.[460] District Judge Rudi Brewster explained that Qualcomm's attorneys had "adamantly denied the obvious and then, when the truth was discovered and exposed by the document production, sequentially contended denial of relevance, justification, mistake, and finally non-awareness."[461]

Magistrate Judge Barbara Major explained how such a colossal failure of the discovery process might have occurred: "one or more of the retained lawyers chose not to look in the correct locations for the correct documents, to accept the unsubstantiated assurances of an important client that its search was sufficient, to ignore the warning signs that the document search and production were inadequate, not to press Qualcomm employees for the truth, and/or to encourage employees to provide the information (or lack of information) that Qualcomm needed to assert its non-participation argument and to succeed in this lawsuit."[462]

Despite Judge Major's castigation of Qualcomm's attorneys including referral of the six attorneys to the State Bar, it is ultimately Qualcomm that is responsible for paying out the more than $9 million in attorney's fees due to its failure to maintain a defensible and reasonable discovery process. The *Qualcomm* case makes it clear that companies can't simply hand off the work of e-discovery to their outside counsel. They have to oversee it and they have to be involved because ultimately they are liable.

456 Id.
457 Id.
458 Id.
459 Qualcomm Inc. v. Broadcom Corp., 2008 WL 66932 at *10 (S.D. Cal. Jan. 7, 2008).
460 Id.
461 Qualcomm Inc. v. Broadcom Corp., 539 F. Supp. 2d 1214, 1228 (S.D. Cal. 2007).
462 Qualcomm Inc., 2008 WL 66932 at *13.

Qualcomm made every effort to distance itself from the discovery gaffes and to place the blame on the attorneys. The declarations that Qualcomm filed based on witnesses and a paralegal, fault outside counsel, saying they were responsible for deciding whose documents got searched and that they didn't ask the right questions. Judge Major, however, wasn't moved, noting that "Qualcomm is a large corporation with an extensive legal staff; it clearly had the ability to identify the correct witnesses and determine the correct computers to search and the search terms to use."[463]

Baker Hughes Inc. v. Homa[464] is an example where the court pressed the discovery respondents to document a defensible process for their collections. The case involved an alleged breach of non-disclosure and non-solicitation agreements by former employees of plaintiff, an oil-field service company that had developed fiber-optic sensing fibers. According to the complaint, defendants had formed a relationship with a group of Austrian firms and illicitly worked with them to compete with plaintiff in the fiber optic business. After submission of proposed discovery orders, the court ordered that defendants "must electronically search all email accounts" of certain identified custodians "using the search terms and instructions" filed by plaintiff; "must" produce emails as .pst files; and "must file a status report," providing the details of their search. The court directed that the status report provide details as to:

- Computers or servers searched
- Custodians whose e-mail accounts were searched
- Description of the system from which the e-mails were produced
- Time periods searched
- Dates and categories of e-mails that could not be produced
- Description of e-mails or attachments that had been discarded, destroyed, or deleted

These cases establish that the best way for enterprises responding to computer discovery to demonstrate compliance and mitigate risk is to implement a reasonable and defensible protocol to comply with subpoenas for production of relevant data and to properly preserve and acquire evidence. Courts will grant an enterprise the opportunity to produce the requested information themselves, but only if they demonstrate technical and organizational competence by having the appropriate resources and court-validated technology employed and in place. If not, the dilatory enterprise may find itself subject to a broad and highly intrusive court-ordered discovery conducted by the opponent and possibly subject to other court sanctions.

§ 9.4 The Sedona Conference® Cooperation Proclamation

The Sedona Conference Cooperation Proclamation has been endorsed by state and federal judges since July 2008. It calls for open and forthright information sharing during civil discoveries. Under

463 GC California, June 2008, "Hard Lessons: What in-house counsel should learn from Qualcomm's e-discovery disaster."

464 2013 WL 684699 (S.D. Tex. Feb. 25, 2013).

the proclamation, lawyers have twin duties of loyalty: to zealously advocate for their clients and to professionally conduct discovery in a diligent and candid manner.

As the Cooperation Proclamation becomes more widely endorsed, judges become more likely to require attorneys to confer and discuss discovery strategy early in the trial and in a good-faith manner, and impose sanctions to punish and deter lawyers who fail to cooperate in the discovery process.

For example, in *Covad Comm. Co. v. Revonet, Inc.*,[465] the plaintiff's boiler plate discovery request instructions did not specify the format in which it wanted the defendant to produce its e-mails. The defendant produced the e-mails first in hard copy and then in .TIFF format. Not satisfied by either format, the plaintiff moved to compel the defendant to reproduce the e-mails in native format. Finding the lawyers on both sides failed to facilitate the discovery process efficiently, Judge Facciola commented that "…the courts have reached the limits of their patience with having to resolve electronic discovery controversies that are expensive, time consuming, and so easily avoided by the lawyers' conferring with each other on such a fundamental question as the format of their productions of electronically stored information." [466]The court then ordered the defendant to produce the requested information in native format on a CD and have the plaintiff incur half of the privilege review cost.

In addition to implicitly ratifying the communication principles of the Sedona Conference, in reaching the decision, the court relied on the Sedona Conference for a definition of "native format" and cited the *Aguilar v. Immigrations and Customs Enforcement Div. of the US Dep't of Homeland Sec.* case, which approvingly quoted statements from the Cooperation Proclamation.[467]

Judge Grimm also commented on the importance of cooperation between the parties in *Mancia v. Mayflower Textile Services Company,*[468] stating that "courts repeatedly have noted the need for attorneys to work cooperatively to conduct electronic discovery, and sanctioned lawyers and parties for failing to do so…"[469] and "[D]iscovery must be initiated and responded to responsibly, in accordance with the letter and spirit of the discovery rules, to achieve a proper purpose, and be proportional to what is at issue in the litigation, and if it is not, the judge is expected to impose appropriate sanctions to punish and deter."[470] In the opinion, Judge Grimm approvingly noted the efforts of the Sedona Conference and called it, "a thoughtful means to engage all the stakeholders in the litigation process—lawyers, judges and the public at large—and provide them with the encouragement, means and incentive to approach discovery in a different way."[471]

The Sedona Conference Cooperation Proclamation continues to gain widespread endorsement. In *William A. Gross Construction Associates, Inc.* (discussed in more detail in §9.8 infra) the court had this to say in the context of keyword searches: "[o]f course, the best solution in the entire area

465 254 F.R.D. 147 (D.D.C. 2008).
466 Id. at 151.
467 Id. at 148-49.
468 253 F.R.D. 354 (D. Md. 2008).
469 Id. at 361.
470 Id. at 360.
471 Id. at 363.

of electronic discovery is cooperation among counsel. This court strongly endorses *The Sedona Conference Cooperation Proclamation*."[472]

In *Cartel Asset Management v. Ocwen Financial Corp.*,[473] counsel pushed the court to the limit in discovery disputes. Citing the no less than eleven conferences or hearings on discovery-related matters and rulings on innumerable discovery motions, the court takes stock of the current state of civil litigation with the advent of expansive e-discovery, and comments that it "has become too expensive and too protracted to permit superficial compliance with the 'meet and confer' requirements . . . This court is left with the impression that counsel are searching for discovery disputes, rather than working cooperatively to avoid or defuse those disagreements... This court has endorsed The Sedona Conference Cooperation Proclamation... and its call for 'cooperative, collaborative, [and] transparent discovery.' "[474]

With increasing number of courts requiring pre-trial conferences to discuss the scope and procedure of e-discovery, the ability to assess and estimate costs of production early becomes essential for a producing party to justify its cost-shifting request. For example, in *Mikron Industries, Inc. v. Hurd Windows & Doors, Inc.*,[475] the court denied the producing party's cost-shifting request because the party failed to offer evidence showing that the cost to produce the requested ESI was excessive.[476]

Similarly, the court in *Peskoff v. Faber* [477] declined to shift $33,000 in production cost when it found that there was no undue burden and the producing party was unwilling to take the discovery obligation seriously.[478] (EnCase offers a way to rapidly assess the size of data to be produced, and by inference, the cost of production, before a full-blown search is performed.)

§ 9.5 Preservation / Spoliation

Preservation is the first step in the e-discovery workflow; the success of the entire process depends on its proper execution. As long as counsel preserves all potentially relevant ESI, they will be able to execute all downstream processes, such as identification, review, and production. However, failure to preserve ESI in a timely manner creates a risk that evidence may be lost. Courts refer to this as "spoliation." When spoliation occurs, a court may issue sanctions depending on the egregiousness of the data loss.

In *Wm. T. Thompson Co. v. General Nutrition Corp.*[479], the court noted the duty to preserve evidence begins when one is "on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible

472 William A. Gross Construction Associates, Inc., 256 F.R.D. 134, 136 (S.D.N.Y. 2009).
473 No. 01-CV-01644-REB-CBS, 2010 WL 502721 (D. Colo. Feb. 8, 2010).
474 Id. at 13.
475 No. C07-532RSL, 2008 WL 1805727 (W.D.Wash. Apr. 21, 2008).
476 Id. at *2.
477 Peskoff v. Faber, 251 F.R.D. 59 (D.D.C. 2008).
478 Id. at 62-63.
479 593 F. Supp. 1443 (C.D. Cal. 1984).

evidence."[480] And, once the duty is triggered, one must "preserve what it knows, or reasonably should know, is relevant to the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request." [481]

Failure to satisfy a party's preservation obligations can lead directly to sanctions. Courts are unequivocal in their response to clear evidence that a party intentionally destroyed evidence. For example, in *Keithley v. Homestore.com, Inc.*,[482] a patent infringement claim, the court imposed monetary sanctions in the form of attorney's fees and expert's costs because plaintiff engaged in a large-scale transfer of source code after its duty to preserve evidence was triggered. Because the source code--evidence subject to the duty to preserve--was modified, i.e. destroyed, by the transfer, the court held defendant responsible for the spoliation.[483] In addition, the sanctions were also justified for failure to produce reports as directed by an order and for failure to have a litigation hold and document retention policy in place.[484] The court imposed monetary sanctions on the defendants in an amount over $250,000.

Further, in *Columbia Pictures v. Bunnell*,[485] the plaintiffs claimed the defendants willfully deleted and modified user forums to remove mention of copyrighted material, and sought default judgment sanctions based on the defendants' spoliation of evidence.

The court set forth five factors to consider when deciding whether to enter default judgment: 1) expeditious resolution of litigation; 2) the court's docket management; 3) risk of prejudice; 4) public policy in deciding cases on their merits; and 5) the availability of lesser sanctions.[486] The court found the defendants engaged in efforts to destroy evidence and provided false testimony under oath. Considering lesser sanctions, the court concluded the prejudice suffered was too great to overcome with an adverse jury instruction. The court also noted past monetary sanctions imposed upon the defendants were clearly ineffective and granted the motion for a default judgment in favor of the plaintiffs.[487]

In *So. New England Telephone Co. v. Global NAPs, Inc.*[488], the court granted the plaintiff's motion for prejudgment remedy, and ordered defendant Global to produce accounting and business records. Over the next two years, defendant Global failed to produce the requested record.[489] The court found defendant Global's continuous failure to produce evidence willful. Moreover, it found that Global intentionally lied to court about its inability to obtain records from third parties, and destroyed

480 Id. at 1455.
481 Id.
482 629 F. Supp. 2d 972 (N.D. Cal. 2008).
483 Id. at 975.
484 Id. at 977.
485 Columbia Pictures, Inc. v. Bunnell, No. 2:06-CV-01093 FMC-JCX, 2007 WL 4877701 (C.D. Cal. Dec. 13, 2007).
486 Id. at *5.
487 Id. at *7-8.
488 S. New Eng. Tel. Co. v. Global NAPs, Inc., 251 F.R.D. 82 (D. Conn. 2008).
489 Id. at 86.

evidence that was relevant to discovery. As a result, the court granted default judgment to the plaintiff in an amount over $5 million.[490]

In *AdvantaCare Health Partners, L.P. v. Access IV,*[491] Gary Dangerfield and Gwen Porter were employees of AdvantaCare who resigned and began a competing business called Access IV. AdvantaCare then hired a computer forensics expert who "determined that Dangerfield had accessed AdvantaCare's computer network and copied a large number of AdvantaCare's files prior to leaving, including files containing company policies and procedures, patient databases, employee lists, and contracts. The forensic [expert] also determined that Dangerfield tried to conceal his copying activities by deleting copied files from his hard drive."[492]

Shortly thereafter, the Court entered a temporary restraining order that prohibited the defendants from using, copying, or destroying any AdvantaCare data, and that required the defendants to permit AdvantaCare to make forensic copies of the hard drives and network servers of Access IV.[493] The court described the defendants' response to the temporary restraining order:

> [The defendants] were served with a copy of the TRO . . . at 4:20 pm on October 6, 2003. Early that evening, Dangerfield visited numerous websites, searching for computer data deletion software. At 9:00 pm, Dangerfield upgraded to BC Wipe, one of the strongest computer file deletion programs available. Between October 7, 2003 and October 10, 2003, Dangerfield deleted more than thirteen thousand files from his home computer using BC Wipe.[494]

Even after this activity was uncovered, the defendants failed to comply with the temporary restraining order, or with agreements they had made with plaintiffs promising to delete AdvantaCare data. The Court entered evidentiary sanctions, ordering that "the trier of fact shall find that Defendants copied all of the files on Plaintiffs' computers" and awarded monetary sanctions of $20,000.[495]

Kucala Enterprises, Ltd. v. Auto Wax Co., Inc., discussed in Chapter 6, likewise involved intentional evidence destruction. Similarly, in the fifth opinion issued in the *Zubulake* line of cases (described more fully in Section 9.4), the Court noted that:

> UBS personnel unquestionably deleted relevant e-mails from their computers after August 2001, even though they had received at least two directions from counsel not to. Some of those e-mails were recovered (Zubulake has pointed to at least 45), but some—and no one can say how many—were not. And even those e-mails that were recovered were produced to Zubulake well after she originally asked for them.[496]

490 Id. at 96.
491 2004 WL 1837997 (N.D. Cal. Aug. 17, 2004).
492 Id. at *1.
493 Id.
494 Id. at *2.
495 Id. at *11.
496 Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 429 (S.D.N.Y. 2004).

As a result, the court issued a negative inference jury instruction, and ordered the defendant to pay the costs of any re-depositions of witnesses necessitated by the defendant's late production of responsive documents.[497]

A federal district court in the District of Columbia addressed spoliation in *United States v. Philip Morris USA, Inc.*[498] The court described the situation as follows:

> [On October 10, 1999, the Court issued an order] requiring preservation of "all documents and other records containing information which could be potentially relevant to the subject matter of this litigation." Despite this Order, Defendants Philip Morris and Altria Group deleted electronic mail ("email") which was over sixty days old, on a monthly system wide basis for a period of at least two years after October 19, 1999. In February, 2002, Defendants became aware that there was inadequate compliance with [the Court's order], as well as its own internal document retention policies, and that some emails relevant to this lawsuit were, in all likelihood, lost or destroyed. It was not until June 19, 2002, four months after learning about this serious situation, that Philip Morris notified the Court and the Government. Moreover, despite learning of the problem in February 2002, Philip Morris continued its monthly deletions of email in February and March of 2002.[499]

The court found that the defendant failed to comply with its order and accordingly, imposed the following sanctions: the court precluded the eleven individuals who failed to comply with the Philip Morris document retention program from testifying in any capacity at trial; the court ordered each of the eleven to pay $250,000; and the court ordered Philip Morris to pay $2,750,000.[500] This case highlights the seriousness with which courts are addressing failures to meet preservation obligations with respect to electronic documents and data.

In *MasterCard International, Inc. v. Moulton*,[501] MasterCard had sued the defendants for copyright and trademark infringement. In the four months following the filing of the lawsuit, the defendants failed to take any steps to preserve potentially relevant e-mails, and instead continued deleting e-mails after twenty-one days in accord with their existing practice. These actions were undertaken despite reminders of the duty to preserve.[502] The court noted the following:

> [W]e are not persuaded that defendants acted in bad faith, that is, for the express purpose of obstructing litigation. They appear simply to have persevered in their normal document retention practices, in disregard of their discovery obligations. The absence of bad faith, however, does not protect defendants from appropriate sanctions,

497 Id. at 437.
498 327 F. Supp. 2d 21 (D.D.C. 2004).
499 Id. at 23-24.
500 Id. at 26.
501 No. 03 Civ. 3613 VMMHD, 2004 WL 1393992 (S.D.N.Y. June 22, 2004).
502 Id. at *3-4.

> since even simple negligence is a sufficiently culpable state of mind to justify a finding of spoliation.[503]

Despite not finding intentional destruction, the court recognized spoliation because defendant's gross negligence led to the destruction of the potentially relevant information. While there was no monetary sanction, the court imposed a significant sanction by allowing the spoliation itself to serve as the basis of an inference of confusion to the public and tarnishment of the trademark.[504]

Another ruling in a shareholder class action case, *Nursing Home Pension Fund v. Oracle Corp.,* further demonstrates the sanctions available to courts when a party fails to comply with e-discovery requests.[505] In the *Oracle* case, US District Judge Susan Illston ruled that Oracle destroyed or failed to preserve CEO Larry Ellison's e-mails sought as evidence of false statements made about the company's financial condition and about the functionality of the Oracle 11i suite in 2001.[506]

Judge Illston also ruled that Oracle improperly failed to produce tapes and transcripts from interviews that a journalist conducted with Ellison in 2001 and 2002 as he gathered material to write "Softwar," a biography of Ellison. Judge Illston found the tapes had been held by the author, Matthew Symonds, who had them destroyed in late 2006 or early 2007. Judge Illston determined that Oracle should have found a way to preserve the information and comply with the discovery order because Ellison knew about the litigation when most of the interviews were conducted. [507]

Judge Illston imposed an adverse influence sanction as to the contents of Ellison's e-mails and the interviews. The adverse influence sanction allows a jury to infer that the spoliated evidence was against the party who failed to produce it.

Once a person or organization has notice of an action, they must be proactive in preserving evidence and modify any inconsistent document-retention policies or automated deletion systems. In *Mosaid Technologies Inc. v. Samsung Electronics Co. Ltd.,*[508] the court imposed a "spoliation inference"[509] and monetary sanctions against Samsung for destruction of electronic data. The court described the case as follows:

> [A]fter the inception of this litigation in September 2001, Samsung never placed a "litigation hold" or "off switch" on its document retention policy concerning email. Unchecked, Samsung's automatic computer e-mail policy allowed e-mails to be deleted, or at least to become inaccessible, on a rolling basis. As a result, Samsung failed to produce a single technical e-mail in this highly technical patent litigation because none had been preserved.

503 Id. at *4.
504 Id. at *5.
505 Nursing Home Pension Fund v. Oracle Corp., 254 F.R.D.559 (N.D. Cal. 2008).
506 Id. at 565.
507 Id. at 566-67.
508 Mosaid Techs. Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332 (D.N.J. 2004).
509 A "spoliation inference" is an adverse inference that permits a jury to infer that "destroyed evidence might or would have been unfavorable to the position of the offending party." Id. at 336 (citing Scott v. IBM Corp., 196 F.R.D. 233, 248 (D.N.J. 2000)).

* * * * *

> The duty to preserve potentially relevant evidence is an affirmative obligation that a party may not shirk. *When the duty to preserve is triggered, it cannot be a defense to a spoliation claim that the party inadvertently failed to place a "litigation hold" or "off switch" on its document retention policy to stop the destruction of that evidence.* As discoverable information becomes progressively digital, e-discovery, including e-mails and other electronic documents, plays a larger, more crucial role in litigation. In this district, in October 2003, Local Civil Rule 26.1 was amended to include a section concerning discovery of digital information. *See* L. Civ. R. 26.1(d). Among other things, that rule requires counsel to investigate how a client's computers store digital information, to review with the client potentially discoverable evidence, and to raise the topic of e-discovery at the Rule 26(f) conference, including preservation and production of digital information. *Unless and until parties agree not to pursue e-discovery, the parties have an obligation to preserve potentially relevant digital information. Parties who fail to comply with that obligation do so at the risk of facing spoliation sanctions.*[510]

Of course, there is nothing wrong with having a data-retention policy or automated e-mail deletion. However, once the duty to preserve attaches, the party must preserve all potentially relevant documents. As stated by the court in *Mosaid Technologies*, "[t]he duty to preserve potentially relevant evidence is an affirmative obligation that a party may not shirk."[511]

The often-overlooked crucial point is that it is *only* potentially relevant data that need be preserved. Irrelevant information need not be kept. In *Tantivy Communications, Inc. v. Lucent Technologies Inc.*, the court described discovery obligations as follows: "[t]he party and its counsel should ensure that (1) all sources of relevant information are discovered, (2) relevant information is retained on a continuing basis, and (3) relevant non-privileged material is produced to the opposing party."[512] Again, irrelevant information plays no part in discovery. Using EnCase Enterprise software, a litigant can search for and preserve the potentially relevant data in a secure container (known as a Logical Evidence File), thereby satisfying its preservation obligation. Having satisfied the criteria laid out in *Tantivy,* the litigant can arguably continue its normal document-destruction processes.

The court in *Broccoli v. Echostar Communications Corp.*[513], described an aggressive document-destruction process:

> Under Echostar's extraordinary email/document retention policy, the email system automatically sends all items in the user's "sent items" folder over seven days old to

510 Id. at 333, 339-40 (emphasis added).

511 Id. at 333.

512 Tantivy Commc'ns. Inc. v. Lucent Techs. Inc., No. Civ.A.2 :04CV79 (TJW), 2005 WL 2860976 at *2 (E.D. Tex. Nov. 1, 2005).

513 Broccoli v. Echostar Commc'ns. Corp., 229 F.R.D. 506 (D. Md. 2005).

> the user's "deleted items" folder, and all items in a user's "deleted items" folder over 14 days old are then automatically purged from the user's "deleted items" folder. The user's purged emails are not recorded or stored in any back up files. Thus, when 21-day-old emails are purged, they are forever irretrievable. The electronic files, including the contents of all folders, sub-folders, and all email folders, of former employees are also completely deleted 30 days after the employee leaves Echostar.[514]

In this case, the court found that Echostar's preservation obligations attached as early as January 2001, but that Echostar did nothing to preserve potentially relevant data. The court had little patience for this approach:

> Given Echostar's status as a large public corporation with ample financial resources, the court finds it indefensible that . . . basic personnel procedures and related documentation were lacking . . . [Echostar was] guilty of gross spoliation of evidence.[515]

Clearly, the court's statement about Echostar's size and resources demonstrates that courts will consider the relative sophistication and resources of parties when assessing compliance with discovery obligations.

Despite the courts' efforts to curb discovery abuses through sanctions and adverse inference orders, and despite efforts by organizations such as the Sedona Conference to guide parties to an amicable discovery phase through issuance of its Cooperation Proclamation, sanctions cases continue to proliferate.

The court in *In re A&M Florida Properties* sanctioned both the plaintiff and its counsel for their failure to timely produce requested e-mails that were not located merely due to a misunderstanding of the plaintiffs' e-mail retention procedures. The court noted that, while neither of the sanctioned parties acted in bad faith, outside counsel "simply did not understand the technical depths to which electronic discovery can sometimes go." Ultimately the e-mails in dispute were located and produced to defendant, leading the court to grant the monetary sanctions order on the basis that plaintiff's counsel had an obligation to "not just request documents of his client, but to search for sources of information."[516]

Two recent cases discussed more fully in § 9.6 below stand out as the most influential cases concerning the evolving litigation hold-preservation-spoliation-sanctions continuum. See, *Pension Committee of University of Montreal v. Banc of America Securities* and *Rimkus Consulting Group, Inc. v. Cammarata*. Read together, the cases are a primer for organizations, counsel, and courts for addressing discovery misconduct and the issuance of adverse-inference instructions.

In *Am. Nat'l Prop. & Cas. Co. v. Campbell Ins., Inc.*,[517] the court denied plaintiff's Motion for Sanctions for Spoliation of Evidence as untimely, citing the facts that it had been 14 months since the

514 Id. at 510.

515 Id. at 512 (internal quotations omitted).

516 No. 09-15173 (AJG), 2010 WL 1418861 at *6 (Bankr..S.D.N.Y. Apr. 7, 2010).

517 No. 3:08-cv-00604, 2011 WL 3021399 (M.D. Tenn. July 22, 2011).

alleged spoliation was discovered, that discovery had already closed, and that trial was weeks away. In so deciding, the court relied heavily on the summary of the law regarding the timeliness of spoliation motions as delineated in Goodman v. Praxair Servs., Inc., 632 F. Supp. 2d 494 (D. Md. 2009).

In *E.I. Du Pont De Nemours & Co. v. Kolon Indus., Inc.*,[518] the court acknowledged defendant's issuance of litigation holds, but found that key employees had intentionally deleted evidence in bad faith. Thus, the court imposed sanctions of an adverse jury instruction and an order that defendant pay plaintiff's attorney's fees, costs, and expenses. Furthermore, the court specifically rejected the argument that because many deleted documents were recovered or located elsewhere, no spoliation occurred. It ruled that alteration is spoliation, that deletion alters the format of the evidence, and that "hence, upon deletion, electronically stored information is spoliated."

In *PIC Group, Inc. v. LandCoast Insulation, Inc.*,[519] a Mississippi court imposed multiple requirements upon defendant for spoliation. For discovery failures, including failure to timely identify relevant materials and spoliation, the court ordered discovery re-opened for a limited purpose, that defendant pay plaintiff's attorney's fees and costs related to the discovery failures, that defendant produce all ESI present on an intentionally wiped hard drive (save attorney-client privileged or settlement-related materials), that defendant pay all fees and costs of the Special Master, and that defendant be prohibited from seeking indemnification for such sanctions from its insurer.

In *Rattray v. Woodbury County*,[520] defendants failed to copy all of a video tape and thus lost a relevant portion as the result of it being automatically overwritten pursuant to a document-retention policy. The court ordered that the jury be allowed to consider whether a portion of the video was destroyed in bad faith and to infer that such evidence would have been unfavorable to defendants. Regarding a requisite showing of prejudice, the court cited that the tape was the only recording of what happened as an "important factor," which "weighs heavier in this case than the lack of actual knowledge that litigation was imminent at the time of the destruction."

In *Siani v. State Univ. of New York at Farmingdale*,[521] the court found defendants merely negligent in their preservation efforts for failing to suspend certain routine file-destruction procedures and for deleting some relevant ESI. The court declined to infer relevance without a finding of bad faith, and determined that plaintiff had produced no extrinsic evidence demonstrating that the missing evidence would have been favorable, and thus declined to impose an adverse inference. The District Court declined to modify or set aside the order, 2011 WL 2580361 (E.D.N.Y. June 28, 2011).

In *United Cent. Bank v. Kanan Fashions, Inc.*,[522] where defendants arranged for the sale (or fabricated the sale) of a server containing relevant information and, when asked, repeatedly assured their attorneys that appropriate preservation efforts were being undertaken, the court found that defendants' spoliation was willful and in bad faith, and ordered monetary sanctions and an adverse

518 No. 3:09-cv58, 2011 WL 2966862 (E.D. Va. July 21, 2011).
519 No. 1:09-CV-662-KS-MTP, 2011 WL 2669144 (S.D. Miss. July 7, 2011).
520 2010 WL 5437255 (N.D. Iowa Dec. 27, 2010).
521 2010 WL 3170664 (E.D.N.Y. Aug. 10, 2010).
522 No. 10 C 331, 2011 WL 4396856 (N.D. Ill. Sept. 21, 2011).

inference. However, the court declined to sanction counsel, who was unaware of what was "going on behind the scenes."

In *Apple, Inc. v. Samsung Elecs. Co. Ltd.*,[523] the court sanctioned defendant for the loss of relevant emails resulting from defendant's failure to halt the auto-delete feature of its proprietary email system. It also cited defendant's failure to appropriately follow up with employees subject to the litigation hold to ensure compliance. As a sanction, the court ordered an adverse inference sanction, allowing the jury to presume that the evidence lost was both relevant and favorable to the plaintiff.

In *Taylor v. Mitre Corp.*[524], the district court dismissed plaintiff's claims and ordered plaintiff to pay defendant's reasonable attorney's fees and costs, based on a finding of intentional spoliation, including physical destruction of a relevant computer and the use of an evidence eliminator and "CCleaner." No punitive monetary sanctions were levied.

Finally, the case of *Tener v. Cremer*,[525] illustrates the growing scope of preservation obligations, in that case imposed upon a non-party. In *Tener*, the appellate court (First Department) addressed "the obligation of a nonparty to produce ESI deleted through normal business operations," and reversed and remanded the order of the motion court which had declined to compel the non-party to attempt recovery of the data.[526] The plaintiff served a subpoena and hold notice on a non-party medical center a year after the litigation commenced seeking the identity of all persons who accessed the internet on a certain day through a specific IP address, in order to obtain discovery relating to alleged online defamation. However, the medical center's normal business processes caused such information to be deleted on a thirty day cycle. In support of plaintiff's motion, its expert opined that the data could be recovered through the use of forensic software. The motion court denied plaintiff's motion, adopting the non-party medical center's arguments that and "it could not, as a non-party, be required to install forensic software on its system." In reversing and remanding, the First Department held that because "good cause" the lower court should have engaged in a cost-benefit analysis "to determine whether the needs of the case warrant retrieval of the data." Specifically, the appellate court remanded for a hearing on:

1. whether the identifying information was written over, as [the nonparty] maintains, or whether it is somewhere else, such as in unallocated space as a text file;
2. whether the retrieval software plaintiff suggested can actually obtain the data;

---

523 No. C 11-1846 LHK (PSG) (N.D. Cal. July 25, 2012).

524 2012 WL 5473573 No. 1:11-cv-01247 (LO/IDD), (E.D. Va. Nov. 8, 2012) adopting recommendations of Taylor v. Mitre Corp., No. 1:11-cv-01247 (LO/IDD), 2012 WL 5473715 (E.D. Va. Sept. 10, 2012). Upon order of the court, plaintiffs laptop computer was ordered to be made available for forensic inspection. The vendor investigating Plaintiff's hard drive used EnCase, which revealed a considerable amount of evidence of Plaintiff's spoliation activity. For instance, on June 4, 2012, three days after this Court's original order for a computer inspection, and the day that Plaintiff learned of the Court's order, Plaintiff downloaded "Evidence Eliminator" software on his Dell laptop. Evidence Eliminator's website, http://www-evidence-eliminator.com, describes the software as "the world's premier computer hard drive cleansing system" that "deep cleans your computer of 'sensitive material', leaving you with a clean PC, a clean conscience and instant peace of mind."

525 2011 N.Y. App. Div. LEXIS 6421 (N.Y. App. Div. 1st Dep't Sept. 22, 2011)

526 Id. at *1.

3. whether the data will identify actual persons who used the internet on April 12, 2009 via the IP address plaintiff identified;
4. which of those persons accessed [the website at issue in the case]; and
5. a budget for the cost of the data retrieval, including line item(s) correlating the cost to [the nonparty] for the disruption.

This case demonstrates the increasing scope of preservation obligations, in *Tener*, extended to non-parties and sources previously considered inaccessible.

Preserve in Place vs. Collect to Preserve

Many companies rely on the so called "preserve in place" strategy–keep documents in their original location and collect only if absolutely necessary. That approach sounds reasonable in theory, but is difficult to execute and can be risky.

"Preserve in place" traditionally referred to preservation of archived data, such as back-up tapes, e-mail archives and document repositories—items that are not altered in the normal course of business. However, recently the term has been expanded to refer to "locking down" files currently in use wherever they are found–workstations, laptops, file shares, repositories, etc.

This preservation strategy relies on either the end user to manually identify and preserve documents subject to the hold, or for a company to utilize search technology to target responsive ESI for lockdown and then change the administrative rights on the target files to "read only." If a user needs to open and work with a read-only file for business reasons, he or she must open a copy and save it with a new name. Each time this is done, a duplicate is created. So every time the file is changed and saved (even via auto-save), it will be locked from further edits as another potentially relevant document. This can lead to additional storage, increased processing and review costs, and business disruption for end users trying to manage their documents in the normal course of business.

The risk with this approach is that if the custodian is also an "administrator" on the computer, he or she can override the in-place preservation and potentially alter the document. In addition, leaving a file in place on a computer in the possession of a custodian exposes the ESI to greater risk of accidental or intentional deletion. Finally, the file metadata and unique hash value of the file may be altered when "locked down," making authentication and duplicate identification problematic.

There is also no practical way to apply a hold in place for broad preservations or ongoing litigation other than to lock down all documents created by a particular author. In the beginning of most cases, it is often impossible to know exactly what may be potentially relevant. Therefore, best practices often require broad preservations (all user-created files), which are then culled/filtered at a later date. Additionally, some cases, such as antitrust, wage-and-hour, or employment discrimination matters allege ongoing conduct, so there may be a need to preserve newly created documents for discovery purposes. This can create business disruption and additional risk if the newly created documents are not properly preserved.

Caveats to preserve in place are as follows:

- Preserve in place leaves the file on the custodian's machine, which could be a laptop that is not under physical control of those responsible for enforcing a legal hold.
- Preserve in place often involves changing system metadata so the document cannot be altered. Additionally, the company cannot keep an electronic document from being deleted if the user of the computer has administrative rights.
- Preserve in place is cumbersome for the custodian because he or she needs to make a copy of the "preserved" file (with appropriate permissions) in order to place it back into use in the regular course of business.
- Preserve in place, without collection, does not protect the ESI from drive crashes, loss of equipment, etc.
- There is no practical way to preserve in place ESI when a broad preservation is required of all user-created documents.

On the other hand, "collect to preserve" is just what it means; you collect the evidence as soon as practical instead of preserving it in place. By immediately collecting all ESI subject to a litigation hold, you minimize business disruption, mitigate the risk of evidence spoliation, facilitate early case assessment, and get the documents into the hands of legal faster.

This approach is both a practical and preferable preservation tactic because of enterprise technology like EnCase eDiscovery that can easily collect (based on narrow or broad culling criteria) the ESI over the network from a central location and store it safely on a secure evidence server. Additionally, for ongoing litigation, the same technology can be used to easily perform secondary collections to catch any newly created evidence.

The only perceived downside to this approach is that it will increase storage costs. However, that argument is weak because storage costs continue to drop, enterprise collections can quickly target just the user-created data or easily apply keyword or conditions (i.e. date ranges) to target only responsive ESI, and, finally, the collected ESI can be compressed for storage.

The benefits to this approach include the ability to:

- Minimize the risk of spoliation by sequestering responsive documents
- Isolate the evidence to avoid business disruption
- Effectively perform broad preservations of all user-created data
- Facilitate early case assessment to get on top of the evidence early
- Prevent alteration to the metadata.

A case in point is *Wilson v. Thorn Energy, LLC*.[527] The court ordered sanctions for defendants' failure to preserve relevant data where defendants failed to back up a flash drive containing all relevant financial records and where that data was lost as the result of the flash drive's failure. In their defense, defendants asserted that they were protected by the "safe harbor" provisions of Fed. R. Civ. P. 37(e).

The court disagreed and held that safe harbor was inapplicable:

527 No. 08 Civ. 9009(FM), 2010 WL 1712236 (S.D.N.Y. Mar. 15, 2010).

> That rule provides that a court may not sanction a party "for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." Fed.R.Civ.P. 37(e). As the Advisory Committee notes explain, the term "routine operation" relates to the "ways in which such systems are designed, programmed, and implemented to meet the party's technical and business needs." Id., advisory committee's notes (2006). Here, however, the data on the flash drive was not overridden or erased as part of a standard protocol; rather, it was lost because the Defendants failed to make a copy. Moreover, even if the loss of the data could be described as "routine," by the summer of 2008, the Defendants were fully aware that the Plaintiffs contemplated litigation to recover the funds that they were owed. Accordingly, the Defendants had a duty to preserve their data. Fujitsu Ltd., 247 F.3d at 436. At a minimum, that duty required that they make a copy of the files on the flash drive. . . The Defendants' failure to do so means that they failed to act in good faith. Rule 37(e) consequently does not preclude an award of sanctions.

Another example is *QK Healthcare, Inc. v. Forest Laboratories, Inc.*[528] In this breach of contract action, the computer of the plaintiff company's president crashed before litigation started but after notice of the dispute. The crash caused destruction of relevant evidence. Furthermore, after commencing the litigation, plaintiff reformatted a computer likely containing relevant evidence. The court granted the defendant's motion for sanctions, finding that the plaintiff reasonably anticipated the litigation and that the ESI was at least negligently destroyed, thus an adverse inference instruction was appropriate.

§ 9.6 Litigation Hold

Litigation Hold is an internal process that corresponds to a party's duty to preserve evidence. Accordingly (as noted above in §9.4), a party subject to litigation must implement a litigation hold "where they knew or should have known that the documents were relevant to litigation or potential litigation."[529] In *Zubulake IV* the Court stated the following with respect to litigation holds:

> The scope of a party's preservation obligation can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (*e.g.,* those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the

528 2013 WL 2147531 (N.Y. Sup. Ct. May 8, 2013).

529 Unigard Sec. Ins. Co. v. Lakewood Engineering & Mfg. Corp., 982 F.2d 363, 368 (9th Cir. Wash. 1992). See also Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. N.Y. 1998) ("The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a part reasonably should know that the evidence may be relevant to anticipated litigation.").

company's policy. On the other hand, if backup tapes are accessible (*i.e.,* actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold.

However, it does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of "key players" to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to *all* backup tapes.[530]

This preservation obligation was extended in *Zubulake V* to include an obligation to oversee compliance with the litigation hold. The court stated, "[a] party's discovery obligations do not end with the implementation of a 'litigation hold'— to the contrary, that's only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents."[531]

Furthermore, a court found the failure to issue a litigation hold at the outset of litigation constitutes gross negligence. In *Toussie v. County of Suffolk,* a discovery dispute arose when plaintiff sought e-mails from relevant employees of the defendant and defendant only produced two e-mails. Through subsequent court intervention and the restoration of archived e-mails more data was recovered. However, it appeared that many e-mails remained unproduced and therefore, plaintiff sought an adverse inference instruction based on defendant's failure to effectively preserve data.[532]

The court found that despite its duty to preserve, the "County did not alter its document and retention procedures in any way as a result of the lawsuit . . . and continued to save electronic data in a virtually inaccessible format."[533] Accordingly, the court reaffirmed that a "failure to implement a litigation hold at the outset of litigation amounts to gross negligence."[534] Although plaintiffs failed to show the deleted files would be relevant evidence favorable to them, the court ordered defendant to pay plaintiff's costs because defendant's failure to produce caused these costs.[535]

In *Acorn v. County of Nassau,* a civil rights case, the plaintiffs alleged the County "failed to institute a litigation hold with regard to this action and to suspend routine document destruction," which, according to Acorn's pleading, led to "the destruction of countless responsive documents."[536] Noting that the duty to preserve evidence began when the County was served with the complaint, the court noted that there was no affidavit supporting the imposition of a "verbal hold" and furthermore, the "verbal hold" that was allegedly implemented was deficient because there was no evidence of who received the hold and how they followed up on hold compliance[537] The court was further strongly

530 Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).
531 Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004).
532 Toussie v. County of Suffolk, No. CV 01-6716(JS)(ARL), 2007 WL 4565160 at *3-5 (E.D.N.Y. Dec. 21, 2007).
533 Id. at *7.
534 Id. at *8.
535 Id. at *10.
536 Acorn v. Nassau, No. CV 05-2301(JFB)(WDW), 2009 WL 605859 at *1 (E.D.N.Y. Mar. 9, 2009).
537 Id. at *2.

dismayed by the failure of the litigation hold to prevent the routine destruction of documents in those departments most likely to be involved.[538]

Because Acorn could not sufficiently demonstrate that the destroyed or lost evidence was favorable to their claim, they were not able to secure an adverse inference instruction. However, because of their gross negligence, the court did impose a sanction for the costs of making the motion, including attorney's fees.[539]

Although *Acorn* does not preclude the validity of a verbal litigation hold, it makes clear that a well-implemented, focused, written litigation hold provides ready evidence of a party's duty to preserve evidence. In addition, if a verbal hold is put in place, there must be credible evidence of who was informed, what they were instructed to preserve, and how they followed up to ensure preservation.

The duty to issue a litigation hold also extends to information held by a party's agents. In *United States v. Maxxam, Inc.* a spoliation claim arose based upon ESI that was allegedly in the possession of a third-party consulting company.[540] Although the evidence was in the possession of a consulting company that had been hired by the defendant's attorney, the court found that since the attorney was the defendant's agent and the consulting firm was retained by the agent, the defendant was responsible for the data.[541] Accordingly, the defendant should have put a litigation hold in place and informed the consulting company of its duty to preserve evidence.

In the first of three notable 2010 opinions addressing issues of a party's failure to properly issue a litigation hold, Judge Scheindlin's lengthy opinion in *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities* revisits precedents established six years earlier in her *Zubulake* line of cases. Specifically, she articulates the standards for legal holds in the context of sanctions for spoliation and made clear that any question regarding preservation decisions and actions will be judged in hindsight (at least in her court). The court articulates its position when it states, "[b] y now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records–paper or electronic–and to search in the right places for those records, will inevitably result in the spoliation of evidence."[542]

The court in *Pension Committee* found that a failure to issue a written legal hold notice was per se gross negligence on the basis that not issuing the notice was likely to result in the destruction of relevant information.[543] The post-*Pension Committee* standard for potential litigants requires a written legal hold notice to be issued at the point a party reasonably anticipates litigation.

Although *Pension Committee* involved a total of 96 plaintiffs, the majority of the issues concerned only 13 of those plaintiffs and their counsel. In discussing the legal hold notices of those 13 plaintiffs, the court noted that counsel's e-mails and memoranda sent to employees "does not meet the standard of a litigation hold" because plaintiff's counsel failed to direct employees to preserve all relevant

538 Id. at *3.

539 Id. at *6-7.

540 United States v. Maxxam, Inc., No. C-06-07497CW (JCS), 2009 WL 817264 at *4 (N.D. Cal. Mar. 27, 2009).

541 Id. at *8-9.

542 685 F. Supp. 2d 456, 462 (S.D.N.Y. 2010).

543 Id. at 475. But see Chin v. Port Authority of New York & New Jersey, 2012 WL 2760776 (2d Cir. July 10, 2012) discussed infra.

records and failed to create a mechanism for collecting records. The memoranda sent by plaintiff's counsel left it to the employees to determine what was relevant and to respond without assistance and supervision of their attorneys.

More importantly, the memoranda did not instruct employees to suspend the destruction of potentially relevant records. These plaintiffs did not issue a formal written litigation hold until 2007–almost four years after they could have reasonably anticipated litigation in April 2003.[544]

Following close in time after *Pension Committee* was the second of three notable 2010 litigation hold cases—Judge Rosenthal's opinion in *Rimkus Consulting Group, Inc. v. Cammarata*,[545] The case involved a group of employees filing a lawsuit to be released from a non-compete agreement with their former employer, Rimkus Consulting. Rimkus filed a countersuit alleging violations of the non-compete agreement and intellectual property theft. And although Judge Rosenthal cites extensively to *Pension Committee*, she declined to follow the Second Circuit standards for negligence and gross negligence, choosing instead to present the facts to the jury to determine defendant's culpability for the intentional destruction of documents.

Importantly, while *Rimkus* ultimately comes out differently because of the facts and differing Circuit precedent, Judge Rosenthal reinforces the *Pension Committee* principles throughout the opinion. Specifically, *Rimkus* recognized the importance of a comprehensive litigation-hold process based on the general rules outlined in FRCP 34 and *Zubulake IV*. The court acknowledged, though, that "applying them to determine when a duty to preserve arises in a particular case and the extent of that duty requires careful analysis of the specific facts and circumstances. It can be difficult to draw bright-line distinctions between acceptable and unacceptable conduct in preserving information and conducting discovery, either prospectively or with the benefit (and distortion) of hindsight." [546]

The final 2010 notable cases involving litigation hold is *Victor Stanley, Inc. v. Creative Pipe, Inc.* (a.k.a. Victor Stanley II). Although not the central issue in the case, Judge Grimm takes the opportunity to analyze the state of the Federal Circuits regarding a party's duty to preserve as part of his comprehensive opinion. He concludes that "the duty to preserve evidence should not be analyzed in absolute terms; it requires nuance, because the duty cannot be identified with precision" (*internal citations omitted*).[547] The court goes on to state, "[t]hus, assessment of reasonableness and proportionality should be at the forefront of all inquiries into whether a party has fulfilled its duty to preserve relevant evidence."[548]

Courts are becoming increasingly less tolerant of parties' failure to issue written legal holds in light of *Pension Committee* and *Rimkus*. In *Crown Castle USA, Inc. v. Fred A. Nudd Corp.*,[549] the court found destruction or loss of documents resulting from failure to issue a litigation hold grossly negligent. As can be the case, the court declined to order dismissal or an adverse inference where the

544 Id. at 473.
545 688 F. Supp. 2d 598, 615-17 (S.D. Tex. 2010).
546 Id. at 613.
547 269 F.R.D. 497 (D. Md. 2010).
548 Id. at 522.
549 No. 05-CV-6163, 2010 WL 4027780 (W.D.N.Y. Oct. 14, 2010).

record did not reveal actual or likely prejudice. The court however, left open the defendant's option to renew their motion following re-depositions of the relevant custodian (at plaintiff's expense). The magistrate judge's recommendations were affirmed by the district court in their entirety.

In the 2011 case, *Haraburda v. Arcelor Mittal USA, Inc.*[550], the plaintiff successfully moved the court to order the defendant to preserve e-mail evidence by claiming the defendant previously deleted e-mails from the plaintiff's account without her permission and refused to issue a litigation hold prior to the rule 26(f) meet and confer. The defendant argued the plaintiff's request was premature as Rule 26(d)(1) prohibited a party from seeking discovery before the Rule 26(f) conference. Disagreeing with the defendant's argument, the court noted Rule 26(d)(1) prohibited requesting production–not compelling preservation–and stated that ruling to the contrary would leave a party with knowledge of an intent to destroy evidence without a remedy. Accordingly, the court found the plaintiff could suffer measurable prejudice based on the suit's heavy reliance on e-mails if evidence was destroyed, and ordered the defendant to implement a litigation hold.

In another 2011 ruling in the case of *Eon-Net LP v. Flagstar Bancorp*[551], the Federal Circuit Court of Appeals upheld a $631,134.00 award for attorney fees, costs, and sanctions against Eon-Net and its counsel. Citing numerous instances of litigation misconduct, the Court ruled against appellant, in part for the destruction of documents prior to the initiation of its lawsuit against Flagstar as well as the intentional failure to implement a document-retention plan. Ultimately, the Court found Eon-Net and its officers had violated their independent duty to preserve evidence during ongoing lawsuits.

Appellant's approach to data preservation left a lot to be desired and likely curried little favor from the court. Eon-Net principal Mitchell Medina stated, "I don't save anything so I don't have to look" and further stated, "[his companies have] 'adopted a document retention policy which is that we don't retain any documents' because those companies have 'evolved into patent enforcement companies which are involved in the business of litigation.'" *Eon-Net v. Flagstar Bancorp* at 18.

With that approach towards preservation, appellants took the extraordinary step of destroying documents from a settled case that were potentially relevant to pending litigation.

Described by the district court as a having a "cavalier approach" towards patent litigation, appellants were cited for numerous other transgressions, including filing objectively baseless litigation. It seems that thumbing your nose at the federal court has become a very expensive pastime.

In one of the more noteworthy cases of 2012 between technology powerhouses Apple and Samsung[552], the defendant Samsung was sanctioned by the magistrate judge for the loss of relevant emails resulting from Defendant's failure to halt the auto-delete feature of its proprietary email system and failure to appropriately follow up with employees subject to the litigation hold. The court ordered an adverse inference sanction allowing the jury to presume that the evidence lost was both relevant and favorable to the plaintiff. The sanction order was ultimately diluted by the District Court and never issued as a jury instruction.

550 2011 WL 2600756 (N.D. Ind. June 28, 2011).

551 2011 WL 3211512 (C.A.Fed. (Wash. July 29, 2011)

552 Apple, Inc. v. Samsung Elecs. Co. Ltd., No. C 11-1846 LHK (PSG) (N.D. Cal. July 25, 2012)

In *Goodman v. Praxair Services, Inc.*,[553] the court ordered an adverse inference for the defendant's destruction of its CEO's laptop, but declined to order sanctions for the destruction of employee computers where plaintiff failed to establish that the hard drives contained relevant ESI. The plaintiff alleged that defendant violated its duty to preserve when it failed to implement a litigation hold, resulting in a significant loss of data, including the contents of relevant hard drives and e-mails, and where its CEO deliberately deleted data, among other things.

The court in *Merck Eprova AG v. Gnosis S.p.A. et al.*[554] issued a $25,000 fine and monetary sanctions for not issuing legal hold and other actions—to deter future misconduct… and to instill a modicum of respect for the judicial process following the defendant's weak efforts to preserve information.

In *Jones v. Bremen High School Dist. 228,*[555] US Magistrate Judge Susan E. Fox sanctioned defendant Bremen High School District 228 for its reckless and grossly negligent failure to impose an effective legal hold, again highlighting the perils of employee self-collection as a method for preservation of ESI.

Defendant learned in October 2007 that Plaintiff Victoria Jones had filed a race discrimination claim against them with the US Equal Employment Opportunity Commission. As a result, defendant's counsel asked three employees to search their own personal e-mail and cull out relevant documents, but failed to supervise the employees' preservation. After plaintiff filed her federal lawsuit in June 2008, defendant's counsel asked additional employees to cull their e-mails in addition to the original three but, again, did not supervise their preservation. During this time period, employees could permanently delete e-mails in a manner that made them unrecoverable, as defendant's e-mail backup tapes were overwritten every 30 days. It was not until October 2008 that defendant began preserving all employees' e-mails in a searchable archive. This despite having a published document retention policy dating back to 2003 which stated that defendant would maintain and preserve all evidence of its "organization, function, policies, procedures or activities."

Plaintiff moved for sanctions due to spoliation. She sought an adverse inference instruction to the jury that the destroyed documents would have supported her claims by containing discriminatory statements. Plaintiff also asked that defendant be precluded from arguing that the absence of discriminatory documents in extant documents showed that no such comments were made and/or that plaintiff was not subject to discrimination or a hostile work environment.

Judge Cox found that plaintiff had demonstrated:

1. That defendant had not reasonably prevented employees from destroying documents concerning the case;
2. Defendant had failed to adequately supervise employee preservation; and
3. That some relevant e-mails probably were lost as a result.

Finding defendant's conduct reckless and grossly negligent, Judge Cox ordered, among other things, that the jury should be told that the defendant had a duty to preserve all e-mail concerning

553 632 F. Supp. 2d 494 (D. Md. 2009).

554 07 Civ. 5898 (S.D.N.Y. Apr. 20, 2010).

555 No. 08 C 3548, 2010 WL 2106640 (N.D. Ill. May 25, 2010).

plaintiff's allegations beginning in November 2007 but did not do so until October 2008 and, therefore, defendant would be precluded from arguing that the absence of discriminatory statements from the period November 2007 to October 2008 is evidence that no such statements were made. However, because the court did not find that there was a deliberate effort on defendant's part to conceal harmful evidence, she denied plaintiff's request for an adverse inference instruction.

In *Chin v. Port Authority of New York & New Jersey*[556], the court rejected the "notion that a failure to institute a 'litigation hold' constitutes gross negligence per se" and ruled that "the 'better approach is to consider the [failure to adopt good preservation practices] as one factor' in the determination of whether discovery sanctions should issue."

In *Voom Holdings LLC v. EchoStar Satellite LLC*,[557] the appellate court held that the lower court "properly invoked the standard for preservation set forth in Zubulake v. UBS Warburg LLC," which requires that a party place a litigation hold once it "reasonably anticipates litigation." Consequently, it then affirmed the lower court's imposition of an adverse inference for defendant's spoliation of ESI.

Reasoning that the litigation holds were not discoverable but that the details surrounding them were, the court in *Cannata v. Wyndham Worldwide Corp.*[558] ordered defendant to produce "information surrounding the litigation hold." This information was to include when defendants learned of claims, when and to whom litigation hold instructions were sent, which categories of information were identified for preservation, etc.

Where plaintiffs sought to compel production of defendant's litigation hold and a list of its recipients, the court in *Tracy v. NVR, Inc.*[559] identified the underlying question as to whether defendant's duty to preserve extended to all potential opt-in plaintiffs. It found that plaintiffs' significant delay in moving for conditional certification and the indirect nature of the evidence sought distinguished the case from *Pippins v. KPMG,* and that plaintiffs failed to make the necessary preliminary showing of spoliation (which would justify production of the litigation hold notice) because they did not establish "that documents that should have been preserved" were lost or destroyed. The court granted defendant's motion for sanctions for opt-in plaintiff's spoliation of hard-copy evidence (originals of a calendar indicating her daily activities, two disparate copies of which had been produced) and ordered that she be precluded from testifying as to her daily work activities during a three-year period.

Another case illustrating the importance of a timely litigation hold is *Sekisui American Corp. v. Hart.*[560] In a lawsuit against former executives for breach of contract, the defendants sought sanctions for deletion of an email folder. Plaintiff sent defendants a Notice of Claim, but failed to issue a litigation hold until fifteen months later and four months before filing their complaint. The plaintiff also failed to notify its IT vendor of the hold for another 6 months. As a result, e-mails in Plaintiff's possession were permanently deleted, allegedly in order to free up server space. The district court awarded sanctions

556 2012 WL 2760776 (2d Cir. July 10, 2012).
557 2012 WL 265833 (N.Y. App. Div. Jan. 31, 2012).
558 No. 2:1-cv-00068-PMP-VCF, 2011 WL 5598306 (D. Nev. Nov. 17, 2011).
559 No. 04-CV-6541L, 2012 WL 1067889 (W.D.N.Y. Mar. 26, 2012).
560 2013 U.S. Dist. LEXIS 115533 (S.D.N.Y. Aug 15, 2013).

in the form of an adverse inference instruction, focusing on the failure to issue the hold and the likely relevance of the email folders of the defendants.

Similarly, in *Jennings v. Orange Reg'l Med. Ctr.*,[561] a state appellate court directed a negative inference charge where defendant failed to forward plaintiff's letter requesting preservation of records to the appropriate party.

These cases illustrate the importance of having an automated legal hold notice process that is integrated with other aspects of the e-discovery process, including collection and review.

§ 9.7 Custodian Self-Collection

A particular ESI collection method that has drawn extensive scrutiny is the practice of allowing custodians to identify, preserve, and collect their own documents. Oftentimes companies will issue a written preservation notice to potential custodians, yet leave it to those individuals to self-comply. As evidenced by several recent decisions, this is a recipe for disaster.

In another seminal e-discovery opinion by Judge Scheindlin in the *National Day Laborer Organizing Network et al. v. United States Immigration and Customs Enforcement Agency*[562], the court reaffirmed the dangers of self-collecting.

United States District Court Judge Shira A. Scheindlin [author of the *Zubulake* (2004) and *Pension Committee* (2010) decisions] issued five decisions in the case, this one dealing with custodian self-collection. The last time we discussed the NDLON case was in the context of metadata and Freedom of Information Act (FOIA) requests [i.e., metadata contained in responsive electronically stored information is producible in FOIA requests (opinion withdrawn)].

The July 13, 2012 opinion still centers on FOIA requests; however, the issue this time around focuses on the effectiveness of the defendants' searches for relevant ESI in response to the plaintiffs' request. The main take-away from this opinion is Judge Scheindlin's harsh criticism of custodian self-collection, which is the method used by many of the defendant agencies in this matter in conducting their searches and collections.

The three plaintiffs (the National Day Laborer Organizing Network, the Center for Constitutional Rights, and the Immigration Justice Clinic of the Benjamin N. Cardozo School of Law) sought information regarding a federal immigration enforcement program launched in 2008 from several United States Federal Agencies [the United States Immigration and Customs Enforcement Agency (ICE), United States Department of Homeland Security (DHS), the Executive Office for Immigration Review (EOIR), the Federal Bureau of Investigation (FBI), and the Office of Legal Counsel (OLC)].

Judge Scheindlin found that several of the searches conducted by the agencies were, in fact, inadequate, and ordered new searches using a list of "search terms and methodologies agreed to by the parties."

In her analysis of the defendants' searches, she stated:

561 958 N.Y.S.2d 168 (N.Y. App. Div. 2013).

562 2012 U.S. Dist. Lexis 97863 (SDNY, July 13, 2012) (with one opinion withdrawn)

[Defendants] argue that "[i]t is also unclear why custodians could not be trusted to run effective searches of their own files, a skill that most office workers employ on a daily basis."

There are two answers to defendants' question. First, custodians cannot "be trusted to run effective searches," without providing a detailed description of those searches, because FOIA places a burden on defendants to establish that they have conducted adequate searches; FOIA permits agencies to do so by submitting affidavits that "contain reasonable specificity of detail rather than merely conclusory statements." Defendants' counsel recognize that, for over twenty years, courts have required that these affidavits "set forth the search terms and the type of search performed." But, some-how, DHS, ICE, and the FBI have not gotten the message. So it bears repetition: the government will not be able to establish the adequacy of its FOIA searches if it does not record and report the search terms that it used, how it combined them, and whether it searched the full text of documents.

The second answer to defendants' question has emerged from scholarship and caselaw only in recent years: most custodians cannot be "trusted" to run effective searches because designing legally sufficient electronic searches in the discovery or FOIA contexts is not part of their daily responsibilities. Searching for an answer on Google (or Westlaw or Lexis) is very different from searching for all responsive documents in the FOIA or e-discovery context.

Judge Scheindlin's message in this case remains clear: organizations should not rely on custodians to uncover potentially relevant ESI in response to FOIA requests. It is a process that requires having the right people and the right technology in place in order to avoid the mistakes and missteps that can occur when you have "lay custodians" conduct them instead.

Samsung Electronics v. Rambus Inc.[563] provides strong criticism of cursory compliance efforts, including the misplaced reliance on custodian self-collection, stating that "[i]t is not sufficient … for a company merely to tell employees to 'save relevant documents' . . . this sort of token effort will hardly ever suffice."[564] The Court determined that the defendants' lack of consistent, systematic, and effective processes to collect and preserve relevant ESI directly led to spoliation of evidence.[565]

At least one court has determined that relying on custodian self-collection is not only negligent, but in fact facilitates a party's ability to engage in misconduct, leading to spoliation. In *In re Hawaiian Airlines, Inc.*,[566] the defendant Mesa Air Group sent a preservation hold notice to its CFO, who was a

563 439 F. Supp. 2d 524 (E.D. Va. 2006).

564 Id. at 565.

565 See also Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614 (D. Colo. 2007) (holding faults Land O'Lakes for simply directing employees to produce relevant information, and relying upon those same employees to exercise their discretion in determining what information to save).

566 No. 03-00817, 2007 WL 3172642 (Bankr. D. Haw. Oct. 30, 2007).

principal witness in the case. Instead of preserving evidence, the CFO responded to the litigation-hold notice by deleting files and wiping his laptops.

Ultimately, the court determined that defendant Mesa Air Group could have taken reasonable steps to prevent or mitigate the CFO's spoliation, such as copying the data from his hard drives.[567] The court noted "instead, Mesa simply told Mr. Murnane to preserve all evidence and trusted him to comply." And as a result, concluded that "[b]ecause Mesa failed to take such steps, Mesa facilitated (the CFO's) misconduct."[568] Consequently, the company was sanctioned with an adverse-inference instruction.

In *Roffe v. Eagle Rock Energy GP, L.P.*,[569] a proposed class action and derivative lawsuit, a transcript of an April 8, 2010 conference call reveals a senior Delaware judge chastising defense counsel for allowing custodians to collect ESI.

The conference was called, among other issues, to discuss the failure of defense counsel adequately to produce e-mail sent or received by the chair and two other members of defendant's conflicts committee. Defendants' counsel argued that it should be found sufficient that e-mail was collected only from two of the three Eagle Rock Energy conflict committee members, with those committee members having personally selected the particular e-mails to be produced.

> "This is not satisfactory," Vice Chancellor J. Travis Laster is quoted in the transcript as saying. As to defendants' counsel producing only those e-mails selected for production by the two committee members, the Vice Chancellor said, "First of all, you do not rely on a defendant to search their own e-mail system. Okay? There needs to be a lawyer who goes and makes sure the collection is done properly."
>
> "[W]e don't rely on people who are defendants to decide what documents are responsive," said Laster, "at least not in this Court." He went on: "[T]he real question in my mind is whether at this point it's enough to do the production the way it should have been done in the first place, or whether there needs to be some additional steps taken to actually image these drives and do some searching to make sure that things haven't been lost since what should have been done in the first place hasn't been done."

The transcript–while not a published decision–certainly puts all Delaware corporations on notice of the expectations of the Chancery Court that custodian self-collection are not defensible.

Google Inc. v. Am. Blind & Wallpaper Factory, Inc.[570] is yet another example in the continuing line of post-December 1, 2006 cases that scrutinize the adequacy of a company's e-discovery preservation and collection process. In this trademark litigation, the court imposed severe evidentiary and monetary sanctions against defendant American Blind based upon its inadequate efforts to preserve, collect, and produce relevant electronic evidence.

567 Id. at *5.

568 Id.

569 No. 5258-VCL (Del. Chanc. Ct. Apr. 8, 2010).

570 No. C 03-5340 JF (RS), 2007 WL 1848665 (N.D. Cal. June 27, 2007).

In *Google*, the defendant American Blind, as part of its unsuccessful defense of the motion, established that it sent written preservation notices to key employee custodians. However, the court was not satisfied with the mere dispersal of preservation notices, and thus ordered American Blind to provide declarations from its employees, explaining "what they *did* with respect to preserving and collecting documents" (emphasis in original).[571] Ultimately, the court found that the evidence demonstrated that "no concerted effort was made to search for internal email" and other computer files, and that the "record demonstrates a willful indifference at American Blind towards ensuring that relevant documents were preserved, collected and produced."[572]

Key conclusions:

- *Google v. American Blind* is another example of the perils of custodian self-collection and the overall strong scrutiny that the courts are consistently applying to an organization's e-discovery collection and preservation process.

- A company does not meet its preservation requirements merely by relying on preservation notices alone, even if tracked by a database. The relevant electronic evidence must be properly collected with the search parameters and the results of such search and chain of custody of responsive documents clearly documented.

The unmistakable message from the cases cited in this section is that diligent and effective ESI preservation and collection efforts are necessary under the FRCP amendments and will be expected as a matter of course going forward. Had these companies immediately executed their preservation duties by properly collecting evidence with the EnCase eDiscovery solution, such penalties would have been avoided. Conversely, companies that rely on custodian self-collection or otherwise fail to establish a defensible and systematic e-discovery preservation and collection process do so at their own risk.

§ 9.8 Metadata

It is routinely acknowledged that metadata, if relevant to the case, is discoverable. It goes without saying that if metadata–or any other kind of information–is irrelevant, there is no obligation to preserve or produce it in discovery.

The ABA's Civil Discovery Standards note that "[a] party requesting information in electronic form should also consider . . . asking for the production of metadata associated with the responsive data."[573] Similarly, The Sedona Conference Principles state that, "[o]f course, if the producing party knows or should reasonably know that particular metadata is relevant to the dispute, it should be

571 Id. at *2.
572 Id. at *5.
573 Civil Discovery Standards 29(b)(ii).

produced."[574] The judiciary is likewise cognizant of this fact. For example, in a case management order issued in 2005, a federal court in Louisiana used the following language:

> Preservation Of Evidence — All parties and their counsel are reminded of their duty to preserve evidence that may be relevant to this action. The duty extends to documents, data, and tangible things . . . "Documents, data, and tangible things" is to be interpreted broadly to include writings, records, files, correspondence, [etc.]. Information that serves to identify, locate, or link such material, such as file inventories, file folders, indices, and *metadata*, is also included in this definition.[575]

Similarly, an Illinois federal district court plainly discussed the discoverability of metadata as follows:

> "On April 25, 2003, WH-TV moved to compel Motorola to produce the files in electronic form. WH-TV stated that it was necessary to have the files in electronic form, because the electronic files contained 'metadata' that are not printed on the hard copies. WH-TV also noted that having the files in electronic form would allow it to search them more easily. On May 2, 2003, this court granted WH-TV's motion to compel."[576]

Often, when faced with a preservation obligation or a discovery request, companies will gather potentially relevant electronic data by asking their employees to comb through their computers looking for documents. While well-intentioned, this activity has the effect of changing much of the key metadata associated with the potentially relevant data, since the employees are using the computer's operating system to gather the information. Historically, in order to preserve the metadata of potentially relevant digital data, one had to make a forensic image of the entire hard drive, or at least a partition. At the time, there was no other way to preserve all of the relevant metadata. Fortunately, with the release of EnCase eDiscovery Version 5, individual files can be collected while preserving their metadata. This revolutionary advance is crucial for cases in which metadata contains potentially relevant information, and is an important part of a defensible electronic discovery process.

The class action case, *Williams v. Sprint/United Mgmt. Co.*[577] is a landmark case with respect to metadata. The plaintiffs--a class consisting of over 1,700 former employees who had been terminated in a reduction-in-force--alleged that age was a determining factor in their terminations. The plaintiffs objected to the defendant's production in discovery of a redacted form of Excel spreadsheets that set forth various criteria concerning how individuals were selected for the reduction-in-force. "Defendant, prior to producing the electronic versions of the Excel spreadsheets, had utilized software to scrub

---

574 The (2004) Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 5 Sedona Conf. J. 151, 193 (2004).

575 In re Vioxx Prods. Liab. Litig., 2005 WL 756742 at *3 (E.D. La. Feb. 18, 2005) (emphasis added).

576 Zenith Elecs. Corp. v. WH-TV Broad. Corp., No. 01 C 4366, 2004 WL 1631676 at *7 (N.D. Ill. July 19, 2004).

577 230 F.R.D. 640 (D. Kan. 2005).

the spreadsheets to remove the metadata."[578] The court noted that "when I talk about electronic data, that includes the metadata."[579] After a thorough review of metadata and the issues pertaining to it, the court relied primarily on the emerging standards of The Sedona Conference Principles, holding that:

> [W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, [FN68] the producing party should produce the electronic documents with their metadata intact, unless the party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order. [FN69] The initial burden with regard to the disclosure of the metadata would therefore be placed on the party to whom the request or order to produce is directed. The burden to object to the disclosure of metadata is appropriately placed on the party ordered to produce its electronic documents as they are ordinarily maintained because that party has access to the metadata and is in the best position to determine whether producing it is objectionable. Placing the burden on the producing party is further supported by the fact that metadata is an inherent part of an electronic document, and its removal ordinarily requires an affirmative act by the producing party that alters the document.[580]
>
> FN68. This same reasoning would apply if the court ordered a party to produce the electronic documents as an "active file" or in their "native format."
>
> FN69. The same principle may apply when a party *requests* electronic documents be produced as they are maintained in the ordinary course of business, as an "active file," or in their "native format."

In a similar ruling, *Nova Measuring Instruments Ltd., v. Nanometrics, Inc.*,[581] the United States District Court held, "[d]ocuments shall be produced in their native file format, with original metadata" and thereby ordered defendants in the patent infringement case to produce them in such a manner.[582] Plaintiff, Nova Measuring Instruments, sought for defendants to produce documents pursuant to Patent L.R. 3-4 in their original and searchable format after plaintiff received 36,000 documents that were deemed "unsearchable": the documents did not display their relevance to the infringement claims. Defendant contended that not all documents presented were relevant. The court held there was no reason not to have the documents--as well as any electronic version in its original format--with metadata as well as separately identifying the documents that corresponded to each inquiry in Plaintiff's Patent L.R. 3-1(c) chart.

The approach used by the *Williams* and *Nova Measuring Instrument* courts--at the very least when

578 Id. at 644.
579 Id.
580 Id. at 652.
581 417 F. Supp. 2d. 1121 (N.D. Cal. 2006).
582 Id.

it pertains to the preservation of electronic data--virtually mandates the use of a collection process that does not alter or destroy the metadata.

In *Bray & Gillespie Management LLC v. Lexington Ins. Co.*, a resort management company brought suit against its insurer after a claim dispute arose. During discovery, the insurer sought ESI and defined ESI to include "without deletion or alteration of meta-data, in its native form."[583] However, when the plaintiff produced the evidence, they partially failed to deliver the metadata and to deliver files in their native format; instead they delivered much of the data in a .TIFF format.

The court agreed with the insurer and found that Bray & Gillespie had violated FRCP 34, which allows the requesting party to specify the forms in which the ESI will be produced. Although Rule 34 allows a party receiving a request to object, the court found Bray & Gillespie failed to object.[584] Because the defendant requested the ESI be delivered with metadata intact and it was not, Bray and Gillespie violated Rule 34. The court held that the .TIFF format did not constitute satisfactory production because documents are not kept in this format in the usual course of business. Although Bray & Gillespie's sanctions were limited to the costs necessary to comply with the order to produce the contested documents,[585] several of Bray & Gillespie's attorneys were ordered to pay for the plaintiff's costs as well as the court's costs to transcribe part of the proceedings.[586]

Despite the relevance of metadata in many cases, there are limits to the production of metadata. In *Kingsway Financial Services, Inc. v. Pricewaterhouse-Coopers, LLP* the plaintiff requested metadata for a number of produced documents.[587] In rejecting the plaintiff's request the court noted:

> In light of the dubious value of metadata and plaintiffs' total failure to explain its relevance to the claims and defenses in this action, plaintiffs' application to compel its production is denied. Given the advanced stage of discovery in this litigation and the absence of any showing that production of metadata would serve any useful purpose, I am left with the strong sense that ordering the production of metadata would not shed any light on any of the claims or defenses in this action.[588]

The court found support for this proposition in *Aguilar v. Immigration & Customs Enforcement Div. of the United States Dep't of Homeland Sec.*, noting:

> In general, metadata is relevant when the process by which a document was created is in issue or there are questions concerning a document's authenticity; metadata may reveal when a document was created, how many times it was edited, when it was edited and the nature of the edits. In the absence of an issue concerning the authenticity of

583 Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co., 259 F.R.D. 568, 573 (M.D. Fla. 2009).
584 Id. at 589.
585 Id .at 590.
586 Id.
587 Kingsway Fin. Servs. v. Pricewaterhouse-Coopers, LLP, No. 03 Civ. 5560(RMB)(HBP), 2008 WL 5423316 at *6 (S.D.N.Y. Dec. 31, 2008).
588 Id.

> a document or the process by which it was created, most metadata has no evidentiary value.[589]

This case and other cases where a court refuses to order production of metadata are not necessarily evidence that metadata is not critical and a required aspect of a particular production. Rather it stands for the more general proposition that discovery is not intended to be open-ended and that a party making an RFP must be able to demonstrate the need for production.

In a more recent opinion on the subject of metadata[590], the court in *S2 Automation LLC v. Micron* addressed several matters, including (1) "whether S2 Automation must produce electronically stored information ('ESI') in the format Defendant Micron Technology, Inc. has requested;" (2) "whether S2 Automation must separately produce metadata;" and (3) "whether S2 Automation must identify the search strategy it used to produce documents in response to requests for production ("RFP")." The court held that the plaintiff's production in PDF was unacceptable and that it must be in native format or in the format requested by the defendant, and that plaintiff's counsel's statements were sufficient to put the adequacy of his compliance with Rule 26(g) in question and require production of plaintiff's search strategy, including its interaction with counsel.

And as courts have become more sophisticated on the issue of metadata, parties are getting less leeway from the courts in the form of production. For example, in *Indep. Mktg. Group, Inc. v. Keen*,[591] the plaintiff produced ESI by printing a collection of documents and scanning them into a nonsearchable PDF filed that lacked metadata. The plaintiff resisted reproduction on the grounds of undue burden based on the estimated $10,000 cost of doing so. The court found that the ESI was not produced by plaintiff as ordinarily kept or in a reasonably usable format, and declined to find that the information was not reasonably accessible or, if it was, that good cause had been shown to compel reproduction.

Another example is *Harry Weiss, Inc. v. Moskowitz*.[592] In this payment dispute case, plaintiff revealed two years into the litigation that it had deleted relevant ESI. Plaintiff claimed this occurred prior to litigation, however defendant's claimed after conducting a forensic examination that the computer was broken after the commencement of litigation. Plaintiff then argued that defendants had not suffered prejudice because many of the files in question had been printed. The court rejected this argument because printing destroyed discoverable metadata. The court found plaintiff's actions grossly negligent at a minimum and precluded plaintiff from offering any evidence at trial in opposition to defendants' defenses and counterclaims.

Key conclusions:

- Metadata is often critical information that reveals the full significance of the data it underlies.
- EnCase eDiscovery preserves ESI in its native format with all metadata intact.

589 Id.(citing Aguilar v. Immigration & Customs Enforcement Div. of the United States Dep't of Homeland Sec, 255 F.R.D. 350, 353 (S.D.N.Y. 2008)).

590 S2 Automation LLC v. Micron Tech., Inc., No. CIV 11-0884 JB/WDS, 2012 WL 3656454 (D.N.M. Aug. 9, 2012).

591 No. 3:11-cv-447-J-25MCR, 2012 WL 207032 (M.D. Fla. Jan. 24, 2012)

592 106 A.D.3d 668 (N.Y. App. Div. May 20, 2013).

- A party needs to be conscious of the relevant metadata associated with discoverable information and use EnCase eDiscovery to preserve the evidence and satisfy the burden of production.
- EnCase eDiscovery provides a defensible evidentiary record demonstrating adherence to metadata discovery protocols.
- EnCase eDiscovery allows counsel to practice aggressive transparency by providing a clear record of metadata and how it is preserved.
- Using EnCase eDiscovery to preserve and process ESI eliminates the risk of metadata spoliation.
- By making every effort to preserve and deliver metadata, a party effectively insulates itself from the risk of spoliation claims.

The following are 10 recommended principles regarding metadata:

1. Develop Policies and Procedures for Handling Metadata

Before litigation is reasonably likely, assess document retention practices as they relate to metadata. Develop, implement, and enforce practices that expressly pertain to metadata outside of the context of litigation. Determine what metadata are created in the normal course of business, whether they are destroyed or preserved in the normal course of business, and what operational, regulatory, or statutory directives pertain to metadata in your industry and state.

If the metadata change is part of the IT process used to manage data, the only concern is when the obligation to preserve ESI begins. At that time, consider whether to stop all processes that may alter any potentially relevant metadata. It may not be possible to continue normal business operations and suspend all processes that alter metadata on active documents needed to operate your business. In some cases it may be appropriate to develop a protocol that preserves metadata each time before a change is made; in other cases, it may be appropriate to develop a protocol that preserves metadata on a regular schedule (i.e., daily, weekly, or some other interval). In yet other cases, the cost and burden to preserve metadata on an ongoing basis may be prohibitive.

Every company should develop consistent protocols and procedures for addressing this in all litigation moving forward. If the circumstances of your business or IT operations present costly or burdensome challenges to preserving all metadata on a going-forward basis, be prepared to raise these issues, first in the context of a voluntary meet-and-confer session with your adversaries and then with the court. Prior to the meet-and-confer session, develop an adequate evidentiary, fact-based record that demonstrates the claimed cost and burden and justifies the proposed resolution.

2. Always Include Metadata in the Litigation Hold

At the inception of litigation, or when it is reasonably anticipated, impose a litigation hold that preserves all potentially relevant ESI, including metadata. A proper litigation hold eliminates the risk of spoliation sanction or an adverse presumption order. In *Krumwiede v. Brighton Associates,*

L.L.C.,[593] the plaintiff's alteration and deletion of files destroyed metadata, which prevented him from authenticating ESI essential to his defense against defendant's counterclaim; default judgment was entered in defendant's favor.

Education and carefully drafted preservation instructions are critical to avoiding issues of spoliation. Education helps show that your company takes the preservation process seriously. Training of document custodians about their preservation obligations is essential. As is always the case, it is important to ensure that personnel training materials provide the appropriate level of information, which is directly related to the purpose of such training.

Document custodians must have a clear idea of what they are to do, which documents are included in the litigation hold notice, and access to appropriate personnel who can provide guidance as questions arise. For example, it is often appropriate to advise custodians that performing simple operations, like opening and saving a text document, can alter metadata, and therefore if you need to open a document to determine whether it is subject to a hold, it is important to close it, rather than save it. On the other hand, in circumstances where technological processes are used to capture and preserve potentially responsive documents without any custodian intervention, there may be no need to provide such instructions.

3. Create a Metadata Protocol to Propose to Your Adversaries

At the inception of litigation, or when it is reasonably anticipated, discuss the kinds of metadata that are associated with potentially relevant ESI and devise a protocol to propose to litigation adversaries. To completely fulfill e-discovery obligations, fully understanding the ESI universe in question is critical. Vetting metadata issues early will greatly reduce the likelihood of mistakes, reduce the cost of complying with discovery obligations, and it will increase your credibility with the court.

4. Consider Enlisting an Expert to Assist in Metadata Preservation and Production

Just after the inception of the litigation, identify and enlist expert assistance to oversee and testify about the methods used to identify, preserve, collect, and produce ESI, including metadata. This resource may include some combination of internal sources like IT personnel and outside experts such as law firms and e-discovery vendors. Moving forward, this group can assist in the design, review, and approval of protocols, testify to document authenticity, and defend against any possible allegation of spoliation, etc.

Members of this group may end up being your 30(b)(6) witness(es). Federal Rules of Civil Procedure 30(b)(6) requires a noticed organization to designate one or more persons to testify on its behalf regarding the subject matter identified in the areas of inquiry. Depending upon the facts of the case and the size of the corporation, these areas of inquiry can be extensive. The testimony will bind the company and may be used for any purpose in the litigation.

In the context of e-discovery, this witness is often called to testify on the steps the corporation

593 No. 05 C 3003, 2006 WL 1308629 (N.D. Ill. May 8, 2006).

took to find and produce responsive documents in order to ensure discovery was diligently completed in good faith. When called to provide sworn testimony on information management, document retention, and e-discovery issues, the witness must be prepared to testify on such topics as location of ESI, access to ESI, how it is maintained and how the data--including metadata--was preserved for the litigation.

5. Disclose Intentions Related to Metadata

At the Rule 26(f) meet-and-confer session, or initial case management conference, disclose all intentions regarding ESI, including metadata, as they relate to propounding and responding to discovery. FRCP Rule 26(f)(3)(C) requires parties to discuss, while preparing a discovery plan, "any issues about the disclosure or discovery of electronically stored information, including the form or forms in which it should be produced."

At the outset of any litigation, the parties should discuss whether the production of metadata is appropriate and attempt to resolve the issue without court intervention.[594]

6. Request Metadata as Early as Possible

During litigation, if metadata might be relevant and/or useful to the case, request it as early as possible, because the propounding party is "the master of its production requests; it must be satisfied with what it asked for."[595]

Failure to make a timely request has consequences. To obtain metadata, the propounding party should specifically ask for it; a delay in requesting production of metadata may cause the court to deny motion to compel or shift cost of production to discovery proponent.[596]

Native production of e-mails can be highly desirable since it allows counsel to see all metadata in context. The costs associated with producing it in native format are generally lower than what is required to produce a text-searchable image with associated load file. There appears to be an increasing trend in e-discovery for the native production of ESI, while in the past the practice was to produce text-searchable (i.e., OCR), branded .TIFF or .PDF format documents with associated load files that contain metadata.[597]

Producing e-mails in their native format will be useful pre-trial during review, because e-mail metadata is needed to conduct proper analytical searches such as e-mail-threading to determine timelines and e-mail history. Likewise, producing e-mails in their native format will be useful at trial for getting such e-mails authenticated and admitted to the court, allowing counsel to show that the

---

594 See Aguilar v. Immigration & Customs Enforcement Div., 255 F.R.D. 350 (S.D.N.Y. 2008); Scotts Co. LLC v. Liberty Mut. Ins. Co., No. 2:06-CV-899, 2007 WL 1723509 at *4 (S.D. Oh. June 12, 2007).

595 Autotech Techs, Ltd. P'ship v. AutomationDirect.com, Inc., 248 F.R.D. 556, 560 (N.D. Ill. 2008).

596 See D'Onofrio v. Sfx Sports Group, Inc., 247 F.R.D. 43 (D.D.C. 2008); Wyeth v. Impax Labs., Inc., 248 F.R.D. 169 (D. Del. 2006); Kingsway Fin. Servs. v. PriceWaterhouse-Coopers LLP, No. 03 Civ. 5560(RMB)(HMP).

597 See Baker Hughes Inc. v. Homa, 2013 WL 684699 (S.D. Tex. Feb. 25, 2013) (ordering production of e-mails as .pst files).

items are what they purport to be. A tool that alters metadata or does not provide metadata can cause a significant problem for authentication of evidence.

7. Ensure that Preservation Protocols are Being Followed

During litigation, if your role is discovery respondent, implement systems to ensure that e-discovery protocols are being followed. It is not sufficient for counsel to issue a litigation hold; he or she must ensure that it is being followed by developing a protocol and having the requisite policy, procedures, and technology in place.

8. Document Your Preservation Efforts

During the litigation, develop a defensible evidentiary record that demonstrates adherence to discovery protocols. It is not enough to merely follow established protocols, it must be proven with admissible evidence that the protocols were followed, or that reasonable systems were in place to ensure compliance with protocols.

Having these protocols in place will help you defend against discovery respondent's allegations of spoliation, motions to compel and motions for sanctions, and adverse inference. Testimony of a competent 30(b)(6) witness, who on the basis of personal knowledge and reference to business records, among other things, can testify about preservation, collection, and production efforts must be provided.

9. Be Prepared to Authenticate All ESI Produced

During litigation, be prepared to authenticate, or challenge, or defend authenticity of ESI, including metadata. Because discovery of ESI is expensive and time-consuming, necessary steps must be taken to make it admissible. Make sure that it is relevant, authentic, and not hearsay or subject to exception.

In *Lorraine v. Markel American Ins. Co.*,[598] cross-motions regarding the enforcement of arbitration award were both denied because of failure to authenticate e-mail documents offered to prove the scope of the arbitration agreement. This is an excellent overview of authenticating ESI. In order for ESI to be admissible, it must be shown to be authentic. Rule 901(a) defines what this entails: "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." The authentication methods discussed in this case include: using hash values; Metadata; 901 (b) (9) Process; 901 Self-Authentication (document under seal); 901(b)(3) comparison and 901(b)(1) Testimony by witness.

598 241 F.R.D. 534 (D. Md. 2007).

10. Practice Aggressive Transparency

During litigation, practice aggressive transparency. Promptly advise your adversary--and/or the court as applicable--of any change to the discovery protocol or error in execution of the protocol. Let them know immediately about any late discovery of new sources of ESI, other issues that could affect your obligation to produce metadata, or the court's perception of good faith in discharging e-discovery obligations.

Cooperation by both parties during a Rule 26(f) meet-and-confer conference is now critical to a successful and defensible production. In *Mancia v. Mayflower Textile Services Co.*, Judge Grimm stressed that litigants must cooperate and communicate in order to avoid inefficient and costly discovery practices. *Mancia* encourages parties to meet and confer before propounding discovery so that discovery can be focused and specifically tailored to what is necessary to resolve the matter.

Because e-discovery is unique and can be confusing, expensive, time-consuming, and risky, both judicial tolerance toward attorneys engaging in gamesmanship and the supreme rule of "volunteer nothing" are quickly coming to an end. Modern discovery was originally envisioned as "an essentially cooperative, self-regulating process," requiring minimal judicial involvement and allowing for disclosure of all relevant facts pertinent to the case.

Metadata is critical in e-discovery. Companies must include metadata in their electronic policies and protocols, and attorneys must discuss it early in each case. It is becoming increasingly clear that, as new technology is deployed, lawyers must embrace creative and technological approaches to grappling with metadata as information inflation continues apace and the value of metadata increases.

§ 9.9 Search

For a company with a network-enabled computer investigation capability, the cost of e-discovery is nominal when compared to a purely outsourced model. In addition to efficiently fulfilling its preservation obligations under the Federal Rules––including with respect to the early attention requirements and preservation of metadata–a litigant with a networked computer investigation and collection capability actually achieves numerous efficiencies by searching for relevant data and collecting the relevant data of custodians off of servers and workstations. As noted by Judge Scheindlin of the Southern District of New York:

> Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved. This makes no sense. Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying.[599]

599 Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318 (S.D.N.Y. 2003).

In the absence of an adequate data-preservation procedure, the court is less likely to allow cost sharing among the parties. In *Semsroth v. City of Wichita,*[600] the defendant brought a cost-sharing motion for discovery costs associated with producing e-mail from 117 employees, as requested by the plaintiff. The e-mail was only stored on disaster relief backup tapes. The defendant had already spent $20,000 in producing electronic documents from their backup tapes and would have had to purchase additional software to produce the remaining e-mail. The plaintiff argued that the defendant should incur all of the costs because they chose to store the e-mail in an inaccessible format. The court agreed, holding that the defendant should in fact incur all of the discovery costs. It noted that the costs already incurred are irrelevant to a cost-shifting analysis because "the majority of those expenses do not directly relate to the restoration and search of the backup tape."[601] If this company had utilized EnCase eDiscovery software, it could have shown that its production was not deficient.

From a single network workstation, a litigant with EnCase eDiscovery can simultaneously target several workstations on its network, and within minutes, view metrics on the size and types of files on a target workstation, conduct keyword searches for--and retrievals of--key documents, copy documents, and if necessary, image a target hard drive. As a result, the litigant can efficiently identify responsive information, and can rapidly search any such data for privileged material, thereby saving countless attorney hours (and the resulting expense) associated with traditional paper document review and the creation of privilege logs.

In short, network-enabled computer forensics is fostering a revolution in terms of the feasibility of large-scale investigations. For instance, in a recent matter involving due-diligence investigation for a merger and acquisition, enterprise computer forensics technology was effectively employed to search more than 5,000 computers distributed in dozens of locations worldwide in only four weeks.[602] The consultants involved completed the effort at a fraction of the costs of less advanced processes.

In support of this targeted collection process, it is important to note that the duty to preserve evidence, including ESI, extends only to "potentially relevant information." *Zubulake IV* recognized no legal duty exists to "preserve every shred of paper, every email or electronic document and every backup tape … Such a rule would cripple large corporations."[603]

The FRCP amendments echo this rule, recognizing the need for a "balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party's routine computer operations could paralyze the party's activities." Fed. R. Civ. P. 26(f) Advisory Committee's Note (2006 Amendment). The Advisory Committee Notes further provide that preservation efforts need only be "reasonable" and "narrowly tailored" to relevant information. *Id.*

Courts consistently agree that only potentially relevant materials fall within the duty to preserve ESI. Thus, preserving parties should be able to use best practices technology to identify and collect

600 239 F.R.D. 630, (D. Kan. 2006)

601 Id. at 640.

602 eExaminer, August 2004; "Mission Impossible; 5,000 Computer Examinations in Four Weeks".

603 Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2004).

potentially relevant materials through defined search criteria. This thinking is reflected in several of the following cases:

The *Treppel v. Biovail Corporation*[604] case provides that defined search strategies are appropriate in cases involving electronic data where the number of documents may be exponentially greater than paper discovery. In support of this decision, the *Treppel* Court cited from The Sedona Conference Principles, which state, "A responding party may properly access and identify potentially responsive electronic data and documents by using reasonable selection criteria, such as search terms or samples."[605] Similarly, in *Zubulake v. UBS Warburg LLC,* ("*Zubulake V*"), the court, as noted above, advocates a targeted search approach where litigation holds are executed by running "a system-wide keyword search" involving a process where the responding party can "create a broad list of search terms, run a search for a limited time frame and segregate responsive documents…"

In *Flexsys Americas LP v. Kumho Tire U.S.A., Inc.*,[606] the court agreed on a compromise solution to a broad request for ESI, recognizing the burden for a large corporate entity of searching through years of electronic files. Accordingly, the court agreed to limit the defined searches to certain individuals "most likely to have information relevant to the arbitration issues." *See also United States v. Greathouse,*[607] [court suggests that the advent of technology "like EnCase" will require law enforcement to conduct narrowly tailored on-site keyword searches instead of seizing entire computers].

The 2006 FRCP amendments likewise support a targeted search-and-collection strategy. The Advisory Committee Notes to Rule 26(f) point to provisions of the sample case-management order in the Manual for Complex Litigation, which provides:

> [t]he parties should attempt to reach agreement on all issues regarding the preservation of documents, data and tangible things. These issues include … the extent of the preservation obligation, identifying the types of material to be preserved, the subject matter, time frame, authors … and key words to be used in identifying responsive materials…

Collection and preservation of ESI must incorporate a defensible process that accomplishes the objectives of preserving relevant data--including metadata--and establishing a proper chain of custody. With the right technology, these results can be achieved without full-disk imaging. However, full-disk imaging and deleted file recovery are emphasized by many e-discovery vendors and consultants as a routine e-discovery practice. While such deep-dive analysis is required only in some circumstances, full-disk imaging is unwarranted as a standard e-discovery practice due to considerable costs and burden. Large-scale, full-disk imaging is burdensome because the process is very disruptive, requires much more time to complete, and--as e-discovery processing and hosting fees are usually calculated on a per-gigabyte basis--costs are increased exponentially with the increased volume of collected ESI.

604 233 F.R.D. 363 (S.D.N.Y. 2006).
605 Id. at 374.
606 No. 1:05-CV-156, 2006 WL 3526794 (N.D. Ohio Dec. 6, 2006).
607 297 F. Supp. 2d 1264 (D. Or. 2003).

To date, courts have not required full-disk imaging as a routine means of collecting ESI in the context of e-discovery. To the contrary, several recent decisions provide that forensic mirror-image copies of computer hard drives are not generally required for e-discovery production. In *Diepenhorst v. City of Battle Creek*,[608] the court declined to require the production of full-disk images absent a strong showing of good cause, noting that the "imaging of computer hard drives is an expensive process, and adds to the burden of litigation for both parties…" The court further noted that "imaging a hard drive results in the production of massive amounts of irrelevant, and perhaps privileged information." [609]

Vasudevan Software, Inc. v. Microstrategy Inc.[610] involved a patent infringement suit, where the court denied the defendant's motion for a forensic examination of plaintiff's email backup systems. The defendant argued that plaintiff deleted emails in previous litigation against Oracle and IBM, during which testimony came out about email deletion. Plaintiff demonstrated that such deletion occurred pursuant to a policy of deleting junk mail due to the small size of its server. Moreover, although defendant pointed to documents it produced that plaintiff did not, plaintiff argued that it had not deleted those documents but that they simply were not responsive to defendant's requests, and so had not been produced. On that record, the court held that forensic examination was not appropriate as there were no serious issues concerning the reliability and completeness of plaintiff's production.

Another example is *In re Pinnacle Eng'g, Inc.*[611] In this unlawful termination case, defendants filed a mandamus petition regarding a trial court order to produce entire computer and network server hard drives and electronic native-file documents to plaintiffs' forensic computer expert. The appellate court granted the petition because plaintiff's requests had not "specifically request[ed] production of electronic . . . data and specif[ied] the form in which [it should be] produced," as required by the Texas Rules of Civil Procedure (Tex. R. Civ. P. 196.4). Plaintiff had merely requested the "network server(s) utilized for electronic data" by three custodians from 2009 to 2011 as well as production of the computer hard drives from the laptops, desktops, Dell notebooks, and tablets of these custodians. The court found that these "requests did not inform [defendants] of the exact nature of the information sought and do not meet the requirements of [the] rule . . . ." Accordingly, the appellate court found that the lower court had abused its discretion in ordering discovery beyond the permissible scope and reversed.

Generally, courts will only require that full forensic copies of hard drives be made if there is a showing of good cause supported by specific, reliable evidence of the alteration or destruction of electronic information or for other reasons. *Balboa Threadworks, Inc. v. Stucky*.[612] However, "[c]ourts have been cautious in requiring the mirror imaging of computers where the request is extremely broad

608 No. 1:05-CV-734, 2006 WL 1851243 at *3 (W.D. Mich. June 30, 2006).

609 Id. at *4 (citing McCurdy Group v. Am. Biomedical Group, Inc., 9 Fed. Appx. 822, 831 (10th Cir. 2001)). See also Balfour Beatty Rail, Inc. v. Vaccarello, No. 3:06-cv-551-J-20MCR, 2007 WL 169628 (M.D. Fla. Jan. 18, 2007) (court rejects discovery request for production of copies of hard drives as overbroad and unwarranted).

610 2013 WL 1366041 (N.D. Cal. Apr. 3, 2013).

611 2013 WL 941820 (Tex. App. Mar. 12, 2013).

612 No. 05-1157-JTM-DWB, 2006 WL 763668 at *3 (D. Kan. Mar. 24, 2006).

in nature and the connection between the computers and the claims in a lawsuit are unduly vague or unsubstantiated in nature." *Ameriwood Industries, Inc. v. Liberman*.[613]

While an organization must establish a systemic and defensible process to search, preserve, and collect relevant ESI, such efforts need not be overly broad and thus unduly burdensome. In fact, an effective e-discovery collection process is one that will both facilitate compliance and mitigate costs.

A closer look at the opinions reveals that courts are criticizing the effectiveness and reliability of searches. Additionally, judges are emphasizing the fact that lawyers must have a defensible and systemized process when conducting a search.

Eurand, Inc. v. Mylan Pharmaceuticals, Inc.[614]

In evaluating the adequacy of plaintiff's search for a specific category of ESI, the court stated that the test to determine the appropriateness of a search is whether the search:

> "could…have been expected to produce the information requested," determined that the information sought was likely to be found in the e-mails of the inventors of a specific patent, and ordered plaintiff to search the e-mails of the relevant inventors within a date range prescribed by the Court; opinion included brief discussion of keyword searching and noted, "[n]either lawyers nor judges are generally qualified to opine that certain search terms or files are more or less likely to produce information than those keywords or data actually used or reviewed.

Kay Beer Distributors, Inc. v. Energy Brands, Inc.[615]

The court denied plaintiff's motion to compel such access, finding plaintiff's request for access to defendant's DVDs containing potentially responsive ESI as well as privileged and non-responsive information overly broad and unduly burdensome in light of defendant's estimated expense to comply.. The court noted that it was unclear what information on the DVDs would be considered responsive or admissible and stated that "[t]he mere possibility of locating some needle in the haystack of ESI… does not warrant the expense [defendant] would incur in reviewing it." Instead the court ordered the defendant to keyword search the DVDs using variations of plaintiff's name and to produce the material identified.

§ 9.9.1 Keyword Searches

Keyword searching is a powerful tool in the discovery of electronic data. Its effectiveness, though, hinges upon the quality of selected search terms; the junk-in-junk-out theory applies in keyword

613 No. 4:06CV524-DJS, 2006 WL 3825291 at *4 (E.D. Mo. Dec. 27, 2006).
614 266 F.R.D. 79 (D. Del. 2010).
615 No. 07-C-11068, 2009 WL 1649592 (E.D. Wis. June 10, 2009).

searching. In recognition of the importance of this process, courts are now imposing higher standards when it comes to the selection of search terms.

The recognition of the complexity is evident in *United States v. O'Keefe*. In *O'Keefe*, the criminal defendant challenged the government's search terms. Judge Facciola recognized the complexity of this aspect of electronic discovery noting:

> Whether search terms or "keywords" will yield the information sought is a complicated question involving the interplay, at least, of the sciences of computer technology, statistics and linguistics . . . Given this complexity, for lawyers and judges to dare opine that a certain search term or terms would be more likely to produce information than the terms that were used is truly to go where angels fear to tread. This topic is clearly beyond the ken of a layman…[616]

Again, in *Equity Analytics, LLC v. Lundin*, plaintiff alleged that the defendant had used his personal computer to access the plaintiff's information illegally.[617] The plaintiff requested to search the defendant's personal computer. Since the defendant used his computer for many other purposes, the computer contained privileged information such as attorney-client communications, business records, medical records, tax records, etc. Given the sensitive nature of this information, the parties disputed the appropriate search terms and search criteria. In considering plaintiff's objection to the defendant's proposed search limitations, Judge Facciola required the plaintiff to submit an affidavit explaining in detail how the defendant's choice of search terms and criteria would fail to capture the desired evidence.[618]

Furthermore, evidence simply showing that a search has been done is no longer sufficient to demonstrate reasonableness in inadvertent production cases. In *Victor Stanley Inc. v. Creative Pipe, Inc*., the defendant alleged that the privileged documents produced were inadvertent because it had used reasonable effort to prevent disclosure by conducting a privilege search using seventy different keyword search terms.[619] The court, however, was not satisfied with the effort because the defendant did not explain how the search terms were developed, how the search was conducted, and what quality control was employed in assess the search's reliability and accuracy. As a result, it found the privilege waived because the defendant's reliance on insufficient keyword search did not constitute reasonable precaution to prevent disclosure. [620]

The court in *William A. Gross Construction Associates, Inc.,* further emphasized the requirements for keyword searches.[621] The case arose out of a delay in construction dispute between a contractor and a project owner. The contractor sought discovery of a nonparty's project-related documents that were electronically stored. The contractor formulated an exceedingly broad keyword search list

616 United States v. O'Keefe, 537 F.Supp 2d 14, 23-24 (D.D.C., 2008).
617 Equity Analytics, LLC v. Lundin, 248 F.R.D. 331, 332 (D.D.C., 2008).
618 Id. at 334-35.
619 Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 253 (D. Md. 2008).
620 Id.at 263.
621 William A. Gross Constr. Assocs. v. Am Mfrs. Mut. Ins. Co., 256 F.R.D. 134 (S.D.N.Y. 2009).

that contained thousands of search terms in addition to those that specifically related to the project. Regarding this overbroad list, the court recognized the project owner "correctly pointed out that use of such extensive keywords would require production of the entire Hill email database."[622] This breadth of discovery would prove to be a burden on the producing party and produce an excessive quantity of material, much of which would be irrelevant and private information.

The court expressed disappointment with the parties before it and with attorneys in the jurisdiction noting their opinion was intended "as a wake-up call to the Bar in this district about the need for careful thought, quality control, testing, and cooperation with opposing counsel in designing search terms."[623] The court approvingly noted prominent keyword search cases from other jurisdictions[624] and concluded by requiring counsel in keyword searches to "carefully craft the appropriate keywords, with input from the ESI's custodians as to the words and abbreviations they use, and the proposed methodology must be quality control tested to assure accuracy in retrieval and elimination of 'false positives."[625]

This case underscores the growing impatience courts have towards poorly selected search terms and reemphasizes the need for cooperation and the importance of quality control to ensure thorough, focused discovery. Furthermore, after such a strongly worded and clearly articulated opinion, this court is (and possibly other courts are) more likely to impose sanctions and attorney's fees when parties fail to implement the outlined discovery procedures.

As technology has evolved and alternative forms of search have emerged (e.g. technology assisted review, See Section 9.1.2), keyword searches have suffered some criticism from vendors and litigants alike. All is not lost, however, as some courts still believe. With fewer than four months remaining on the bench, Magistrate Judge Nan Nolan brought closure to a heated discovery dispute in the high-profile *Kleen Products, LLC et al. v. Packaging Corporation of America, et al.*, 1:10-cv-05711 case. At issue in the dispute was plaintiffs' motion to order defendants into a do-over on their document collection and production process. The plaintiffs moved the court to require defendants to use alternative technology (suggesting either "predictive coding" or "content-based advanced analytics") as opposed to the custodian-specific keyword search the defendants had already employed. The request came at a time when defendants were nearly finished with their collection and were preparing for production. As could be anticipated, the plaintiff's untimely motion provided an even more contentious discord between the parties.

Apart from parties' willingness or unwillingness to cooperate on discovery issues, the idea of technology assisted review has come to top of the agenda in many e-discovery discussions. Often overshadowed in these discussions is the continued need to use keywords in some capacity to search, collect cull, and review electronically stored information. In fact, keywords can be the starting point for initial sample set used to train the predictive coding algorithms. And since most litigants

622 Id. at 134-35.

623 Id. at 134.

624 Id. (citing Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 260 (D. Md. 2008); United States v. O'Keefe, 537 F. Supp. 2d 14 (D.D.C. 2008)).

625 Id. at 136.

have experience negotiating keyword lists, this continues to be a good starting point for identifying potentially relevant data.

Judge Nolan made a herculean effort to move the discovery disputes along in this case. At one of the many discovery hearings, she foreshadowed her likely decision on plaintiff's motion should they continue down the path of asking for the imposition of a completely different technology by stating her support for The Sedona Conference Principles for Electronic Document Production, Principle 6: Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.

Perhaps if the parties had employed The Sedona Conference Principle 3 early in the discovery process, they could have avoided this costly expedition and monopolization of the court's precious resources.

> *Parties should confer early in discovery regarding the preservation and production of electronically stored information when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities.*

In one of the more straightforward statements to the court, counsel for one defendant speaking on behalf of all defendants stated:

> *We really believe both sides are trying to do the same thing which is to figure out who are the people and where are the places in the company where responsive, relevant information exists and how can we get it produced?*
>
> *The difference is that because the plaintiffs are obviously coming to this without having worked at these companies, they need to describe things in a certain level of generality, and the companies very familiar with how their businesses work have attempted to identify the actual people who are doing the things that are the subject matter of the plaintiffs' complaint.*

If only it were that easy. The asymmetrical nature of this antitrust case could mean plaintiffs' counsel's discovery detour is more tactical than substantive. Plaintiffs produced less than 1% of the volume of documents, compared to the cumulative total of the seven defendants (roughly 25,000 pages for plaintiffs compared to around 3 million pages, with additional productions likely to happen in the coming months for defendants). Waiting until the defendants were 99% finished with their collection and processing to demand an alternative approach would not likely have occurred in a case where the moving party would be subjecting itself to the same costs and burdens it is asking the court to impose on the other party. Incidentally, it is not clear if the plaintiffs employed the same technology for their collection and production that they asked the court to impose on the defendants.

Ultimately, Judge Nolan was able to inform the plaintiffs enough that they withdrew their motion, leaving one to conclude that in the famous words of Samuel Clemens (better known as "Mark Twain"),

the son of a not-so-famous attorney and judge, "the reports of my death are greatly exaggerated." So too are the reports of the death of keywords.

Cases continue to affirm the use of keywords for searching and identifying relevant ESI. Some examples are as follows:

E.I. Du Pont De NeMours & Co. v. Kolon Indus.[626]

In this trade secret misappropriation case, plaintiff sought fees and expenses for its spoliation sanctions motions, as the court had previously ordered an adverse inference instruction and expenses, costs, and fees as a sanction. The defendant argued that the sanction should be reconsidered in light of plaintiff's misuse of search terms, which defendant argued were overbroad and inefficient. The court rejected defendant's arguments, finding plaintiff's terms reasonable, and granted the application for attorneys' fees and expenses.

Neustar, Inc. v. F5 Networks, Inc.[627]

In this dispute over search terms in a breach of license agreement case, the court agreed with defendant that plaintiff had not shown good cause for using terms that would return 60,000 rather than 20,000 documents defendant's terms generated. The court ordered that defendant's should be used in the search.

Potts v. Dollar Tree Stores, Inc.[628]

The defendant sought physical production of plaintiff's computer in this Title VII and Equal Pay Act case. Plaintiff objected to the production. The court directed the parties to agree to a word search of the plaintiff's computer by an agreed neutral party to assess whether the plaintiff's computer contained relevant information.

Robert Bosch LLC v. Snap-on Inc.[629]

In this patent infringement case, the plaintiff moved to compel production, *inter alia*, of documents based on two search terms: (diagnostic! and test!) and ([ECU or "electronic control unit"] and diagnostic!). Defendant objected that the terms were overbroad and commonly used, as well as redundant of searches of variations of product names that it had agreed to run. The court found that the proposed search terms could hit on documents outside of the defendant's prior search, and also found that the terms were not overbroad. Accordingly, it granted the motion with respect to the terms. However, the court also ordered that defendants may use techniques to limit over production, including filtering by where terms appear (*e.g.,* only in the email signature), and proximity connectors.

626 2013 WL 458532 (E.D. Va. Feb. 6. 2013).
627 2013 WL 1755489 (N.D. Cal. Apr. 24, 2013).
628 2013 WL 1176504 (M.D. Tenn. Mar. 20, 2013).
629 2013 WL 1018080 (E.D. Mich. Mar. 14, 2013).

Creating a Defensible Search Strategy

The first step to a defensible search is to understand some basic search terminology:

1. Responsive: ESI that is relevant and retrieved;
2. False positives: ESI that is not relevant but is retrieved;
3. False negatives: ESI that is relevant and not retrieved; and,
4. Non-responsive: ESI that is not relevant and not retrieved.

The goal of an effective and accurate search is to minimize the false positives and false negatives.

Keywords can be searched using a simple list of words or coupled with more advanced keyword searches using "Boolean" operators, proximity, and GREP expressions (a command-line text search utility originally written for Unix). In terms of search speed, a keyword search without any expressions is the fastest for upfront collections, followed by, Boolean, GREP, and proximity searches, in that order.

A defensible keyword strategy requires an iterative approach: (1.) negotiating search terms with opposing counsel, (2.) running the agreed searches, (3.) reviewing the search results, and (4.) adjusting the searches through a series of meet-and-confers and data sampling.

Best Practices

1. Create a broad list of keyword terms and refine:

    a. Too many keywords can slow down collection/processing and create false positives. In most cases, using more than 100 keywords will not be as effective as using carefully crafted search terms.
    b. Check keywords for grammar, spelling, and case-sensitivity.
    c. Interview the potential witnesses for keyword clues.
    d. It is important to understand the context and lingo in which the target populations of documents were created in order to target words they might have used when creating documents.
    e. Review all known evidence for keyword clues.
    f. Discuss the case with opposing counsel for possible keyword clues.

2. Reducing False Positives (over-inclusive results):

    a. Conduct random sampling of the responsive data to test the effectiveness of the key search terms. Sampling potentially responsive data after applying keywords and adjusting the key search terms will achieve better results.
    b. Conduct random sampling of the nonresponsive data to ensure the search criteria isn't missing potentially responsive evidence.

c. Review all false positive hits. Think carefully about the context of each keyword. If the keyword is a *common* word or phrase, first determine whether there is another *uncommon* word or phrase that will identify the same file. If you can simply replace the inefficient word or phrase with an efficient term, your collection/processing will proceed more quickly than if you employ Boolean or proximity searching.
d. Avoid using custodian names or company names, as these will be in every email address and signature line.
e. Avoid using the names of software or hardware used in the target computer environment as a key term; For example, trademarks such as Microsoft, Adobe, Norton, McAfee, Dell, IBM, Mac, etc.
f. If the keywords are generating false-positive hits, determine whether a more complex term may be used. If the term is an acronym (e.g. CIA is hitting on fa*cia*l) making CIA case-sensitive will help reduce false positives.
g. If there is not another word or phrase that can replace the inefficient term, determine whether another word or phrase in conjunction with the original term will eliminate the false-positive hits. If the existence of two terms within the same document will greatly reduce false positives, use Boolean.
h. If Boolean connectors do not sufficiently reduce false-positive hits, determine the maximum proximity of two terms (how many words apart) and use a proximity approach.

3. Broadening too restrictive terms (under-inclusive results):

a. If a greater number of hits were expected, the search term may be too restrictive.
b. Sample the target data set for false negatives.
c. Always review terms that return zero or few positive hits.
d. Check grammar to determine if it represents the way that a target custodian is likely to type the term.
e. Would abbreviation or hyphens be used?
f. Would two words rather than a sentence be more appropriate?
g. When using white-spacing techniques, consider stemming.

Because of these limitations, cooperation by both parties during a Rule 26(f) meet-and-confer conference is now critical to a successful production.[630]

In sum, keywords when used properly, remains a highly defensible and effective search technique from collection through review. The important point to remember is that civil discovery is based on good faith and reasonableness, not Euclidean precision.

630 See William A. Gross Constr. Assocs. v. Am Mfrs. Mut. Ins. Co., 256 F.R.D. 134 (S.D.N.Y. 2009); Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354 (D. Md. 2008).

§ 9.9.2 Technology Assisted Review

Technology-assisted review (TAR), also referred to as "computer-assisted" review has been a most prominent technology development affecting e-discovery in the past few years. The utility of a particular type of algorithm-driven review, known as "predictive coding" was recently challenged and upheld in the *Da Silva Moore*[631] case, a decision rendered by Magistrate Judge Andrew Peck and confirmed by US District Judge Andrew Carter[632]. Under the new technology, lawyers review a sample set of documents for relevancy and privilege. That sample review set then informs the "artificial intelligence" of the predictive coding software to do the same for the remainder of the document collection in an iterative process.

Predictive coding is considered by some to be the next evolution in e-discovery technology for legal applications, entirely supplanting keyword searching and linear review. But many questions remain, including how the economics of predictive coding fit into e-discovery and what the minimum volume of documents are required to justify its use. Any new technology that challenges the status quo is often met with skepticism, but in the litigation arena where millions of dollars and the law may be at issue, the process of adopting a new technology is even more cautious and deliberate. While predictive coding offers the promise of potentially faster, less expensive e-discovery, questions still remain about its widespread adoption.

It is important to understand that predictive coding does not replace most of the electronic discovery process. It is a supplemental tool that can be beneficial in reducing costs. Yet litigants considering a predictive coding solution should not be lulled into thinking a few court opinions warrant a wholesale change in their approach to e-discovery. A few of the more noteworthy predictive coding cases are discussed below.

As mentioned above, US Magistrate Judge Andrew Peck issued the first known order approving the use of predictive coding as an acceptable way to search for relevant ESI in *Da Silva Moore v. Publicis Group*. Judge Peck acknowledged that predictive coding may not be appropriate in all cases, but can be a valuable tool in "large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review."[633]

Plaintiffs in this case expressed concerns regarding the use of predictive coding, including its reliability. The Court held that plaintiffs' concerns regarding reliability were premature, especially in light of plaintiffs' ability to participate in the electronic discovery process in a "checks and balance" capacity.[634] The transparent process consisted of the defendant providing plaintiffs' counsel with all of the non-privileged documents from the seed or sample set and the issue tag(s) coded for each document so that plaintiffs could check the accuracy of the computer's predictions before they were applied to the remaining documents.

Judge Peck ruled:

631 Da Silva Moore v. Publicis Group, No. 11-CV-1279, 2012 US Dist. LEXIS 23350 (S.D.N.Y. Feb. 24, 2012).

632 Da Silva Moore v. Publicis Group, No. 11-CV-1279, 2012 US Dist. LEXIS 58742 (S.D.N.Y. April 26, 2012).

633 Da Silva Moore at 40.

634 Id. at 24-26.

> "[the] use of predictive coding was appropriate considering: (1) the parties' agreement [to use the process], (2) the vast amount of ESI to be reviewed (over three million documents), (3) the superiority of computer-assisted review to the available alternatives (i.e., linear manual review or keyboard searches), (4) the need for cost effectiveness and proportionality under Rule 26(b)(2)(C), and (5) the transparent process proposed by [defendant] MSL."[635]

Whereas *Da Silva Moore* was the first federal court opinion on predictive coding, the first known state court order approving the use of predictive coding for electronic discovery came from Virginia Circuit Court Judge James H. Chamblin in *Global Aerospace Inc. v. Landow Aviation, L.P. d/b/a Dulles Jet Center*[636]. Here, defendants filed a motion asking the court to approve the use of predictive coding when the parties could not agree regarding how to review the large volume of documents in defendants' possession that were potentially relevant to the lawsuit.

Defendants argued that a traditional, manual review of the documents would cost an estimated $2 million. Defendants also argued that using predictive coding would lead to the location of more responsive documents than a traditional manual review. Plaintiffs objected to the use of predictive coding on the grounds that it was not as effective as traditional manual review and that, regardless of the process implemented, defendants should produce all responsive documents. Judge Chamblin approved the use of predictive coding despite the plaintiffs' objection that traditional manual review of electronic discovery would yield more accurate results and noted that plaintiffs are not without recourse, as they are still permitted to "raise with the Court an issue as to completeness or the contents of the production or the ongoing use of predictive coding." In the short term, the potential exists for subsequent state court cases concerning predictive coding to have dramatically different outcomes given the complexity of the technology and the lack of a national standard.

Following closely on the heels of Judge Peck's *Da Silva Moore* opinion was a case in the Seventh Circuit that appeared to be headed to the top of the list of predictive coding cases. In *Kleen Products LLC v. Packaging Corp of America*[637], the parties litigated the question of whether the plaintiffs could force the defendants to be required to utilize predictive coding to conduct their e-discovery review prior to producing documents to plaintiffs. The Court held several days of evidentiary hearings on the issue, at which point Judge Nan Nolan strongly suggested to the plaintiffs that the timeliness of their request was improper given the near 99% completion of the defendant's traditional review. Eventually, the parties entered into a stipulation, wherein the plaintiffs agreed that they would not argue the need for defendant's to use predictive coding for any documents produced in response to discovery requests served prior to October 1, 2013.

In one of the more recent predictive coding opinions, Judge Robert Miller, Jr., of the United States District Court for the Northern District of Indiana, in the *In re Biomet M2a Magnum Hip Implant*

635 Id. at 35-36. US District Judge Andrew Carter subsequently adopted Judge Peck's opinion on April 26, 2012. See Da Silva Moore v. Publicis Group, No. 11-CV-1279, 2012 US Dist. LEXIS 58742 (S.D.N.Y. April 26, 2012).

636 Global Aerospace Inc. v. Landow Aviation, L.P. d/b/a Dulles Jet Center, No. CL 61040 (Vir. Cir. Ct. Apr. 23, 2012).

637 Kleen Products LLC v. Packaging Corp of America, 1:10-cv-05711 (N.D. Ill. Aug. 21, 2012).

Products Liability Litigation[638] case issued an order on April 18, 2013 authorizing predictive coding by the defendant despite the fact that the defendant proceeded with e-discovery before the cases were centralized, and ignored plaintiff directives to not begin document production until the MDL had been confirmed.

In his order, Judge Miller noted that Biomet had produced 2.5 million documents to plaintiffs, and the Plaintiffs' Steering Committee believes production results should be close to 10 million documents. The cases were centralized in the summer of 2012. Judge Miller went on to say:

> Biomet used a combination of electronic search functions to identify relevant documents. Keyword culling was used first, reducing the universe of documents and attachments from 19.5 million documents to 3.9 million documents, comprising 1.5 terabytes of data. Removal of duplicates left 2.5 million documents and attachments. Statistical sampling tests of a random sample projected, with a 99 percent confidence rate, that between .55 and 1.33 percent of the unselected documents would be responsive and (with the same confidence level) that between 1.37 and 2.47 percent of the original 19.5 million documents were responsive. In comparison, Biomet's keyword/de-duplication approach had identified 16 percent of the original 19.5 million . . .
>
> Biomet invited the Plaintiffs' Steering Committee to suggest additional search terms and offered to produce the rest of the non-privileged documents from the post-keyword 2.5 million so the Steering Committee can verify that Biomet is producing the relevant documents. The Steering Committee has declined those offers, believing they are too little to assure proper document production.
>
> The steering committee contended that Biomet's initial use of the keyword approach tainted the process, and that the company "began with the less accurate keyword search." It asked the court to direct Biomet to return to the original documents, and using predictive coding, have both plaintiffs and defendants jointly enter the "find more like this" commands. Biomet cited a variety of grounds, including costs. "The Steering Committee responded that Biomet gambled when it spent millions on document production that several of plaintiffs' counsel warned Biomet not to undertake until the Panel had centralized the cases."

Judge Miller ruled that the defendants were not required to begin from the beginning, weighing the proportionality of the cost of starting over against the alternative approach proposed by the plaintiffs. In essence, defendants took the risky approach of asking for forgiveness rather than permission and it paid off this time.

As with the introduction of any new technology, especially in a field as sensitive to protocol and tradition as the law, the initial forays into the use of predictive coding have been met with skepticism

638 In re: Biomet M2a Magnum Hip Implant Products Liability Litigation; No. 3:12-MD-2391 (N.D. Ind. Apr. 18, 2013).

and reluctance. Predictive coding, despite its touted cost-savings, is expensive as a one-time use.[639] Courts and litigants have also recognized that in cases with a low volume of relevant documents, parties are not required to retain a single discovery vendor to apply predictive coding and can conduct document review using traditional methods.[640] As time goes on and more decisive action on the part of policymakers and guidance from more courts becomes more mainstream, TAR could be brought more into the mainstream of e-discovery practice. Moreover, more cost-effective and comprehensive TAR technologies, not based on algorithm-driven review, are likely to evolve.

§ 9.10 Privilege

The exponential growth of electronically stored information (ESI) that must be preserved and the inability to properly segregate those documents has had an enormous impact on an organization's ability to preserve privileged information. The result has been that privileged and non-relevant documents have been produced to opposing parties in litigation; this has often resulted in the waiver of protections normally afforded a producing party.

In 2008, Evidence 502 (Rule 502) was amended. The amendments to Rule 502 provide guidance as well as better legal protection for a claim of inadvertent waiver of privileged communications involving ESI. The core protection amended Rule 502 provides is a reduction of the risks associated with large volume ESI productions. (*See Real eDiscovery, Winter 2010, Protecting Privilege with FRE 502 by Patrick Oot, Esq. and John J. Rosenthal, Esq.).*

The following are some of the more notable cases on this topic:

In *Green v. Beer,*[641] where, in light of plaintiffs' lack of e-mail proficiency, plaintiffs' son received privileged e-mails from plaintiffs' counsel and then passed them on to his parents, the district court reversed a finding by the Magistrate Judge that privilege was waived and held that, because the son was "a necessary conduit in delivering the attorney's confidential emails," the privilege was not waived.

Taking up the issue, the district court identified an exception to the principle that communications involving third parties are generally not privileged where "the purpose of the communication [to a third party] is to assist the attorney in rendering advice to the client" and where the party asserting the privilege can establish that the client had a reasonable expectation of privacy with respect to the communication at issue, and that disclosure to the third party was necessary for the client to obtain informed legal advice. The court further established that disclosure to an agent of the attorney or the client does not result in waiver. The court held that:

> A finding that privilege has not been waived in this case is appropriate as a matter of public policy. Email permits attorneys and their clients to engage in prompt communication, often regarding time-sensitive matters. A client lacking proficiency in Internet technology should not be prevented from enjoying the advantages of email

639 One court awarded $2.9 million in fees for a one-time use of predictive coding for the review of 12 million record. Gabriel Technologies v. Qualcomm, 2013 WL 410103 (S.D. Cal. Feb. 1, 2013).

640 EORHB, Inc. v. HOA Holdings LLC, 2013 WL 1960621 (Del. Ch. May 6, 2013).

641 2010 WL 3422723 (S.D.N.Y. Aug. 24, 2010).

> correspondence for fear that the necessary assistance of a third party--here, the Green Plaintiffs' son--in sending or receiving such correspondence will lead to the forfeiture of the attorney-client privilege.

Community Bank vs. Progressive Casualty Insurance Company[642]

In this insurance litigation, the plaintiff requested a protective order to prevent defendant's use of privileged material and work product inadvertently disclosed by a non-party as evidence in a summary judgment motion.

Although the plaintiff had previously returned privileged documents inadvertently sent to the defendant on numerous occasions, the court found the defendant's assurances that it would afford the plaintiff the same courtesy were "too amorphous to be binding." The use of the word "courtesy" instead of "agreement" in the parties' communications demonstrated that the expected reciprocal conduct was moral in nature, not a legal right, and the communications did not reference applicability to non-parties.

Citing Fed.R.Evid. 502(b), the court also found the plaintiff took no reasonable precautions to prevent the disclosure since no supervision of the non-party's production occurred. However, the court determined that the defendant violated Fed.R.Civ.P. 26(b)(5) by using the privileged exhibits in its summary judgment motion prior to resolution of the dispute.

Based on this behavior, the court ordered the defendant to pay one-half of the plaintiff's fees and costs associated with the motion, and prohibited use of the exhibits as substantive evidence.

Stengart v. Loving Care Agency, Inc.[643]

Employers who wish to investigate employee electronic communications need to have clearly articulated written policies that employees do not have any expectation of privacy in their usage of employer-provided computers.

In *Stengart*, a former employee sued her employer for violating New Jersey's Law Against Discrimination. In response, the employer searched the former employee's company-owned laptop computer and found, in the web browser's history, e-mails she had exchanged with her attorney using her own private, password-protected e-mail account. The e-mails were obtained by the forensic imaging of the employee's company-owned computer.

The employer contended that the employee waived her privilege by using the company's computer to send e-mails to her attorney, citing the company's electronic communications policy, which stated, "[o]ccasional personal use is permitted" and then described several prohibited uses, including soliciting for outside business ventures or charitable organizations, or sending inappropriate sexual, discriminatory, or harassing messages.

However, in an effort to protect attorney-client communications, the court concluded that "[a]

642 08-cv-1443 (WTL/WGH) (S.D. Ind. 2010) (slip op.).
643 990 A.2d 650 (N.J. 2010).

s written, the policy create[d] ambiguity about whether personal email use is company or private property when using a company owned computer."

If the attorney-client privilege was not an issue, this case would likely have been decided differently. Although the court correctly held Stengart had a limited expectation of privacy when communicating via e-mail with her lawyer, the court cited the ambiguity of the policy as the reason for its decision. In fact, the court went on to say that "companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies."

Thorncreek Apartments III, LLC v. Village of Park Forest[644]

It's the nightmare scenario that litigators hope will never happen to them: the waiver of privilege. However, this nightmare became a reality for a litigant in a case in the Northern District of Illinois in 2011. United States Magistrate Judge Sidney Schenkier ruled that a party's inadvertent disclosure waived their rights to maintain certain documents as privileged.

Defendant Village of Park Forest was using a third-party vendor, Kroll Ontrack, to help manage e-discovery in litigation with Plaintiff Thorncreek. Together, the Village and Kroll developed a three-step review process of the data, which was located on backup tapes. The first step involved using both agreed-upon and court-ordered search terms. The second step of the process involved Kroll Ontrack making all the search results available to a Village attorney to review for responsiveness and privilege. The third step of the process allowed counsel for Thorncreek to review the documents that were left after the Village attorney's review.

The Village, however, did not realize an issue had arisen until counsel for Thorncreek attempted to use a privileged document in a deposition in December of 2009. The Village's counsel objected to the use of the document at the deposition. Attorneys for the Village did not turn over a privilege log until April of 2010, which contained 159 documents. Parties were able to reduce this list to six documents.

The Court determined that parts of the remaining six documents were in fact privileged. The Court's analysis then turned to determining whether the Village had waived disclosure. The issue to determine was whether the Village took reasonable steps after it was realized that documents were inadvertently produced, pursuant to FRE 502.

Judge Schenkier took issue with the process that the Village and Kroll Ontrack developed for the production of documents. "We have little confidence in the reasonableness of the Village's precautions when the most the Village can say is that it 'thought' that marking documents as 'privileged' during its review would cause Kroll to withhold it from the production database that Thorncreek could later view." *Id*. at 6. The Court suggested that the Village should have reviewed the database of documents which were going to be produced to Thorncreek before the database became available to the plaintiff. "Thus, the Village's procedures for privilege review were completely ineffective, each and every document the Village sought to retain as privileged was inadvertently disclosed." *Id*.

644 2011 U.S. Dist. LEXIS 88281 (N.D. Ill. Aug. 9, 2011)

As this case demonstrates, organizations cannot simply delegate their e-discovery obligations to the services of a third-party vendor. Having a truly defensible, repeatable, in-house e-discovery process requires proactive and persistent involvement from both corporate legal and IT, as well as having the right technology in place. While missteps and unforeseen events are bound to happen during the course of any litigation, having the right in-house technology enabling defensible collection and review makes you less likely to have a court find "little confidence" in your e-discovery, and to avoid the nightmare scenario that took place in this case.

Holmes v. Petrovich Dev. Co., LLC[645]

Here, the trial court did not err in finding that correspondence with employee's attorney sent from her work computer was not privileged, where the employee was aware of policies prohibiting personal use and notifying employees that files and messages would be monitored, and that there was no right of privacy as to information created or maintained on company computers.

In re Fontainebleau Las Vegas Contract Litig.[646]

In this case, the court found that privilege had been waived where a third party produced servers without conducting a review of the contents. The court took into consideration the fact that privileged materials were stored on a server shared with other entities who presumably had access to those materials, a fact which would also likely result in waiver.

In *Pacific Coast Steel, Inc. v. Leany*,[647] the court denied defendants' motion for a protective order and for the return of allegedly privileged documents where defendants failed to take reasonable means to preserve confidentiality. The court cited, for example, defendants failing to remove privileged e-mail from a server sold to plaintiffs or to prevent those e-mails from entering plaintiffs' system, and an individual defendant's failure to request the return of those emails or the removal from the system upon his termination from plaintiffs' corporation, despite accepting a copy of his computer and other files and his alleged representation by counsel.

§ 9.11 Proportionality

The decision by Judge Rosenthal in *Rimkus Consulting Group, Inc. v. Cammarata*[648] demonstrates that the federal judiciary is now waking up and using proportionality to determine what is reasonable and acceptable in preservation and discovery conduct. Additionally, Judge Grimm in *Victor Stanley, Inc. v. Creative Pipe, Inc.*,[649] stated, "courts have tended to overlook the importance of proportionality in determining whether a party has complied with its duty to preserve evidence in a particular case, this

645 119 Cal. Rptr. 3d 878 (Cal. Ct. App. 2011).
646 2011 WL 65760 (S.D. Fla. Jan 7, 2011).
647 No. 2:09-cv-12190-KJD-PAL, 2011 WL 4573243 (D. Nev. Sept. 30, 2011).
648 688 F. Supp. 2d 598 (S.D. Tex. 2010).
649 Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (D. Md. 2010).

should not be the case because Fed. R. Civ. P. 26(b)(2)(C) cautions that all permissible discovery must be measured against the yardstick of proportionality." As Judge Waxse recently stated, "We don't need to change the rule; we need to start using the rule."

The notion of "proportionality" is evident in both e-discovery cases and the Federal Rules of Civil Procedure. Both sources recognize that the duty to preserve, as well as the sanctions for failure to do so, should be in proportion to the matter at issue.

FRCP Rule 26(b)(2)(C) states:

> On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:
>
> (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
>
> (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
>
> (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

The Sedona Principles Addressing Electronic Document Production (2007) similarly state, "Electronic discovery burdens should be proportional to the amount in controversy and the nature of the case; [o]therwise transaction costs due to electronic discovery will overwhelm the ability to solve disputes fairly in litigation."[650]

In a more recent examination of proportionality, the Sedona Conference Commentary on Proportionality in Electronic Discovery states that, despite the recent amendments to the federal rules, "courts have not always applied proportionality in circumstances when its application was warranted (*internal citation omitted*). When courts have applied proportionality, they have not always described it as such (*internal citation omitted*). In the electronic era, it has become increasingly important for courts and parties to apply the proportionality doctrine to manage the large volume of ESI and associated expenses now typical in litigation."[651]

Consistent with the Sedona Conference's emphasis on proportionality, the American College of Trial Lawyers Task Force on Discovery and the Institute for the Advancement of the American Legal System's March 11, 2009 Final Report states that, "Proportionality should be the most important principle applied to all discovery."[652] The report goes on to state that "parties and counsel should

650 Id. at 513.

651 The Sedona Conf., The Sedona Conference Commentary on Proportionality in Electronic Discovery, 11 Sedona Conf. J. 289, 293 (2010).

652 Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (D. Md. 2010).

attempt in good faith to agree on proportional discovery at the outset of a case but failing agreement, courts should become involved. There simply is no justification for the parties to spend more on discovery than a case requires."[653]

More and more, courts are gaining an understanding of the significant, out-of-control costs surrounding electronic discovery and starting to apply the rules to reign in the parties. And despite a party's requirement to estimate and disclose the potential value of a case to the court and opposing counsel in order to invoke a proportionality argument, it is an unavoidable necessity to limit excessive costs borne from discovery fishing expeditions. Even in circumstances where estimating the value of a case early on in the litigation is claimed to be too speculative, courts have found a way to invoke the proportionality argument.

For example, in *Mancia v. Mayflower Textile Services Co.*, a FLSA wage and hour case, Judge Grimm declared that the record before him lacked the sort of factual information he required to make a proportionality determination on its face. Thereafter, he ordered counsel to meet and confer as to the likely range of damages that could be anticipated to be awarded to the plaintiffs if they prevailed at trial.[654] Where a party is likely to overestimate the value of case at the outset, leveraging the cost of discovery against this overestimate serves as a powerful strategy.

Judge Grimm continued his emphasis on proportionality in *Victor Stanley II,* when he stated that "courts have tended to overlook the importance of proportionality in determining whether a party has complied with its duty to preserve evidence in a particular case, this should not be the case because Fed. R. Civ. P. 26(b)(2)(C) cautions that all permissible discovery must be measured against the yardstick of proportionality."[655]

In *Bellinger v. Astrue*, a case involving a Title VII claim where the plaintiff claimed she was denied a promotion and received unequal pay because of her gender, the court sustained the defendant's objection to discovery requests seeking a substantial amount of information that "[t]he likely benefit of the discovery . . . is slight or non-existent, particularly in light of the narrow scope of the plaintiff's claims and the broad range of discovery that has already been produced."[656]

And while most of the ESI proportionality issues addressed by the courts have involved FRCP Rule 26(b), Rule 26(g)(1) plays an arguably even more important role in advancing proportionality in civil litigation. It is quietly becoming the federal judiciary's rule of choice in enforcing discovery issues.

Rule 26(g)(1) states in part:

> Every disclosure under Rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney of record in the attorney's own name—or by the party personally, if unrepresented—and must state the signer's address, e-mail address, and telephone number. By signing, an attorney or party

653 Id.

654 253 F.R.D. 354, 364 (E. Md. 2008).

655 Victor Stanley, Inc.,, 269 F.R.D. at 497.

656 No. 06-CV-321 (CBA)(SMG), 2010 WL 1268063 (E.D.N.Y. Apr. 2, 2010).

certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry:

(A) with respect to a disclosure, it is complete and correct as of the time it is made; and

(B) with respect to a discovery request, response, or objection, it is:

(i) consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law;

(ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and

(iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.

The court in *Mancia, supra,* stated that Rule 26(g)(1) is "[o]ne of the most important, but apparently least understood or followed, of the discovery rules." Unfortunately most of the early emphasis on Rule 26(g)(1) has involved responding to parties' failures to comply. (See, *R & R Sails v. Insurance Co. of State of PA*[657] (court sanctioned defendant and trial counsel nearly $40,000 for failure to include computer-based claim logs along with the paper claim file.) However, cases such as *Mancia* have exposed the requesting party to proportionality analysis under (B)(ii) and have given responding parties ammunition to push back on overly broad discovery requests.

In *Pippins v. KPMG LLP*,[658] the court denied defendant's motion seeking to limit its preservation obligation related to thousands of hard drives belonging to potential class members where the defendant "failed to establish that the contents of the disputed hard drives were not relevant," "failed to establish that the hard drives do not relate to 'key players' in the litigation" (reasoning that any of the individual Audit Associates could be a "key player" in "any one of many potential actions" if the Motion to Certify was denied), and because "KPMG ha[d] not demonstrated that the materials it [sought] to dispose of [were] duplicative of materials that are already subject to its preservation efforts." The court also indicated its reluctance to apply the principle of proportionality to preservation obligations.

Focusing on cooperation and proportionality, the court in *Kleen Prods. LLC v. Packaging Corp. of Am*[659].resolved discovery disputes regarding the identification of an additional custodian and the restoration of backup tapes, among other things, and granted defendant's motion for a protective order precluding its obligation to respond to follow-up discovery regarding recipients of its litigation

657 251 F.R.D. 520, 528 (S.D. Cal. 2008).

658 No. 11 Civ. 0377 (CM)(JLC), 2011 WL 4701849 (S.D.N.Y. Oct. 7, 2011).

659 No. 10 C 5711, 2012 WL 4498465 (N.D. Ill. Sept. 28, 2012).

hold letter. The court also granted plaintiffs' request for additional custodians from two defendants, although it limited the increase to eight additional custodians from each. Finally, the court denied plaintiff's motion to compel defendants to search their backup tapes after defendants were able to demonstrate that doing so would impose an undue burden.

Courts examining the doctrine of proportionality, whether raised by the requesting or responding party, face a complex analysis and a balancing of many factors. Complicating these factors will be the continued evolution of technology and the uncontrollable proliferation of ESI.

The Sedona Conference® Principles of Proportionality

1. The burdens and costs of preservation of potentially relevant information should be weighed against the potential value and uniqueness of the information when determining the appropriate scope of preservation.
2. Discovery should generally be obtained from the most convenient, least burdensome, and least expensive sources.
3. Undue burden, expense, or delay resulting from a party's action or inaction should be weighed against that party.
4. Extrinsic information and sampling may assist in the analysis of whether requested discovery is sufficiently important to warrant the potential burden or expense of its production.
5. Nonmonetary factors should be considered when evaluating the burdens and benefits of discovery.
6. Technologies to reduce cost and burden should be considered in the proportionality analysis.

§ 9.12 Social Networking

Social networking (or social media) is the term used to describe websites, such as Facebook, MySpace, and LinkedIn, which allow users to publish personal and professional information, and connect and interact with other users via web-based technologies. Due to the ease-of-use and instantaneous manner in which it provides information to users, social networking is becoming one of the most popular forms of communication today. Many in-house legal departments are recognizing the ever-increasing use of social media by their employees, and have taken steps to try to either curb or control the use of these websites. While the impact of social networking upon electronic discovery is still in its earliest stages, the following cases demonstrate its potential for being a prevalent issue in the years to come.

EEOC v. Simply Storage Mgmt., LLC[660]

EEOC brought Title VII action against employer alleging sexual discrimination by the supervisor. Defendant sought discovery of social networking site ("SNS") profiles or other communications from

660 No 1:09-cv-1233-WRL-DML, 2010 WL 3446105 (S.D. Ind. May 11, 2010).

Facebook and MySpace.com. Court determined that (1) SNS content was not shielded from discovery simply because it was designated "locked" or "private"; (2) SNS content is discoverable when relevant to a claim or defense of a case; and (3) allegations of extreme emotional distress and post-traumatic stress disorder merited limited discovery of SNS content and communications.

Barnes v. CUS Nashville[661]

In this series of orders, Facebook, Inc. objected to a subpoena to produce information from the account of a nonparty witness. The court found that the Secured Communications Act ("SCA") prohibits disclosure of the information from Facebook. In the later order, the court determined that in order to expedite discovery, the Magistrate Judge would create a Facebook account for the sole purpose of reviewing photographs and related comments *in camera*.

Crispin v. Audigier[662]

Plaintiff filed suit against a garment manufacturer and other defendants alleging breach of an oral license to use his works of art in the production of streetwear apparel. Defendants served third-party subpoenas on several social networking websites, including Facebook and MySpace, Inc. seeking communications sent by plaintiff.

The court found that the private messaging and e-mail webmail services constituted electronic communication services (ECS) under the Stored Communications Act (SCA), and that the web-hosting website and SNS were ECS providers under the SCA. Accordingly, because the webmail and private messaging communications were inherently private, *i.e.*, not reasonably accessible to the general public, they were prohibited from disclosure under the SCA.

As to subpoenas seeking Facebook wall postings and MySpace comments, the court requested additional evidence as to whether the general public has access to this information, specifically, the plaintiff's privacy settings.

Griffin v. State[663]

Criminal defendant convicted of second-degree murder sought appeal based on the trial court's admission of a page from a MySpace profile indicating that the defendant's girlfriend threatened a key witness to dissuade his testimony.

The appellate court found that the evidence was sufficient to authenticate the MySpace profile printout. The printout featured a photograph of the defendant and his girlfriend in an embrace, contained the user's birth date, and identified the defendant by a known nickname. The defense proffered no evidence to dispute the accuracy of the State's evidence.

---

661 No. 3:09-0764, 2010 WL 2196591 (M.D. Tenn. May 27, 2010); 2010 WL 2265668 (M.D. Tenn. Jun. 3, 2010).

662 No. CV-09-09509 MMM, 2010 WL 229323 (C.D. Cal. May 26, 2010).

663 995 A.2d 791 (Md. Ct. Spec. App. 2010).

McCann v. Harleysville Insurance Company of New York[664]

Order denying a motion to compel disclosure of a Facebook account in a personal injury action. The appellate court reasoned:

> [defendant] failed to establish a factual predicate with respect to the relevancy of the evidence. Indeed, defendant essentially sought permission to conduct a 'fishing expedition' into plaintiff's Facebook account based on the mere hope of finding relevant evidence.

Ledbetter v. Wal-Mart Stores, Inc.[665]

District Court of Colorado denied plaintiffs' motion for a protective order for their Facebook, MySpace, and Meetup.com pages, reasoning that plaintiffs had put their personal physical and mental states at issue, and the confidentiality protective order entered in the case would adequately address any potential privacy concerns.

Moreno v. Hanford Sentinel, Inc.[666]

California appellate court held plaintiff's MySpace post public even though it was deleted, and thus plaintiff could not maintain an invasion of privacy suit against the defendant, who had republished the posting.

Mailhoit v. Home Depot U.S.A., Inc.[667]

The court found that the defendant's requests for social-media content belonging to the plaintiff failed to describe the information to be produced with Rule 34(b)(1)(A)'s "reasonable particularity" requirement and were therefore not reasonably calculated to lead to the discovery of admissible evidence. The court therefore denied most of the defendant's motion to compel.

Offenback v. L.M. Bowman, Inc.[668]

Defendants in this case requested an in-camera review of the plaintiff's Facebook and MySpace accounts, arguing the plaintiff's claims of physical and psychological impairment made relevant any evidence that documented the plaintiff's social life, physical capabilities and emotional state of mind. To the extent that such information was relevant under Fed.R.Civ.P. 26, the plaintiff agreed that limited public information on his Facebook account was discoverable. Thereafter, plaintiff provided

664 78 A.D.3d 1524 (N.Y. App. Div. 4th Dep't 2010).
665 No. 06-cv-01958-WYD-MJW, 2009 WL 1067018 at *4-5 (D. Colo. Apr. 21, 2009).
666 91 Cal. Rptr. 3d 858, 863 (Ct. App. 2009).
667 2012 WL 3939063 (C.D. Cal. Sept. 7, 2012)
668 2011 WL 2491371 (M.D. Pa. June 22, 2011).

the password to the court. Upon review, the court agreed to the relevance of a limited number of photographs and postings that reflected the fact that the plaintiff continued to ride motorcycles, went hunting and rode a mule, and therefore ordered production of this information. In a closing footnote, the court stated it was confused as to why intervention was necessary since the parties agreed that at least some of the information was relevant. The court further noted the plaintiff should have reviewed his own Facebook account for potentially responsive information, only soliciting the court's assistance if a dispute remained.

§ 9.13 Cloud Computing

The storage of ESI in the so-called "cloud" has created new legal and technical challenges. In order to define an e-discovery process around a cloud, you need to first understand the type of cloud that may be storing ESI.

> **Public cloud**: Public or external cloud is where resources are dynamically provisioned on a self-service basis over the Internet, via web applications/services, from an off-site third-party provider. Sometimes referred to as SAAS (software as a service).
>
> **Hybrid cloud**: A hybrid cloud consists of multiple internal and/or external providers, which is the typical choice of most enterprises. A hybrid cloud can consist of a local device, such as a plug-in appliance with cloud services.
>
> **Private cloud**: Private or internal cloud services emulate cloud computing on a private network. Private cloud delivers some benefits of cloud computing, capitalizing on data security, corporate governance, and reliability. Private cloud requires a company to buy, build, and manage the infrastructure, and as such do not benefit from the lower up-front capital costs and reduction in hands-on management of public cloud services.

The challenge in e-discovery is finding a way to collect and document information from the cloud in a legally defensible manner in this complex environment. Before probing the technical challenges of recovering electronically stored information (ESI) from online e-mail services, a company lawyer first should determine whether his or her client in fact has a legal obligation to preserve potentially relevant ESI stored in the cloud.

The general rule of law is that a company must produce all relevant or potentially relevant ESI in its possession, custody or control. When the company outsources its corporate email services and/or storage to an online email provider or a "cloud" computing application, courts likely will find that—while outside the company's possession or physical custody—employees' emails stored through the company's arrangements in an outsourced "cloud" nonetheless are within the company's legal control.[669] For this reason, many companies insist in their contracts with these services that there be

669 See, e.g. Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008).

specific and detailed provisions regarding security, location, management, preservation obligations, e-discovery collection protocols, and access to all the ESI. The preservation obligation is far less certain with respect to ESI created and stored on employees' personal e-mail or social media platforms such as Google, Facebook, Twitter or Yahoo. Companies generally cannot lawfully reach directly into an employee's personal online e-mail or social-network postings (although the situation may be different if the information is cached on a workplace computer, as described below).

It is likely that a court today would find that an employer does not have a legal obligation to preserve ESI stored in the cloud on these individually controlled platforms because the company has neither possession, custody, nor control. For this reason, some companies' acceptable-use policies ban or discourage employees from using any of these media for business communications.

The only exception may be an obligation to preserve any residual ESI that reasonably can be found somewhere in the possession, custody, or control of the company. Forensic examination and collection of ESI will focus on any data artifact remaining on the end user's computer in the web cache. Forensic solutions such as EnCase Forensic and EnCase Enterprise are able to capture not only the surviving cached image of ESI, but also its metadata, including when the data was created or last accessed.

The problem for forensic practitioners and companies facing e-discovery preservation obligations is that data is stored on servers owned and controlled by third parties. As such, they are not under the end user's control—a key requirement in traditional forensics, where the examiner has either physical control of the target hard drive, or can take control of the drive over the network by using EnCase Enterprise.

This lack of control of the physical hard drive makes the collection of electronically stored information (ESI) problematic with cloud-based evidence. The challenge for the examiner is how to collect and document information from the cloud in a legally defensible manner.

Companies that utilize cloud services for storage and e-mail specifically address these issues in their contract with the service. The contract between the cloud provider and the customer must be specific and detailed regarding security, location, management, preservation obligations, e-discovery collection protocols, and accessing the data.

The collection of ESI from the cloud presents not only technical challenges, but legal challenges as well. Currently, there is very little law on this subject.

Top legal considerations include:

1. Cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information.
2. A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the typical cloud provider.
3. For some types of information and some categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider.

4. The location of information in the cloud may have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information.
5. Information in the cloud may have more than one legal location at the same time, with differing legal consequences.
6. Laws could oblige a cloud provider to examine user records for evidence of criminal activity and other matters.
7. Legal uncertainties make it difficult to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users.
8. Responses to the privacy and confidentiality risks of cloud computing include better policies and practices by cloud providers, changes to laws, and more vigilance by users.

A typical legal problem that arises is that collecting cloud-based data stored in foreign countries may risk violating that country's privacy and criminal laws i.e. the European Union (EU) Data Protection Directive. Issuing a subpoena for the evidence has obvious hurdles as well.

If you are considering storing ESI in a cloud environment, you should consider these questions:

1. What kind of data will be in the cloud?
2. Where do the data subjects reside?
3. Where will the data be stored?
4. Where are the servers?
5. Will the data be transferred to other locations and, if so, when and where?
6. Can certain types of data be restricted to particular geographic areas?
7. What is the compliance plan for cross-border data transfers?

As interest in the cloud increases, these challenges will be addressed through new laws and data-access protocols.

§ 9.14 Discovery in United States Federal Agencies

The United States Federal Government, which issues the Federal Rules of Civil Procedure and is charged with enforcing the nation's laws, is arguably held to a higher standard when it becomes a litigant in civil matters. Some key recent decisions illustrate this point.

The *United Medical Supply Company v. United States* case scrutinizes the adequacy of the Federal Government's paper and e-discovery preservation and collection process.[670] The United States Court of Federal Claims imposed sanctions against the United States based upon its "reckless disregard of its duty to preserve relevant evidence."[671] In this case, the Justice Department attorney sent document hold notices via e-mail. However, due to faulty information and a lack of a concerted and systemic process to preserve and collect relevant information, much of the information was not preserved.

670 United Med. Supply Co. v. United States, 77 Fed. Cl. 257 (Fed. Cl. 2007).
671 Id. at 275.

The court noted that "It is the duty of the United States, no less than any other party before this court, to ensure, through its agents, that documents relevant to a case are preserved. Indeed. . . as the enforcer of the laws, the United States should take this duty more seriously than any other litigant . . . [T]he court concludes that it must impose spoliation sanctions against the United States."[672] The court, citing the then recently amended Federal Rule of Civil Procedure 37(f) "safe harbor provision", rejecting the government's argument that spoliation sanctions required a finding of bad faith. Instead, as per the "good faith" provisions of Rule 37(f), parties now have an affirmative duty of good faith to preserve evidence at the outset of litigation. The court explained: "[a]side perhaps from perjury, no act serves to threaten the integrity of the judicial process more than the spoliation of evidence … To guard against this, each party in litigation is solemnly bound to preserve potentially relevant evidence."[673]

The Federal Claims Court relied on the e-discovery amendments to the FRCP and existing e-discovery cases, including *Residential Funding Corp. v. DeGeorge Financial Corp.*,[674] to impose evidentiary and monetary sanctions.[675] *United Medical Supply Co., Inc.* illustrates that federal agencies must put a process in place to enable e-discovery preservation and collection capabilities. This capability is separate and independent of any records-retention processes, and, in fact, must be able to systematically override any such practices once a legal preservation obligation is triggered. This case, in conjunction with *Miller v. Holzmann* (see below), make it eminently clear that federal agencies will be held to at least an equal if not even higher standard on e-discovery compliance than private litigants.

Miller v. Holzmann is one of many post-December 1, 2006 cases that scrutinize the adequacy of an organization's e-discovery preservation and collection process. The case originated from a FOIA request, but quickly escalated to federal court.[676] The Court, noting approval for the proposition from the seminal e-discovery case *Zubulake v. UBS Warburg. Ltd*, quoted from The Sedona Principles, "[t]he obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data."[677]

The court went on to find that the government failed to comply with its duty to preserve, and that its failure was unreasonable:

> Lawyers employed by the Department of Justice, and particularly the competent and experienced ones assigned to this case, knew or should have known that a response to a FOIA request by an agency may lead to exactly what happened here, the retention and non-disclosure by the agency of information that may nevertheless be discoverable in a case then being litigated by that Department.[678]

672 Id. at 274.
673 Id. at 259.
674 306 F.3d 99, 108 (2d Cir. 2002).
675 Id. at 275.
676 Miller v. Holzman, No. 95-1231 (RCL/JMF), 2007 WL 172327, *1-2 (D.D.C. Jan. 17, 2007).
677 Id. at *6.
678 Id.

Miller v. Holzmann illustrates a growing trend where FOIA non-compliance will likely evolve into district court actions, with the FRCP e-discovery amendments utilized to enforce the original requests. Federal agencies can significantly mitigate this risk by establishing effective and repeatable e-discovery processes that comply with the rules of discovery and ensure the integrity of non-discoverable data by narrowing the search criteria.

In the criminal case of *United States v. Sedaghaty*, the defendant moved to suppress electronic evidence and prevent additional searching of nine computer hard drives seized and copied during the execution of a search warrant. Citing *United States v. Comprehensive Drug Testing*, the defendant argued that the government exceeded the warrant's scope by searching the computer hard drive. Acknowledging the importance of the cited case, the court noted that the warrant and seizure in this case predated the Comprehensive Drug decision, which was not intended to be applied retroactively. Finding the procedure utilized was consistent with pre-existing case law, the court determined appropriate search terms were used that were reasonably related to the items described in the warrant. The court also noted that the government exercised care in this case that exceeded what is required given the nature of white collar crimes and denied the defendant's motion to suppress.

§ 9.15 State Rules Update

The National Conference of Commissioners on Uniform State Laws met in August, 2007 to formulate uniform state electronic discovery rules. Following a week of dialogue and debate, the group proposed the Uniform Rules Relating to the Discovery of Electronically Stored Information.[679] The Model State Rules are comparable to the FRCP, and change only what is necessary to accommodate various state procedures.

The Federal rules do not define the term "Electronically Stored Information" ("ESI"), but the proposed uniform state rules do provide a definition. "Electronically stored information" refers to that information that is stored in an electronic medium and is retrievable in perceivable form. The commissioners also define "electronic" in Rule 1(2) to mean: "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities."

There are several differences between the FRCP and the Uniform Rules. One significant difference is their respective treatment of the protection of "not reasonably accessible" ESI. Federal Rule 26(b)(2)(B) protects such information from production unless the requesting party makes a good-cause showing. The Federal Rule does not spell out the considerations for such good cause; but only refers to the limitations of Rule 26(b)(2)(C). One must look to the Rule Commentaries to find a non-exhaustive list of seven considerations:

> (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be

679 The rules are available at: http://www.law.upenn.edu/bll/archives/ulc/udoera/2007_final.htm

> obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

The proposed Uniform Rules also protect "not reasonably accessible" ESI in Rule 8(a), however, this protection is limited by a different good-cause showing. This good- cause showing is determined by an exhaustive list of four considerations. Rule 8(c) reads:

> The court may order discovery of electronically stored information that is from a source that is not reasonably accessible because of undue burden or expense if the party requesting discovery shows that the likely benefit of the proposed discovery outweighs the likely burden or expense, taking into account (1) the amount in controversy, (2) the resources of the parties, (3) the importance of the issues, and (4) the importance of the requested discovery in resolving the issues.

One final significant difference can be found in state Rule 8(e), which describes a "proportionality" restraint on the production of all ESI, even readily accessible live data:

> (e) The court shall limit the frequency or extent of discovery of electronically stored information, even from a source that is reasonably accessible, if the court determines that: (1) it is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive; (2) the discovery sought is unreasonably cumulative or duplicative; (3) the party seeking discovery has had ample opportunity by discovery in the proceeding to obtain the information sought; or (4) the likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues, and the importance of the requested discovery in resolving the issues.

Companies are using the FRCP as the model approach and, as needed, are adjusting their response plans to comply with state laws.

State Law Summary

The following is a summary of the 50 states (and the District of Columbia) and the extent to which they have amended their state laws to reflect ESI rule changes made in the FRCP:

States adopting FRCP-like ESI rules (25):

> Alabama, Alaska, Arizona, Arkansas, California, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Montana, Nebraska, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Tennessee, Utah, Vermont, Virginia, Wyoming

States adopting approaches similar to the Texas model[680] (3):

Texas, Idaho, Mississippi

States with limited ESI amendments (6):

Connecticut, Louisiana, New Hampshire (incorporated only mandatory discussion at meet-and-confer), Nebraska, New York, North Carolina (only business courts require discussion of e-discovery issues)

States considering ESI amendments (13):

Connecticut, Delaware, D.C., Illinois, Kentucky, Massachusetts, Missouri, New Hampshire, New York, North Carolina, South Carolina, Washington (incorporated a rule similar to FRE 502 on September 1, 2010)

States not modifying rules for ESI (11):

Colorado, Florida, Georgia, Hawaii, Nevada, Oregon, Pennsylvania, Rhode Island, South Dakota, West Virginia, Wisconsin

Notable State Cases

In *Barrow v. Miner,*[681] the Ohio Sixth District Court of Appeals (Lucas County) ruled that the trial court's dismissal of plaintiff's claims was not an abuse of discretion where plaintiff failed to preserve evidence and purposefully acted to destroy evidence by utilizing scrubbing software.

The Washington State Supreme Court held that metadata is a public record that must be disclosed under the State of Washington's Public Records Act (PRA) in *O'Neill v. City of Shoreline.*[682]

In *Romano v. Steelcase Inc.,*[683] a personal injury action, the Supreme Court, Suffolk County, New York held that the private information the defendant was seeking from plaintiff's social networking website accounts was material and necessary for defendant's defense; the plaintiff did not have a reasonable expectation of privacy in information published on social networking websites; and the defendant's need for access to plaintiff's private information on social networking websites outweighed any privacy concerns voiced by plaintiff.

The Appellate Court of Illinois, First District, Fifth Division, affirmed the decision of the trial

680 See Tex. R. Civ. P. 196.4 Electronic or Magnetic Data (http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi03.pdf/$file/ElecDi03.pdf); Idaho R. Civ. P. 33 (http://www.isc.idaho.gov/rules/ircp33.rul) and Idaho R. Civ. P. 33 (http://www.isc.idaho.gov/rules/ircp34.rul); Miss. R. Civ. P. 26(b)(5) (http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi11.pdf/$file/ElecDi11.pdf).

681 2010 WL 4016815 (Ohio Ct. App., Lucas County Oct. 15, 2010).

682 2010 WL 3911347 (Wash. Oct. 7, 2010).

683 2010 WL 3703242 (N.Y. Sup. Ct. Sept. 21, 2010).

court of Cook County, dismissing the plaintiff's complaint with prejudice as a sanction for spoliation, which involved the deletion of electronic files from the plaintiff's computer with sophisticated data-wiping programs just prior to meeting a court-ordered deadline for producing the computer for examination in *Peal v. Lee.*[684]

In *TR Investors v. Genger,*[685] the Court of Chancery of Delaware found that the defendant committed spoliation of evidence when he and his computer consultant destroyed all the information on the unallocated space of corporation's computer database. The defendant used "wiping" software to clean the computer system of information and attempted to keep his activities a secret, despite a court order that enjoined the destruction of any company-related documents. The sanctions included the production of documents previously protected as privileged, the raised burden of proof for the defendant on any defense or counterclaim, and payment of $75,000 in attorneys' fees and expenses.

An $8 million default judgment was reinstated by the Washington State Supreme Court against the defendant automobile manufacturer for the "willful efforts to frustrate and undermine truthful pretrial discovery" in failing to produce in a timely manner database records from a consumer hotline concerning car seats in *Magana v. Hyundai Motor America*[686].

ADD Beard Research, Inc. v. Kates[687]*("Kates II")* concerns an ex-employee, who deleted relevant data, replaced and then lost the hard drive of his laptop, and defragmented his laptop on the eve of its production. He and his new employers, who failed to take sufficient action to prevent destruction of the laptop, were held jointly responsible for the spoliation of possible evidence and were ordered to pay $76,906.80 in plaintiff's attorney and expert fees and expenses in seeking sanctions.

In the absence of a demonstration of the particular characteristics of the electronic storage devices involved, the familiarity of its experts with those characteristics, and a reasonable likelihood that the proposed search methodology would yield the information sought, the Supreme Court of Texas held that the plaintiff was not entitled to production of computer hard drives, granted the defendant's writ of mandamus, and ordered the trial court to vacate its order in *In re Weekley Homes, L.P.*[688]

In *ADD Ex parte Cooper Tire & Rubber Co.*[689], the Supreme Court of Alabama concluded that Fed. R. Civ. P. 26(b)(2)(B) and the factors applied in *Wiginton v. CB Richard Ellis, Inc.*[690] should be used in considering the extent to which parties in Alabama state court actions must respond to discovery requests for electronically stored information. This was in light of evidence presented by the defendant that the burden of producing responsive e-mails would entail thousands of hours and hundreds of thousands of dollars.

684 2010 WL 3001338 (Ill. App. Ct. 1st Dist. July 30, 2010).
685 2009 WL 4696062 (Del. Ch. Dec. 9, 2009).
686 220 P.3d 191 (Wash. 2009).
687 981 A.2d 1175 (Del. Ch. 2009).
688 295 S.W.3d 309 (Tex. 2009).
689 987 So.2d 1090 (Ala. 2007).
690 229 F.R.D. 568 (N.D. Ill. 2004).

10. Employee Data Privacy (US)

§ 10.0 Overview

Email is firmly established as the primary form of workplace communication. In recent years, employment litigation and other cases involving alleged workplace misconduct have routinely involved evidence in the form of e-mail or other computer-generated records created in the course of business. With most of a typical company's "documents" and other information existing in electronic form, employer monitoring--and in many cases, seizure of these files--has become commonplace.

In considering employee privacy in the context of monitoring e-mail and other computer files, it is important to note that the rights of government employees may differ in many aspects from their counterparts in the private sector. For instance, the United States Constitution's Fourth Amendment restrictions on unreasonable searches and seizures afford potential additional protections for government employees who are subject to monitoring of their e-mail, text messages, and computer files.

As the Fourth Amendment only acts as a check on government actions,[691] the scope of the Amendment's protections is more limited when applied to non-government workers. Conversely, employer manuals and other written information setting forth company policy largely govern privacy rights in the commercial workplace. As such, workplace privacy issues in the private and public sector are addressed separately in this section.

§ 10.1 Preliminary Considerations for Employers

The issue of employee monitoring is complex, and employers should seek the advice of their counsel when considering the implementation of a written policy governing these issues. The following are some preliminary considerations:

> Employers should monitor all developments in this rapidly developing area of law. In addition to the Connecticut and Delaware statutes,[692] the California legislature passed a law that would have mandated an employee's written consent, among other requirements, before employers could monitor their employees' e-mail, Internet usage and stored computer files.[693] Only the somewhat unexpected veto of Governor Gray

691 See, e.g., Flagg Bros., Inc. v. Brooks, 436 U.S. 149, 156 (1978) (stating that most constitutional rights "are protected only against infringement by governments"); Jackson v. Metropolitan Edison Co., 419 U.S. 345, 349 (1974) (describing "essential dichotomy" between deprivations of rights by state action and private conduct).

692 See § 9.01.

693 Cal. SB1016, sponsored by Debra Bowen, D-Redondo Beach.

Davis blocked the enactment of the statute. Similar bills are being considered in other states and in the US Congress.

Employers should ensure that all employees are informed and that consent is given in writing to any of the monitoring activities described earlier. Proper written consent provides an exception to almost all existing laws governing employer monitoring in the United States.

Employers and their counsel should be mindful of cases that hold employers liable for the wrongful conduct committed by an employee through the Internet and/or their own network. This adds to the equation of the employer's interests of not only protecting their intellectual property and internal resources, but also being charged with a duty to prevent wrongful online conduct of their employees.

Employers should be consistent and even-handed in their monitoring activities in order to avoid common law invasion of privacy claims. An employee could in theory state a claim for improper monitoring if an ordinary reasonable person would find that the circumstances involved "a substantial and highly offensive invasion of privacy."[694] For instance, a targeted, non-routine search for incriminating electronic documents to provide a pretext for the termination of an employee may be construed as unreasonable by some courts.

§ 10.2 The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 (ECPA) is a federal statute that some contend has application to an employer's workplace e-mail monitoring activities. The ECPA includes two categories relevant to this discussion: Title I prohibits interception of messages in transit,[695] while Title II, the Stored Communications Act, prohibits access to and disclosure of stored information. The "stored information" provision under Title II has been narrowly construed to only apply to information in intermediate storage incident to transmission, such as an e-mail residing on a server prior to being retrieved by the recipient.

Thus, the ECPA prohibits three types of intrusions into electronic communications: intercepting messages while they are in transit, accessing information in intermediate storage incident to transmission, and disclosing information at any point in the process.[696] While the ECPA may seem to give employees broad protection from e-mail monitoring, the Act contains several exceptions that sharply limit its scope.

First, it is apparent that Congress did not intend the ECPA to govern the relations of employees to

694 Smyth v. Pillsbury Co., 914 F. Supp. 97, 100 (E.D. Pa. 1996) (recognizing the theoretical possibility of such a claim).
695 See 18 U.S.C. §§ 2511, 2521, 3117, 3121-3127 (1994).
696 Yochai Benkler, "Rules of the Road for the Information Superhighway" § 1, § 20.3[1] (West 1996) (discussing effects of ECPA's passage).

their employers, but rather intended to regulate intrusions by unauthorized outsiders into the electronic communications of organizations. As such, most commentators believe that the ECPA does not cover workplace local area networks (LANs) and thus provides no protection for employees when they send e-mail over their workplace computer networks.[697] The language in the ECPA prohibiting disclosure of electronic communications only applies to those entities that provide electronic communication services "to the public,"[698] while intra-office networks offer services only to employees. Thus, under this construction of the ECPA, any e-mail sent by employees over a nonpublic network would not be subject to the Act.

Second, even if the ECPA did apply to proprietary LANs, the Act contains an exemption allowing access to stored communications when authorized by the entity providing electronic communications services.[699] On its face, this provision allows the network provider to access any stored communication that had been sent over the network without violating the ECPA. If an employer owns the network, it could then access all communications sent by employees.

In *Bohach v. City of Reno,*[700] the plaintiffs--two police officers--sought an injunction preventing the City from continuing an internal affairs investigation. In rejecting the plaintiffs' claim that the investigators violated the EPCA by retrieving the plaintiffs' pager messages stored on the City's telephone network, the court noted that the City was the provider of the electronic communications service used by the officers.[701] It then held that "[section] 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage. Because the City is the provider of the 'service,' neither it nor its employees can be liable under § 2701."[702]

Employers should be aware that actually intercepting e-mail messages in transit, as opposed to accessing stored communications, would likely constitute a violation of the ECPA.[703] Interception is generally defined as the act of accessing a message or preventing it from reaching its destination at any point between the time the message is sent and the time the intended recipient receives it. To date, most courts have taken a narrower view of what constitutes "interception" of e-mail, establishing that under the ECPA, interception can only occur during the fraction of a second the message is actually traveling along the wires connecting computers.[704]

---

697 See, e.g., Michael D. Scott et al., Scott on Multimedia Law § 12.04 [[A] (2d ed. Supp. 1997) (asserting that ECPA "would not apply to corporate or other 'non-public' computer networks . . . . [A] company's review of e-mail transmitted through or stored on its computer system would not violate the ECPA"); Kent D. Stuckey et al., Internet and Online Law § 5.03[1] (Release 2 1998) (stating that ECPA "does not . . . protect against employers monitoring the e-mail of their employees").

698 18 U.S.C. §§ 2511(3)(a), 2702(a)(1) (1994).

699 See 18 U.S.C. § 2701(c)(1) (1994) (exempting all "conduct authorized . . . by the person or entity providing a wire or electronic communications service"). The provider of electronic communications services is known as the "network provider."

700 Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).

701 See Id. at 1232. The officers had used the police department's alphanumeric paging system to send messages to each other. See Id. at 1233. The contents of these messages led to an internal affairs investigation of the officers.

702 See Id. at 1236.

703 Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 463 (5th Cir. 1994).

704 Id. at 463 (holding that seizure of e-mail sent to bulletin board but not yet read by intended recipients did not constitute unlawful interception). See also United States v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996).

Fraser v. Nationwide Mutual Insurance Co.[705] is the latest case to hold that an employer's retrieval of an employee's e-mail from post-transmission storage does not constitute an "interception" under the ECPA. In *Eagle Investment Systems Corporation v. Tamm*,[706] the court similarly determined that no "interception" occurred when an employee obtained a stored e-mail from a coworker without his consent.

In *Steve Jackson Games, Inc. v. United States Secret Service*, the Fifth Circuit addressed the issue of whether the seizure of a computer storing private e-mail that had been sent to an electronic bulletin board but not yet read by the recipients constituted an "intercept" proscribed by Title I of the ECPA. The court determined that such a seizure was not an interception because the e-mail was not being transferred, but was instead in storage incidental to transmission.[707]

Other courts have reached similar conclusions regarding the definition of interception as used in the ECPA.[708] However, at least one court has since determined that the viewing of information from a secure web page in intermediate storage prior to being read by its intended recipient constitutes an "interception."[709] These rulings indicate that e-mail could almost always be seized before it reached its intended recipient without being "intercepted," and thus triggering the tough restrictions of Title I of the ECPA.

§ 10.3 Employee Monitoring in the Private Sector

While an employer is generally prohibited by law from intercepting e-mail messages transmitted over the Internet,[710] monitoring employee e-mail and stored computer files, including Internet history files, is generally permitted in most states without written consent or notification. Connecticut and Delaware each require employers to obtain written consent from their employees or provide written notice to their employees before any such monitoring can take place.[711] A bill for a similar statute, dubbed the "Notice of Electronic Monitoring Act" (S.2898), was introduced in Congress in July 2000,

705 Fraser v. Nationwide Mutual Insurance Co., 135 F. Supp. 2d 623 (D. Penn. 2001).

706 Eagle Investment Systems Corp. v. Tamm, 2001 WL 576133 (D. Mass. May 22, 2001).

707 Steve Jackson Games, 36 F.3d at 463.

708 See United States v. Councilman, 245 F. Supp.2d 319 (D. Mass. 2003); Bohach v. City of Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) ("The statutes therefore distinguish the 'interception' of an electronic communication at the time of transmission from the retrieval of such a communication after it has been put into 'electronic storage.'"); United States v. Reyes, 922 F. Supp. at 836 ("[T]he definitions [in the ECPA] thus imply a requirement that the acquisition of the data be simultaneous with the original transmission of the data.").

709 Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035 (9th Cir. 2001); opinion withdrawn, 262 F.3d 97 and superseded by 302 F.3d 868 (9th Cir. 2002). Konop initially created some concerns about a broader definition of "interception." However, and in response to these concerns, the opinion has been withdrawn and superseded.

710 See 18 U.S.C. §§ 2511, 2521, 3117, 3121-3127 (1994).

711 Connecticut Public Act no. 98-142. http://www.cga.ct.gov/ps98/Act/pa/1998PA-00142-R00HB-05398-PA.htm There are exceptions under this statute where the employer has reasonable grounds to suspect that the employee is engaging in unlawful conduct or conduct creating a hostile workplace environment, and such monitoring may produce evidence of this misconduct. 19 Del. C. § 705. The only explicit exceptions under the Delaware law are for "processes that are designed to manage the type or volume of incoming or outgoing electronic mail or telephone voice mail or Internet usage, that are not targeted to monitor or intercept the electronic mail or telephone voice mail or Internet usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and/or protection."

but never made it out of committee. Counsel should remain vigilant in monitoring any developments in the law at both the state and federal levels.

In considering the propriety of employer monitoring of employee e-mail and computer files, the primary question is whether and to what extent written agreements and policies addressing such monitoring are in place. Policy about written notification that e-mail and computer files are subject to access by the employer generally governs whether an employee can claim a reasonable expectation of privacy in those files. These rules, in the form of e-mail, Internet use, and stored computer file policies, must limit employees' privacy expectations in their electronic communications and stored computer files, but must do so consistently with laws that prohibit interceptions of electronic communications in transit. Moreover, it is important that these rules and policies are expressly acknowledged and consented to in writing by the employee.

Balancing of Interests

In determining an employee's privacy interests, the courts will balance the employer's interest against the reasonable privacy rights of the employee. Preventing theft of intellectual property and policing unauthorized activity are generally seen as compelling interests justifying an employer's reasonable monitoring activities.[712] Additionally, employers may potentially be held liable for an employee's online misconduct where the company's computer networks are the means for the offense.[713] Some legal experts have hypothesized that when an employee utilizes an employer's computer systems to engage in such activities as hacking, online harassment, or copyright infringement, an employer may be liable for those activities.[714] In *Blakey v. Continental Airlines,*[715] the New Jersey Supreme Court found that Continental Airlines could be potentially liable for an employee's harassing postings on an Internet bulletin board hosted by the airline for its employees.

In reversing a lower court's order dismissing Blakey's complaint, the Court reasoned that since the company provided the Internet forum for employees' use, Continental had a duty to monitor e-mail postings to ensure that employees were not harassing one another. In another leading decision in this area, *Smyth v. Pillsbury Co.*, the US District Court for the Eastern District of Pennsylvania determined that "a company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[716] Thus, with the employers' interest in preventing theft and unauthorized activity coupled with the possibility of third-party liability for *failing* to monitor the employees' online conduct usage, the monitoring of e-mail and Internet usage by employees is a critical, if not mandatory, necessity for employers in the private sector.

Still, employers are wise to ensure that proper written notifications are in place. The case of *Muick*

712 Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).
713 See, e.g., Jeffrey S. Nowak, Employer Liability for Employee Online Criminal Acts, 51 Fed. Comm. L.J. 467 (1999).
714 Id.
715 Blakey v. Continental Airlines, 751 A.2d 538 (2000).
716 Smyth v. Pillsbury Co., 914 F. Supp. at 100.

v. Glenayre Electronics[717] upheld the propriety of an employer's search of its employee's hard drive, but predicated the reasonableness on the existence of written notifications and existing company computer use polices. The Court's rationale in *Muick* is consistent with an emerging trend requiring these policies. Notably, the decision implies a different result had such written notifications not been in place.

When employees do have an expectation of privacy, however, as with attorney-client communications, even this may be diminished by virtue of clear employer policies. In *Stengart v. Loving Care Agency, Inc.*,[718] a former employee sued her employer for violating New Jersey's Law Against Discrimination. In response, the employer searched the former employee's company-owned laptop computer and found, in the web browser's history, e-mails she had exchanged with her attorney using her own private, password protected e-mail account.[719] The employer contended that the employee had waived her privilege by using the company's computer to send e-mails to her attorney. The company's electronic communications policy stated that "[o]ccasional personal use is permitted" and described several prohibited uses including soliciting for outside business ventures, charitable organizations, or sending inappropriate sexual, discriminatory, or harassing messages.[720]

The New Jersey Supreme Court concluded that "[A]s written, the Policy creates ambiguity about whether personal e-mail use is company or private property," and for important public policy concerns underlying the attorney-client privilege, held the former employee had an expectation of privacy in her e-mail exchanges with her lawyer.[721] However, the court went on to say that companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies.[722]

In *United States v. Bailey*,[723] a federal district court in Nebraska held that the defendant, who signed on to his work computer through a "splash" screen that included a consent to search, "had no expectation of privacy in the work computer owned by someone else, because every time he accessed the work computer he physically acknowledged that he was giving consent to search the computer. Such repeated warnings about consent to search, followed by such repeated acknowledgments, categorically and without more defeat [defendant]'s claim of privacy."[724] Thus, under the *Bailey* court's reasoning, an employer that requires its employees to sign on through "consent to search" screens or warnings is on solid grounds when conducting searches of an employee's hard drive.

However, employers should be mindful not to exceed the scope of their written policies or intrude "offensively" on their employees' reasonable expectations of privacy. In *Hernandez v. Hillsides, Inc.*,[725] a private employer who was concerned that one of its computers was being used after regular

717 Muick v. Glenayre Electronics, 280 F.3d 741 (2002).
718 Stengart v. Loving Care Agency, Inc., 201 N.J. 300 (2010).
719 Id. at 309.
720 Id. at 311.
721 Id. at 315, 321.
722 Id. at 324.
723 United States v. Bailey, 272 F. Supp.2d 822 (D. Neb. 2003).
724 Id. at 824.
725 Hernandez v. Hillsides, Inc., 47 Cal. 4th 272 (Cal. 2009).

working hours to view pornographic sites contrary to its written workplace policy, installed electronic equipment that gave it the capacity to secretly watch and record employee activities behind closed doors in a semi-private office. The California Supreme Court held that "[t]he workplace policy, that by means within the computer system itself, [employees] would be monitored about the pattern and use of Web sites visited, . . . is distinguishable from and does not necessarily create a social norm that in order to advance the same interest, a camera would be placed inside [the] office, and would be aimed toward a computer workstation . . ."[726]

However, the court outlined that "an employer may have sound reasons for monitoring the workplace, and an intrusion upon the employee's reasonable privacy expectations may not be egregious or actionable under the particular circumstances."[727] Noting that "offensiveness" was an indispensable part of the privacy analysis, and that employees in the office "were not at risk of being monitored or recorded during regular work hours and were never caught on camera or videotape," the court did not find "highly offensive" circumstances in this case.[728] While employees may not have had a reasonable expectation of being recorded, the activation of the surveillance system was narrowly tailored in place, time, and scope, and was prompted by legitimate business concerns.[729]

The bottom line is that there is no "bright line" rule as to when an employee has an expectation of privacy or when an employer's conduct may violate employee privacy. Employers grappling with monitoring of employee electronic usage are best advised to have clear policies on which employees sign off, making clear that employees do not have an expectation of privacy in their usage of employer-provided equipment, and that the employer can and will monitor such usage.

§ 10.4 Monitoring of Government Employees

Federal, state, and municipal employers constitute a very large sector of the US economy, and they have aggressively digitized their workplaces. E-mail and texting capabilities are now common at all levels of government, and e-mail continues to be promoted as the preferred method of conducting government business. In addition, the federal government has instituted an aggressive telecommuting program, which generates extensive electronic records.[730] Included within these aggressive plans for digitizing government workplaces are equally aggressive monitoring programs.[731] Unlike their private sector counterparts, federal employees are afforded a degree of protection under the Fourth Amendment's prohibition against unreasonable search and seizures.[732] However, those protections

726 Id. at 294.
727 Id. at 290.
728 Id. at 295, 301.
729 Id. at 301.
730 See, e.g., Mike Causey, Telecommuting Today, Wash. Post, July 8, 1997, at B2.
731 See, e.g., H.G. Reza, The Few, the Proud, the Online, L.A. Times (Orange County ed.), Dec. 25, 1997, at E1, available in LEXIS, News Library, LAT File.
732 O'Connor v. Ortega, 480 U.S. 709, 715, 107 S. Ct. 1492, 1496 (1987) (a plurality decision); Shields v. Burge, 874 F.2d 1201, 1203-04 (7th Cir. 1989).

can also be substantially limited by the implementation of written policies and agreements that reduce employees' reasonable expectations of privacy.[733]

United States v. Simons[734] is a notable case that directly addresses issues of monitoring and seizure of a federal employee's computer files in the workplace. In *Simons,* systems administrators of the Foreign Bureau of Information Service (FBIS) division of the CIA searched an employee's hard drive over a remote network connection after routine network monitoring detected unauthorized Internet connections from his computer to sex-related websites. The FBIS previously instituted a written policy regarding Internet usage by employees stating that employees were to use the Internet for official government business only. The policy specifically prohibited accessing unlawful material and stated that "[u]sers shall . . . [u]nderstand FBIS will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate."

The record reflects three distinct levels at which FBIS, and then the CIA Office of the Inspector General (OIG), searched and ultimately seized Simons' computer files. First, FBIS investigators performed text searches across the network, resulting in numerous sex-related keyword "hits" originating from Simons' computer. The FBIS network administrator then remotely accessed and copied files from Simons' computer to determine the existence of unauthorized downloaded Internet files. After determining that some downloaded images appeared to be child pornography, investigators from the CIA OIG directed Simons' hard drive be seized from his office without a warrant, despite their knowledge that Simons' computer likely contained images of child pornography.

Simons contended on appeal from his conviction that the FBIS's search of his computer files stored on his hard drive in his office over the network violated the Fourth Amendment. Simons further contended that the OIG's warrantless seizure of his hard drive also violated the Fourth Amendment. The court found the remote network searches of Simons' computer to be proper because, in light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet. Notably, the appellate court declined to recognize any privacy distinction between the network-wide keyword text searches (which Simons did not contest) and the subsequent remote search and seizure of files contained on Simon's hard drive (which Simons objected to).[735]

However, the court found that Simons did have a reasonable expectation of privacy in his office, so the warrantless entry and seizure of his computer potentially violated the Fourth Amendment absent the applicability of a specific exception to the warrant requirement.[736] While the FBI's written policies addressed Internet usage and network monitoring, the court found that the policies did not sufficiently address privacy expectations regarding computer files stored on the hard drives and other media actually contained within the employee's office.[737] However, citing the US Supreme Court decision of *O'Connor v Ortega, supra,* the court held that a government employer's interest in "the efficient and proper operation of the workplace" justified the warrantless work-related search

733 O'Connor, 480 U.S. at 717, 107 S. Ct. at 1497; 480 U.S. at 737, (Blackmun, J., dissenting).

734 United States v. Simons, 206 F.3d 392 (4th Cir 2000).

735 Id. at 398, n. 9.

736 Id. at 399-400.

737 Id. at 399 n 10.

of Simons' computer, especially since the *O'Connor* Court held that when a government employer conducts a search pursuant to an investigation of work-related misconduct, the Fourth Amendment will be satisfied if the search is reasonable in its inception and its scope.

A search normally will be reasonable at its inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct."[738] Such searches will be considered permissible in its scope "when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]."[739]

Obviously, the best practice for an investigator in this situation would be to obtain a warrant, if feasible, prior to physically seizing a government employee's computer, as courts outside of the Fourth Circuit may not reach many of the conclusions of the *Simons* Court. Further, this case illustrates the importance of comprehensive written policies that not only address e-mail and network activity monitoring, but also the access of stored files on the employee's computer.

Clear policies shape the reasonable expectations of employees, even when warrants are not necessary. In *O'Connor v. Ortega*, *supra*, the US Supreme Court held that the "special needs" of the workplace justified an exception to the rule that warrantless searches are *per se* unreasonable under the Fourth Amendment.[740] The case of *Quon v. City of Ontario*[741] illustrates how text messages may give rise to such "special needs."

Quon, a police officer for the City of Ontario (City), brought suit against the City and its police department for violating the Fourth Amendment and the Stored Communications Act (SCA) by obtaining and reviewing a transcript of messages from his two-way, work-issued pager. Quon also brought suit against the City's wireless provider for violating the SCA by giving the City the transcript.[742] Quon had exceeded his monthly character limit for several months, so the police chief demanded and received transcripts of his text messages from the wireless provider, whereupon it was discovered that many of Quon's messages were not work related, and some were sexually explicit.[743] The investigating officer used Quon's work schedule to redact from his transcript any messages he sent while off duty, but the transcript showed that few of his on-duty messages related to police business.[744]

The Ninth Circuit Court of Appeals reversed a District Court ruling, and concluded that the search was not reasonable because even though it had been conducted on a legitimate, work-related rationale, it could have been conducted less intrusively. The Court of Appeals further concluded that the wireless provider had violated the SCA.[745] The City's subsequent petition for certiorari was granted.

The US Supreme Court preferred to dispose of the case on narrow grounds than to issue a broad holding concerning employees' privacy vis-à-vis employer-provided technology equipment. The Court

738 O'Connor, 480 U.S. at 726, 107 S. Ct. at 1502.
739 Id. (citing New Jersey v. T.L.O., 469 U.S. 325, 342, 105 S. Ct. 733 (1985)).
740 O'Connor, 480 U.S. at 725.
741 City of Ontario v. Quon, 130 S. Ct. 2619 (2010).
742 Id. at 2626.
743 Id. at 2625-26.
744 Id. at 2626.
745 Id. at 2627.

did not consider the merits of the SCA claim, but nevertheless dismissed Quon's argument that the warrantless search was *per se* unreasonable in light of the Ninth Circuit's conclusion that the wireless provider violated the SCA.[746] Instead, because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the Court found it reasonable under the government employer's standard set forth above under *O'Connor*.[747]

In dictum, the Court explained the difficulty in predicting how employees' privacy expectations would be shaped by evolving workplace norms, and the degree to which society would recognize those expectations as reasonable:

> Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.[748]

§ 10.5 Monitoring the Military

Although members of the military are government employees, their expectations of privacy may be less than civilian employees. In *US v. Plush*[749], the US Air Force Court of Criminal Appeals held that a military officer does not have a reasonable expectation of privacy in his work computer. Plush had brought his government-issued laptop computer into a government repair facility for repair of a cracked screen. While performing routine maintenance on the computer, the staff sergeant in charge of computer maintenance noticed unusually large files in the recycle bin and temporary Internet files, including more than 1,200 graphics files, three of which contained sexually explicit photographs.

This was the basis for an authorization for a subsequent forensic analysis of the laptop and two desktop computers that were located in Plush's office. The forensic analysis revealed that the three computers contained nearly 4,500 sexually explicit images. In denying an appeal of a conviction of conduct unbecoming of an officer, the Court stated that "the nature of military life provides members with a minimal expectation of privacy in government property, due to government ownership, the non-personal nature of military offices, and the inherent right of command to inspect property under its control."[750]

The Court also noted that "Air Force policy requires the monitoring of telecommunications systems, including computers; Air Force policy provides that use of such equipment constitutes

746 Id. at 2632.
747 Id. at 2632-33.
748 Id. at 2630.
749 United States v. Plush, 2004 WL 2191813 (A.F. Ct. Crim. App. Sep. 21, 2004).
750 Id. at 3 (internal citations and quotations omitted).

consent to monitoring; and Air Force policy further requires a notice and consent log-on banner to be installed on all computers."[751] As a result, the Court held that "the appellant could not reasonably have expected a right to privacy as to his laptop computer."[752]

In *United States v. Long*,[753] a case consistent with *Plush,* the United States Navy-Marine Corps Court of Criminal Appeals held that a computer network system administrator could properly turn over information about criminal activity only if such information was found during normal system maintenance. The administrator had testified that "there was no ongoing monitoring of the network at the time and that he specifically acted at the behest of law enforcement officials in retrieving the e-mails." [754] The Court opined:

> So long as [the computer network system administrator] conducts his activities through ongoing system monitoring or confines his searches to those necessitated to ensure that the system is operating properly and that no user is abusing the system or using the system in an unauthorized manner, the system administrator can also properly turn over any evidence of criminal conduct to the authorities. Once he becomes the agent of law enforcement, however, either through conducting a search for criminal activity at their request or by permitting them to participate actively in his monitoring and administering function, he loses that special status afforded him under the law and becomes equally subject to the requirements of the 4th Amendment regarding probable cause and proper search authorization.
>
> We conclude that it is reasonable, under the circumstances presented in this case, for an authorized user of the Government computer network to have a limited expectation of privacy in their e-mail communications sent and received via the Government network server. Specifically, while the e-mails may have been monitored for purposes of maintaining and protecting the system from malfunction or abuse, they were subject to seizure by law enforcement personnel only by disclosure as a result of monitoring or when a search was conducted in accordance with the principles enunciated in the 4th Amendment.
>
> We conclude that the appellant had a subjective expectation of privacy in the e-mails sent and received on her Government computer vis-à-vis law enforcement and that this expectation of privacy was reasonable. The military judge therefore erred in denying the defense motion to suppress the e-mails at trial. [755]

The increase in e-mail use as the primary method of intra-office communication has given rise to issues concerning both employers' rights to monitor those communications and employees' privacy

751 Id.
752 Id. at 4.
753 United States v. Long, 61 M.J. 539 (N.M. Ct. Crim. App. 2005).
754 Id. at 543.
755 Id. at 546.

rights under the Fourth Amendment. While the Fourth Amendment does not apply to private employers, private employers must comply with certain state regulations that require notice and employees' consent. [756]

On the other hand, while the government is bound by the Fourth Amendment when it comes to employees' privacy rights, recent holdings have established that government monitoring and searching of its own employees' hard-drives are within the Fourth Amendment as long as they are conducted to identify and prevent malfunctions and illegal activity. [757]

756 Smyth v. Pillsbury Co., 914 F. Supp. 97, 100 (E.D. Pa. 1996); Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 463 (5th Cir. 1994).

757 United States v. Long, 61 M.J. 539 (N.M. Ct. Crim. App. 2005); United States v. Plush, 2004 WL 2191813 (A.F. Ct. Crim. App. Sep. 21, 2004).

11. International E-Discovery

§ 11.0 Overview

§ 11.1 E-Discovery Outside the US and Cross-Border Litigation

Introduction

Companies operating in the global economy routinely generate, move, and store data around the world. For example, when litigation arises in the UK or US that implicates data residing in Europe, basic actions required to satisfy British and American disclosure or discovery obligations may put the company in violation of European laws that recognize and protect individual privacy rights in employee workplace data.

With no established protocol available for handling international disclosure/discovery (hereinafter "discovery") responses, little published decisional law and scattered official guidance, corporations and their counsel have struggled for years to balance competing legal obligations under US and European law.

These issues have taken center stage in recent years with the publication of significant guidelines and recommendations by authorities in the EU regarding the proper handling of EU data in the US discovery process. Nonetheless, organizations often are in search of best practices in light of still-emerging protocols.

This section will provide overviews of electronic discovery issues for Europe generally (primarily data protection issues), the United Kingdom, Canada and Australia. It concludes with summaries of US court decisions relating to cross-border discovery.

European Data Protection – An Overview

European member states have widely varying court rules pertaining to disclosure of electronically stored information (ESI). The common-law jurisdictions of the United Kingdom and Ireland provide for disclosure of ESI, while the majority of European courts, with civil law systems, oversee relatively little electronic disclosure.

Pervasive data privacy rights, however, apply throughout Europe and frequently complicate litigants' efforts to search, preserve, collect, process, review, and produce relevant ESI collected from European employees and citizens. These data privacy rights originally were recognized under the Directive 95/46/EC of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (the "EU Directive") and subsequent EU member state enabling legislation.

The EU Directive does not itself have the force of law; rather, it provides the overarching framework for the data-protection laws required to be enacted by each of the EU member states. National data-protection legislation may differ from and expand significantly upon the EU Directive.

In addition, other national laws and regulations may have a direct bearing on the handling of data sought in US discovery. Because of the number of possible sources of rules affecting disclosure in the UK and US of data residing in Europe, we recommend that local counsel be consulted in any such circumstances.

For a fuller treatment of these issues, we recommend reading a white paper by Denise Backhouse and Patrick Burke, which is part of the Appendix hereto: "Seeking a Balance in the Discovery Equation: Pre-Trial Disclosure/Discovery in UK and US Civil Litigation of European-Based Data." Portions of this whitepaper are excerpted herein.[758]

In principle, absent specific justification, the EU Directive restricts the "processing" and subsequent transfer outside of the European Economic Area (EEA) of "personal data" by "data controllers" and "data processors." These terms, deceptively familiar to the ears of US litigators, take on special meanings under the EU Directive and associated national laws. Understanding them is key to comprehending the reach of the EU data-protection laws.

Under the EU Directive, "personal data" is defined as: "any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[759] This encompassing definition is generally interpreted to include business e-mail and electronic records which by their nature contain identifying information in fielded metadata.

Further, heightened protections are afforded to subclasses of "sensitive personal data" that concern the data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or pertaining to the subject's health or sex life.[760] The scope of activity that constitutes "processing" is similarly expansive, including: "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[761]

---

758 On January 25, 2012 the European Commission published its proposal for harmonizing EU data protection, applying a single set of rules across Europe. While many of the overarching data-protection principles would remain, the proposed new rules expand the scope to cover businesses based outside of the EU that process the personal data of EU citizens and increase fines for noncompliance up to €1 million or up to 2% of their annual worldwide turnover (depending on whether the organization is an "enterprise"). In addition, the proposed rules expand on individuals' rights by providing a right of data portability between systems and the "right to be forgotten" or removed from an organization's files. There is also requirement that consent be explicit and a breach notification requirement. Organizations with 250 or more employees would be required to appoint a data-protection officer. The proposal is under review and it remains to be seen whether there will be significant modifications before it is approved.

759 EU Directive, Art. 2(a).

760 EU Directive, Art. 8(1).3.

761 EU Directive, Art. 2(b).

Consequently, "processing" covers almost any activity undertaken by a data controller or data processor using automatic means regarding personal data. This includes the acts of preserving and storing electronic data for litigation purposes. Furthermore, the term "processing" extends to hard-copy files that are part of an organized filing system.

Accordingly, many activities that are typically associated with discovery compliance or with conducting an internal investigation in general, such as the collection, preservation, and organization of data belonging to selected company personnel, applying search terms, and the review of selected data, would all fall within the broad definition of "processing." For example, under the European Union ("EU") Data Protection Directive and related national enabling legislation, measures taken simply to preserve emails and electronic records for potential use in a UK or US lawsuit under a litigation hold directive are in themselves likely to violate protected European employee privacy rights.

A "data controller" is "the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[762] Many key provisions of the data-protection legislation focus on the data controller. Moreover, "the law of the EEA[763] country where the 'data controller' is established will apply to the question of whether the relevant personal data can be legitimately 'processed' under the EU Directive and the local laws which implement the [EU] Directive."[764] Furthermore, if separate entities in a corporate group are established in several countries with different personal data-processing laws, the laws of each country could apply to the processing of personal data.[765]

A "processor" is a "natural or legal person . . . or any other body which processes personal data on behalf of the controller."[766] As with "processing," the term "processor" has a much broader meaning than in the United States, where typically it refers to a technology service provider retained to prepare electronically stored information for use in discovery. In contrast, under the European laws the term includes any entity that stores or processes data in its ordinary course of business.

The EU Directive and member state data-protection acts ("DPA"s) set out certain exceptions to the general prohibition on processing and transferring personal data outside of the EEA, and to the extent that it is permitted, establish criteria for proceeding with data processing and transfer. Although several of the exceptions grounds appear on their face to provide adequate justification to proceed with UK or US discovery, piecemeal guidance over many years warned practitioners to be cautious in their reading of the provisions, particularly when the case is litigated from a non-European court.

Article 8's prohibitions do not apply if the data subject gives explicit consent to the processing of the data, or where the processing is necessary to meet the obligations of the controller in the field of employment law, or to protect the vital interests of the data subject or another person where the data

762 EU Directive, Art. 2(d).

763 The European Economic Area, or EEA, consists of the EU member states plus Iceland, Norway and Liechtenstein.

764 The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery at (Public Comment Version Aug. 2008) (the "Sedona Framework)") at 12.

765 Id.

766 EU Directive, Art. 2(e).

subject is incapable of giving his or her consent.[767] Similarly, processing by certain types of foundations or trade unions may be an exception to the general proscriptions of the directive, as is the processing of data made public by the data subject.[768] Other exceptions exist in the context of medical treatment and law enforcement.[769]

Article 29 of the EU Directive established an independent Working Party with advisory status, composed of a representative of each EU member state's data-protection and privacy authority. Over many years, the Article 29 Working Party has provided piecemeal guidance on a variety of issues concerning cross-border discovery. In February 2009, the Article 29 Working Party issued WP 158[770], in which it recognizes the tension between US disclosure obligations and European data protection requirements.

The document focuses on US, not UK, electronic disclosure requirements, which hew to more "proportionate" obligations and have yet to create the same level of conflict with EU data-privacy restrictions. However, while explicitly acknowledging that "the parties involved in litigation have a legitimate interest in accessing information that is necessary to make or defend a claim," the Working Party cautioned that "this must be balanced with the rights of the individual whose personal data is being sought."[771] The following is an analysis of guidance in interpreting the EU Directive and related national legislation provided by the Article 29 Working Party in WP 158 and earlier publications.

To the extent that company records contain employee "personal data," any "processing" of that data must be "lawful" and in accord with the EU Directive and applicable national DPAs. Moreover, Article 6 of the EU Directive requires that data controllers ensure that personal data is:

(a) Processed fairly and lawfully.
(b) Collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical, or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.
(c) Adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed.
(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.
(e) Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member states shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical, or scientific use.

767 EU Directive, Art. 8(2)(a)(c).
768 Id. Art. 8(2)(d), (e).
769 See id. Art. 8(3)-(7).
770 Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf
771 Id. at 2.

The Article 29 Working Party has examined the concept of lawful processing in detail. Lawful processing must address the principles of finality, legitimacy, proportionality, and transparency.[772]

Here, "finality" requires that personal data "must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes." Id. "Legitimacy" requires that data only be processed for legitimate purposes and in accord with the provisions of Article 7 of the EU Directive. Id. "Proportionality" forbids the processing of data for a purpose beyond that for which it was collected and requires that the processing of personal data so collected "still [be] fair to the worker." "Transparency" requires that employers notify employees of the data they are collecting about them, give employees access to and as the case may be, update such data upon request, and inform employees of why the data is being processed, the categories of entities to which the data may be disclosed, and the eventual transfer/disclosure of their personal data outside of the EU.

While Article 6 of the EU Directive spells out what a controller must consider when it is permitted to process personal data, Article 7 enumerates the circumstances in which processing can take place at all.[773] On their face, provisions regarding consent (Art. 7(a)), compliance with a legal obligation (Art. 7(c)), and legitimate interests (Art. 7(f)) appear to provide sufficient bases for processing employee data in the context of discovery compliance.

However, these provisions are construed narrowly. While meeting a legal obligation (Art. 7(c)) looks like a good fit for proceeding with US discovery compliance, in fact the legal obligations must arise under domestic or communitywide legal obligations.[774]

Regarding consent, the Article 29 Data Protection Working Party has stated that it must be freely given and rescindable at will.[775] Furthermore, specific and fully informed consent is required.[776] Thus, if a controller seeks consent from a data subject regarding the processing of his or her personal data, the controller will need to specify the purpose for which the data is to be processed and the means and manner of the data processing. See id.

Furthermore, the controller can process the data only for the specific purpose for which the data was collected and may not commingle the data with other data collected for some other purpose. See id. Obtaining "consent" appears to be one of the few promising approaches for US (and UK) litigators to effectuate collection and production of European employees' ESI within the bounds of EU data privacy. Relying on consent, however, can be problematic.

Even in those matters where consent is a strategic possibility, the need to obtain consent from all data subjects—not just the record custodian—and the right of data subjects to withdraw their consent

---

772 See Article 29 Data Protection Working Party, Opinion 8/2001 on the Processing of Personal Data in the Employment Context (Sept. 13, 2001), (5062/01/EN/Final WP 48) (WP 48) at 3, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf.

773 See EU Directive, Art. 7(a)-(f).

774 See Article 29 Data Protection Working Party, Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime (Feb. 1, 2006), (00195/06EN WP 117) (WP 117) (finding that "any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive 95/46/EC").

775 See WP 48 at 23; WP 187.

776 Id.

or to cure any incomplete or inaccurate information poses substantial hurdles for parties relying on consent as a basis for processing.[777]

In WP 158, the Article 29 Data Protection Working Party stated that it considers it "unlikely that in most cases consent would provide a good basis for processing."[778] In reaching this conclusion, the Working Party explained that the consent of third parties identified in the data (for example, customers) is required and assessed the related practical difficulties.[779] The Working Party also noted that for consent to be freely given, data subjects "must have a real opportunity to withhold . . . consent without suffering any penalty, or to withdraw it subsequently if [the data subject] changes his mind."[780] For these reasons, the Working Party reiterated its earlier conclusion that "[r]elying on consent may . . . prove to be a 'false good solution,' simple at first glance but in reality complex and cumbersome."[781]

The Working Party observed that "the requirements of the litigation process may be found to be necessary for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed under Article 7(f)" and thus justify the processing of personal data.[782] The authors also state, however, that "[t]his basis would only be acceptable where such legitimate interests are not overridden by the interests of fundamental rights and freedoms of the data subject." Id.

Factors in the necessary "balance of interests" test between the controller and the data subject require examining the fundamental concepts of proportionality, transparency and notice, data access and the right to cure, and data security. Proportionality is derived from Article 6 of the EU Directive, which requires the fair and lawful processing of data and that data be collected for "specified, explicit, and legitimate" purposes. This requires "data controllers involved in litigation to take such steps as are appropriate . . . to limit the discovery of personal data to that which is objectively relevant to the issues being litigated."[783]

To accomplish this, the Working Party recommends applying filters to limit the processing of data not called for in the litigation.[784] It also observed that filtering should take place locally, where the personal data resides, before the portion deemed relevant to the litigation is transferred to another, non-EEA jurisdiction.[785] For a discussion of how companies have used EnCase® network-based filtering and collection technology to accomplish "surgically" targeted collection of German employees' ESI to the satisfaction of certain German works councils, see Guidance Software's white paper, included in the Appendix hereto, entitled "Obtaining German Works Council Approval to Collect Employee E-mail and Electronic Documents". Companies use EnCase eDiscovery technology

777 See EU Directive, Art. 12(b) (data subject has the right to rectify incomplete or inaccurate data); EU Directive, Art. 14(a) (data subject's right "to object at any time").

778 Id. at 8.

779 Id.

780 Id. at 9.

781 Id. (quoting Article 29 Data Protection Working Party, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (Nov. 25, 2005), (2093/05/EN WP 114) (WP 114) at 11, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

782 See WP 158 at 9.

783 WP 158 at 10.

784 Id. at 11.

785 Id.

to search European employees' ESI and collect only that ESI which contains certain keywords and falls within relevant timeframes, leaving the remaining non-responsive ESI untouched. These companies are able to provide employees with reassurance that truly personal communications are not being swept up, reviewed, and disseminated.

Once implemented, the surgically targeted collections can be made transparent to employee representatives, who can receive notification each time the search technology is used. This provides employees with the opportunity to decide–on a case-by-case basis–whether, and to what extent, their privacy rights have been implicated.

Organizations can also build trust with their European employees through transparency of process and technology. Before implementing a collection approach, companies are well advised to sit down with employee representatives, unions and/or works councils to explain the techniques and privacy safeguards being employed. Such advance notice, and invitations for employee feedback, can go a long way.

The Working Party suggests, where possible, the use of anonymization or redaction techniques. Id. These tools attempt to "scrub out" the names, e-mail addresses and other personal information through the use of search algorithms. Some UK and US litigators have followed this approach, finding ways to use the content of the ESI while adapting to their inability to know the identities of the authors and recipients of communications, as well as the other scrubbed-out content.

The Working Party considered the issue of who could make the objective determination of relevancy, including the possibility of outsourcing this role to a trusted third party.

The Working Party recognizes that [filtering] may cause difficulties in determining who is the appropriate person to decide on the relevance of the information, taking into account the strict time limits laid down in the US Federal Rules of Civil Procedure to disclose the information requested. Clearly it would have to be someone with sufficient knowledge of the litigation process in the relevant jurisdiction. It may be that this would require the services of a trusted third party in a Member State who does not have a role in the litigation but has the sufficient level of independence and trustworthiness to reach a proper determination on the relevance of the personal data.

The Working Party also recommended that parties in this situation should explain to the relevant US court the difficulties posed by a production request and seek a protective order to comply with EU and national rules.[786]

Transparency addresses the kind and timing of information that must be provided to a data subject when his or her data is being processed in accord with Article 7(f) of the EU Directive. Relying on Article 10 of the EU Directive, the Working Party opined that, in the context of pre-trial discovery, data subjects should receive advance, general notice of the possibility of personal data being processed for litigation in the United States and that once personal data was processed for discovery purposes, the identity of any recipients of the data should be given to the data subject; the purposes of the processing and the categories of data at issue should be identified, and data subject should be informed of their rights with respect to that data. Id.

786 Id.

Similarly, under Article 11, notice should be provided to data subjects "as soon as is reasonably practicable after the data is processed" in those situations where the data is collected from a third party (e.g., computer data from the employer's network) and not directly from the subject. Id. Interestingly, the Working Party also observed that the timing of notice contemplated by Article 11 concerning data in the possession of a third party could be delayed if there is a risk that such notice would jeopardize the safety or integrity of the data and/or impede the company's ability to investigate matters.[787] The Working Party cautioned that such an exception regarding notice "must be applied restrictively on a case by case basis." Id.; see also WP 117 at 13 (discussion of Article 11 notice in the context of the establishment of whistleblower hotlines).

This notice is more than an informational tool. It provides the data subject with an opportunity to exercise his or her "right to object at any time on compelling legitimate grounds to the processing of the data relating to them" under Article 14 of the EU Directive. WP 158 at 12; see also WP 117 at 9. Compelling legitimate grounds for such objection would include violations of the EU Directive's principles of data quality and proportionality (as found in Article 6 of the EU Directive and discussed supra), notice (as addressed by Articles 10 and 11), rights of access, rectification, and erasure under Article 12, and the secure handling of data as required by Article 17.[788]

The data subject's right to access his or her data and to cure inaccurate or incomplete data is another fundamental right that must be balanced when assessing the feasibility of processing data under Article 7(f) of the EU Directive. Moreover, Article 12 gives the data subject the right to have access to the data held about him or her in order to check its accuracy and rectify it if it is inaccurate, incomplete, or outdated. And, as noted by the Working Party, the right to access and to cure allows a data subject to check the personal data that has been processed and to satisfy himself or herself that the data to be transferred "is not excessive."[789]

Of all the rights examined thus far when considering whether the processing of personal data under Article 7(f) is a possibility, the right to data access and cure poses significant issues for counsel conducting an internal investigation or, worse yet, responding to a disclosure or discovery demand or investigative subpoena. For example, giving document custodians the ability to winnow out "excessive" materials raises compliance concerns about the completeness of a US production and could lead to the expenditure of a great deal of time, effort, and money validating the decisions made by custodians. This problem is circumvented by companies that have the capability–provided by EnCase eDiscovery–to apply targeted search and collection technology against the various locations on the network where employees' ESI resides.

Similarly, altering or removing data from a "production set" of materials as a result of withdrawals of employees' consents could give rise to allegations of spoliation or obstruction. Indeed, the Working Party, with measured understatement, noted that "this right could give rise to a conflict with the

787 Id. at 12.

788 See WP 117 at 9- 15.

789 WP 158 at 12.

requirements of the litigation process to retain data as at a particular date in time and changes (whilst only for correction purposes) would have the effect of altering the evidence in the litigation."[790]

The final factor to be weighed concerns the need for the data controller to "take all reasonable technical and organizational precautions to preserve the security of the data to protect it from accidental or unlawful destruction or accidental loss and unauthorized disclosure or access," as mandated by Article 17 of the EU Directive.[791] The aforementioned precautions apply not only to the controller, but to other actors in the litigation drama, including the law firms involved in the matter, the court adjudicating the matter, and retained experts, who must also comply with the principles of the EU Directive.[792]

Given the complexities associated with processing personal data, passage along the road to the lawful and fair processing of employee data subject to the rules established by the EU Directive and the laws enacted by EEA states is neither easy nor quick. Because of this, companies and their counsel should, where possible, begin assessing avenues for the processing of data in the EU before an immediate need arises.

Companies facing the data-processing challenge posed by the European rules and regimes must consider nuances in the local statutory regime, state-specific precedent on the topic of personal data protection, formal and/or informal rulings or guidance offered by national data protection bodies, as well as the applicability of regulations outside the context of data protection (other applicable restrictions may arise under, for example, blocking statutes, industry- or subject-matter specific laws, and labor and workplace laws and regulations).

Assuming that a mechanism can be found to process personal data, a means must be found to facilitate the onward transfer of that data from its home to the United States so that it can be examined by counsel or produced in litigation. As was the case with processing, the onward transfer of personal data from the EEA to the United States has its own labyrinth of rules that must be negotiated. Transfer to the UK is, of course, less problematic, although not always without legal obstacles.

Turning to the concept of onward transfer, the EU Directive and national DPAs significantly restrict the transfer of personal data to locations outside of the EEA. With a few exceptions, transfer of data to countries lacking an adequate level of protection for personal data is prohibited; specifically, the United States is deemed to provide inadequate protection.[793] It is not, usually, an issue with regard to transfers to the UK. Although the term "transfer" is not defined, the EC has stated that "all the cases where a controller takes action in order to make personal data available to a third party located in a third country" could be deemed a transfer of personal data. To the extent the data controller is located in a Member State, the laws of that state will dictate whether and how personal data can be transferred outside the European Community.[794]

790 See WP 158 at 12.
791 Id.
792 Id. at 12-13.
793 See EU Directive, Art. 25.
794 Transfer FAQ, page 19.

If the data controller is located outside the Community, the laws of the Member State where the processing equipment is used will apply.[795] Article 26 of the EU Directive addresses derogations to that general prohibition. Possible grounds for onward transfer of data from the EEA to a location like the United States, include apparently promising grounds of unambiguous consent by the data subject[796] and/or that the onward transfer is "necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims."[797]

Unfortunately, both exceptions, like those relating to processing, are limited as to transfers to the US. For example, consent in this context must be given prior to the transfer, and be unambiguous, specific to the transfer at issue, freely given, and informed.[798] Furthermore, consent must be obtained from all identifiable data subjects, and not just the data custodian. The conditions under which an onward transfer can be justified as being "legally required" are also interpreted narrowly by the Article 29 Data Protection Working Party.

The Working Party emphasizes that the concept of "establishment, safeguarding or defense of legal claims" must here again be subject to strict interpretation. Thus, for example, the parent company of a multinational group, established in a third country, might be sued by an employee of the group currently posted to one of its European subsidiaries. The exception in Article 26(1)(d) appears to allow the company to legally request the European subsidiary to transfer certain data relating to the employee if these data are necessary for its defense.[799]In addition, this exception can only be applied if the rules governing criminal or civil proceedings applicable to this type of international situation have been complied with, notably as they derive from the provisions of the Hague Conventions of 18 March 1970 ("Taking of Evidence" convention) and of 25 October 1980 ("Access to Justice" Convention). WP 114 at 15.

The Working Party members revisited these issues in WP 158, stating that "[w]here the transfer of personal data for litigation purposes is likely to be a single transfer of all relevant information, then there would be a possible ground for processing under Article 26(1)(d) of the Directive where it is necessary or legally required for the establishment, exercise or defense of legal claims."

This potentially helpful exception, however, is very limited. First, this applies in the context of "litigation": a transfer based on Article 26(1)(d) cannot be premised "on the grounds of the possibility that legal proceedings may be brought one day in US courts."[800] Second, a requirement of a single delivery of data, although possible in some matters, does not allow for supplemental production or

795 Id.

796 Art. 26(1)(a).

797 Art. 26(1)(d).

798 See EU Directive, Arts. 2(h), 26(a).

799 Council Directive 95/46/EC, at 46 (exception applies when "the transfer is necessary or legally required… for the establishment, exercise or defence of legal claims."); but see, Article 29 Working Party, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, 15 (Nov. 25, 2005) ("The exception in Article 26(1)(d) appears to allow the company to legally request the European subsidiary to transfer certain data relating to the employee if these data are necessary for its defense. In any event, this exception cannot be used to justify the transfer of all the employee files to the group's parent company on the grounds of the possibility that such legal proceedings might be brought one day.").

800 WP 158 at 13, citing WP 114 at 15.

future additional custodians. Third, the reference to "relevant" presupposes that a relevancy review has taken place within the EEA member nation in which the data is located.

Nevertheless, WP 158 may suggest a softened approach to the use of the Hague Convention as a necessary step to using Article 26(1)(d) as a basis for the onward transfer of data from that stated in WP 114, which is quoted above.[801]

Although a discussion of all the issues associated with reliance on the Hague Convention as a means of facilitating discovery is beyond the scope of this paper, the Working Party's take on the efficacy of resort to the Hague seems optimistic: "[w]hilst there may be some concerns about the length of time such a procedure could take, the courts, for example in the U.S., are experienced in the use of the Hague and such timescales can be built into the litigation process." Moreover, US courts take the view that the procedures afforded by the Hague Convention are but "one method of seeking evidence [abroad] that a court may elect to deploy."[802]

Indeed, the complexities associated with invoking the Hague Convention, the timeframe associated with achieving results under the Hague, and the convention's requirements for specificity with respect to how document requests must be made are among the reasons cited by US litigants for proceeding abroad under the Federal Rules of Civil Procedure, without resort to the treaty. Furthermore, resort to the Hague treaty would not be an option in matters that had not yet ripened into an actual case.

In WP 158, Working Party authors recognize that resorting to the Hague Convention cannot be an absolute precondition for the onward transfer of personal data, because some EEA member nations have not signed the Hague Convention and other members that have signed it did so with reservations under Article 23 of the treaty with respect to compliance with discovery demands arising from foreign—i.e., US—litigation.[803]

For example, France limits discovery in that country to only those means referenced expressly in the treaty, i.e., letters rogatory, depositions before a diplomatic official, or depositions before a duly appointed commissioner.[804] Similarly, Germany does not appear to permit pre-trial document discovery under the Hague Convention,[805] while Italy limits pre-trial discovery to only the tools afforded by the treaty, and further limits discovery to those matters deemed "civil or commercial"[806] under Italian law.[807].

As a result of this recognition, the Working Party now notes that resorting to the treaty for data found in countries that (1) are signatories to the treaty and (2) have not signed with reservations about US (or other foreign) discovery is an apparently independent basis for the onward transfer of

801 Hague Evidence Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, T.I.A.S. No. 7444, 847 U.N.T.S. (1972).

802 Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa,482 U.S. 522, 541 (1987).

803 See WP 158 at 13.

804 See ABA Section of Antitrust Law, Obtaining Discovery Abroad 112 (2d ed. 2005).

805 Id. at 137.

806 Id. at 158

807 See generally, Sedona Framework at 17, citing Soiret, The Foreign Defendant: Overview of Principles Governing Jurisdiction, Venue, Extraterritorial Service of Process and Extraterritorial Discovery in US Courts, 28 Torts & Ins. L.J. 533 (1993).

personal data: "Where it is possible for the Hague Convention to be used, the Working Party urges that this approach should be considered first as a method of providing for the transfer of information for litigation purposes."[808]

Given the limitations on invoking the Hague Convention, for a company trying to review materials in order to meet regulatory obligations or to detect internal wrongdoing, compliance with Article 26(1)(d) or a handful of narrowly tailored alternative avenues for the onward transfer of data are the only options available for now.

Furthermore, the French Commission nationale de l'informatique et des libertés, CNIL, has recently published its own recommendations on the transfer of personal data specifically in the context of American discovery proceedings.[809].

In its Recommendations, the CNIL generally endorses the data-processing principles explained above, but also confirms that all US discovery requests must comply not only with applicable French data protection laws, but must also be made through the Hague Convention, in accordance with the French blocking statute.[810]

Companies and counsel subject to UK disclosure and US discovery obligations are actively seeking a way forward that respects the privacy rights of Europeans. The Article 29 Working Party cited The Sedona Framework in WP 158 and is engaged in dialogue with the Sedona Conference, which it is hoped will eventually result in a more nuanced appreciation and understanding of the issues on both sides of the discovery equation. Such endeavors highlight the points of similarity in the different systems.

In the absence of agreed-upon protocols, a company with data residing in Europe that might be used in or transferred to the United States should consider taking the following data-protection "readiness" steps to position itself to best address the dictates of the EU Directive:

A. Implement audited and certified data-management policies and procedures designed to minimize the potential for privacy infringement. These measures should include:

   (1) Structuring or segregating data to facilitate the ready identification of personal data, especially data of a highly personal or sensitive nature.
   (2) Implementing in-house technology – such as EnCase® eDiscovery – that enables companies to conduct surgical collections of European employees' ESI that protects against collection of employees personal data except that which meets targeted search criteria.
   (3) Availing themselves of technologies that can be used to anonymize or redact data (to the extent the use of such technology is otherwise consistent with discovery or other legal obligations).

808 WP 158 at 14.

809 The official text in French is available at: http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT00002098 1625&dateTexte=&oldAction=rechJO&categorieLien=id.

810 Law no. 68-678 of July 27, 1968, created by law no. 80 538 of July 16, 1980.

(4) Informing data subjects and their representatives, through their respective European employers, of any further transfer of their personal data, for company management purposes and/or compliance with US mandatory laws.
(5) Implementing computer systems and email usage policies that clearly define acceptable usage of computers and networks and the ownership of that equipment and data on that equipment, and that set users' expectations of privacy for the data stored on the machine or device they use.
(6) Obtaining, when necessary, general and matter-specific consent from employees/data custodians. While as previously discussed, consent in itself may be of limited value, it may have the practical effect of setting expectations and reducing the likelihood of surprise and complaints.

B. The company should consider taking steps to familiarize itself with the nuances of the applicable legislation and with existing means that can be used to facilitate the flow of data between Europe and the United States and/or among EU member states. For example, the company might:

(1) Designate an employee or select counsel to liaise with local data-protection officials in an effort to make sure any local authorization or certification is received for transfers of data; and/or
(2) Take advantage of existing mechanisms for the transfer of data from the EEA to the United States. These mechanisms include enrolling in the Safe Harbor certification program sponsored by the US Department of Commerce, the use of Standard Contractual Clauses, and/or the implementation of Binding Corporate Rules (BCRs) governing inter-company data transfers. While a full discussion of these mechanisms is beyond the scope of this section, it should be noted that each of them requires adherence to strict rules that may severely limit their application to a situation in which information is being gathered in Europe and then transferred to the US for disclosure to a third party, such as a federal investigating agency or an adverse party in a litigation matter.

C. In the context of responding specifically to US discovery requests, a company should consider the following options:

(1) Carefully consider the nature of the discovery request to determine whether some portion of the information sought resides in the United States or is otherwise available from a source that does not implicate EU data-protection issues.
(2) Work closely with local in-house IT or IT Security personnel or, where appropriate, third-party service providers resident in the member nation, to filter or cull the data (e.g., by the use of key terms) so that extraneous information is eliminated before it is used in or transferred to the United States. Both WP 158 and the CNIL Recommendations

contemplate the leveraging of trusted third-party service providers in managing the discovery process.

(4) Alert the US court or agency to the data-protection issues and seek a protective order or confidentiality agreement pertaining to the materials, including an end-of-matter data disposition plan.

(5) Work with opposing counsel or the agency requesting the data in an effort to narrow the scope of the request as much as possible and to agree to a court order setting protocols for tighter security and confidentiality for European employees' data produced, even when used as evidence in the case.

(6) Consider the use of Standard Contractual Clauses to facilitate the onward transfer of data to third parties.

(7) Carefully consider whether there are any additional national laws and rules--especially those aimed at thwarting "foreign" discovery--that might come into play.

United Kingdom

The legal obligations with respect to electronic disclosure–as electronic discovery is known in the UK–-have evolved dramatically over the past few years. Much of the impetus for the new recognition of the importance of e-disclosure to the proper adjudication of civil litigation has come from the judiciary itself, confronted with the growing reality that more and more of the critical evidence in cases consist of e-mail and electronic documents. For a deeper treatment of these issues, we recommend you read two white papers found in the Appendix, portions of which have been excerpted in this section:

- The Place of EnCase® eDiscovery in Electronic Disclosure for Major Corporations in UK Courts (by Chris Dale)
- eDisclosure after Jackson: Developments in Electronic Disclosure in England and Wales (with an update on US eDiscovery Law) (by Chris Dale, Denise Backhouse and Patrick Burke)
- The Civil Procedure Rules ("CPR") feature a narrower scope of discovery under Part 31 than previously required under the Rules of the Supreme Court. Specifically, previous discovery rules required a party to turn over relevant documents, or documents "relating to matters in question in the action," whereas now the analysis does not turn on relevancy, but rather on specific language featured in Part 31.6 of the CPR, "Standard disclosure-what documents are to be disclosed":

  31.6 Standard disclosure-what documents are to be disclosed

  Standard disclosure requires a party to disclose only:

  (a) The documents on which he relies; and
  (b) The documents which-
    (i) Adversely affect his own case;

(ii) Adversely affect another party's case; or
(iii) Support another party's case; and
(c) The documents which he is required to disclose by a relevant practice direction.

Essentially, a party is required to disclose the existence of documents on which he relies, those which adversely affect his case, and those which support or adversely affect another party's case. This narrow scope protects against the "delivery of thousands of documents which may [just] be relevant but which add nothing to the judge's fact-finding exercise."[811]

Under the CPR, parties can request disclosure of documents which are "just relevant," but such requests are subject to the court's discretion to tailor disclosure to the issues and circumstances of the case. Among the factors the court will consider are not only the legal principles at issue in the case, but also the practicalities and costs of disclosure.

Under the broad scope of previous UK disclosure rules, electronic disclosure of anything relevant often created a large volume of responsive documents which inevitably leads to high costs of review on the back-end. By contrast, the new CPR limits disclosure to documents that matter to the parties involved, which has the potential to limit review costs. However, the cost burden of electronic disclosure may only be lessened if the parties are efficient in their ability to identify documents that matter.

The most important themes in the UK are the following:

- Education as to the rules and practice
- The need to understand the technology
- The duty of cooperation
- The primacy of original documents as evidence
- Preservation of evidence
- The role of the court in case management

An agenda prepared for US purposes would look very similar. Lord Justice Jackson's Final Report[812] stated:

> The first point which needs to be made about e-disclosure is that it is inevitable in cases where the parties hold the relevant material electronically. For the parties to print all the material out and then exchange it in hard copy would often be impracticable. With all but the smallest volumes of material, that course would not be cost effective. Thus in cases where edisclosure is a consideration, it is often a practical necessity rather than an optional course.[813]

811 Id.
812 Available at: http://www.judiciary.gov.uk/about_judiciary/cost-review/jan2010/final-report-140110.pdf.
813 Jackson Report at Para 2.1 on page 365.

The same point recurs in two quotations from *Earles v Barclays Bank Plc* [2009] EWHC 2500 (Mercantile) (08 October 2009)[814]:

> Since 2000 most key contemporaneous commercial documents are contained in Electronically Stored Information ["ESI"] – today over 90% of communications are recorded in that form – phone records, texts, e-mail, bank records etc. ESI are "documents" under the Civil Procedure Rules: CPR 31.4 and 31PD.2A. Accordingly, the rules for "Standard Disclosure" apply: CPR 31.6. i.e. "only" those documents that are "supportive" or "adverse" to each party's cases. The abundance of this ESI in cyberspace means that potential litigants, in particular organizations such as Banks at the current time, need to anticipate having to give disclosure of specifically relevant electronic documentation and the means of doing so efficiently and effectively.[815]

> It might be contended that CPR 31PD 2A and electronic disclosure are little known or practiced outside the Admiralty and Commercial Court. If so, such myth needs to be swiftly dispelled when over 90% of business documentation is electronic in form. The Practice Direction is in the Civil Procedure Rules and those practising in civil courts are expected to know the rules and practice them; it is gross incompetence not to.[816]

There is an acceptance that most documents are electronic, that it is cheaper to handle electronic documents electronically, that the disclosure rules cover them, and that ignorance of the rules is unacceptable.

The usual order is for "standard disclosure," which requires that a party disclose only the documents on which he relies, hose which adversely affect his own or another party's case, and those which support another party's case (Rule 31.6). A party is required only to make a reasonable search, "reasonable" being judged by a set of factors set out in Rule 31.7 and in the Practice Direction to Part 31.

Paragraph 2 of the Practice Direction, inserted in 2005, imposes obligations specific to electronic disclosure, including an obligation to discuss sources with opponents before the first case-management conference, the form in which documents are to be exchanged, and the keyword or other forms of electronic search that may be used. The first two of these but, curiously, not the third, expressly provides that difficulty or disagreement must be referred to the judge at the earliest practical date, if possible at the first case-management conference. The absence of such an obligation in respect of keyword searches does not prevent it from being raised as an issue before the court.

It is generally assumed that standard disclosure is automatic, but the strict position is that standard disclosure follows an order to that effect made usually at the first case-management conference. It is

814 Available at: http://www.bailii.org/ew/cases/EWHC/Mercantile/2009/2500.html.

815 Id. at Para 21.

816 Id. at Para 71.

open to the parties to agree that there be no disclosure, or disclosure in stages or disclosure on a basis wider than standard disclosure; any such order is subject to the court's approval.

The court has a general duty of active management (Rule 1.4) in pursuit of the overriding objective (Rule 1) and, as a general matter may, in addition to any specific powers and duties, "take any other step or make any other order for the purpose of managing the case and furthering the overriding objective."

The invisibility of the practice direction to Part 31 CPR, and in particular the absence of both inter-party discussion and judicial management, was highlighted in 2008 by *Digicel (St. Lucia) Ltd & Ors v. Cable & Wireless Plc & Ors*.[817] There was no discussion between the parties before the case-management conference, and the judge hearing it simply made an order for standard disclosure.

After disclosure, the claimants brought two applications, one as to the scope of the keywords used by the defendants to reduce their document population, and one as to 800 or so backup tapes which the defendants disclosed as existing but said of them that it was disproportionate to investigate them. Both of these subjects should, of course, have been discussed pursuant to the practice direction quite apart from the general duty of cooperation imposed by the rules.

The result in that case was an order that the defendants redo their searches using a set of keywords decided on by the judge and that they should begin immediate discussions as to the tapes. In the wider sense, the result of the case was a new focus on the disclosure obligations. That, it has to be said, did not attract the attention it deserved, in the sense that it remained possible a year later to ask an audience if they had heard of either the practice direction or *Digicel* and get almost no response, even amongst those who had self-selected as being interested in the subject. At a high judicial level, *Digicel* was undoubtedly one of the factors that prompted the Deputy Head of Civil Justice to ask Senior Master Whitaker to devise a questionnaire whose function was to provide a formal framework for the discussions required by Paragraph 2A.2 of the practice direction.

Lord Justice Jackson's Report on Litigation Costs

The best summary of what was intended by the practice direction and questionnaire is contained in the final report of Lord Justice Jackson into litigation costs at page 365:

> Parties and their legal representatives should consider, at an early stage, the use of technology in order to identify potentially relevant material, to collect, analyze and review it. Subsequently this will assist with the creation of lists of documents to be disclosed and giving disclosure by providing documents in electronic format.
>
> Unless a party intends to request that the action be allocated to the small claims track or the fast track, that party must exchange with the other party or parties and file with the court Answers to the ESI Questionnaire attached to the Practice Direction.

817 [2008] EWDC 2522 (Ch) (23 October 2008).

> The ESI Questionnaire requires the parties to provide information about any documents which they hold in electronic form and which are to be disclosed in the proceedings, along with details of their electronic storage systems. They are also asked to detail any issues that may arise about the accessibility of such documents. The Answers to the ESI Questionnaire must be supported by a statement of truth.
>
> After exchange of Answers to the ESI Questionnaire and before the first CMC, the parties must discuss the disclosure of ESI, including the scope of the reasonable search for ESI and any tools and techniques which might reduce the burden and cost of disclosure of ESI.
>
> If the parties encounter difficulties or cannot reach agreement, issues arising in relation to the disclosure and inspection of ESI should be referred to a judge for directions, if possible at the first CMC.
>
> The extent of the reasonable search will depend upon the circumstances of the case. The parties should bear in mind the overriding principle of proportionality. Many of the factors that may be relevant in deciding the reasonableness of a search for ESI are listed in paragraph 2A.4 of the current practice direction supplementing CPR Part 31.
>
> Where a party is giving disclosure of ESI, a List of Documents may by agreement between the parties be an electronic file in a defined and agreed format.
>
> Unless the parties agree otherwise or the court directs otherwise, where electronic copies of disclosed documents are provided to another party, the electronic copies should, unless this is not reasonably practicable, be provided in their native format.

Having thus recited the purpose of the practice direction and questionnaire, Lord Justice Jackson went on to say at page 366:

> In my view, the substance of this practice direction is excellent and it makes appropriate provision for e-disclosure. On the assumption that this practice direction will be approved in substantially its present form by the Rule Committee, I do not make any recommendation for procedural reform in relation to e-disclosure.

Disclosure and electronic disclosure are treated as separate subjects in both the preliminary report and the final report on litigation costs by Lord Justice Jackson. One is left in no doubt as to the importance that he attaches to the subject from his opening paragraph about it at page 364, which is quoted above.

He made only one express recommendation as to e-disclosure, which was for education, expressed in the following terms:

> I recommend that e-disclosure as a topic should form a substantial part of (a) Continuing Professional Development ("CPD") for solicitors and barristers who will have to deal with e-disclosure in practice and (b) the training of judges who will have to deal with e-disclosure on the bench. Service providers will have a part to play in such CPD or training. Indeed they will have a commercial interest in contributing to the process. However, they should do so within the context of a well structured programme, which is provided or approved by the relevant professional bodies.

Many of those who submitted observations to him during the consultation phase emphasized the vital role of the judge in managing cases. The primary purpose of case management is the management of time and costs, and Lord Justice Jackson considered carefully how best to encourage judges to play their part in this.

Apart from his fairly stern references to present defects, he proposed a new Rule 31.5A, known as the "menu option"–his only other formal disclosure recommendation apart from the one about education. In addition to setting out proposed procedural matters (some of which overlap with what is proposed in the Whitaker draft practice direction) he set out expressly a range of options which judges and parties must consider, with the starting point is that none of them is the default. The options––listed at page 371–include:

a) An order dispensing with disclosure; or
b) An order that a party disclose the documents on which it relies, and at the same time requests any specific disclosure it requires from any other party; or
c) An order that (where practical) directs, on an issue-by-issue basis, the disclosure to be given by a party on the material issues in the case; or
d) An order that a party give standard disclosure; or
e) An order that a party disclose any documents which it is reasonable to suppose may contain information which may (i) enable the party applying for disclosure either to advance his own case or to damage that of the party giving disclosure, or (ii) lead to a train of enquiry which has either of those consequences; or
f) Any other order in relation to disclosure that, having regard to the overriding objective, the court considers appropriate.

Some specific powers are then recited, with the concluding recital that: "In exercising its discretion . . . the court will consider what disclosure would be proportionate to the circumstances of the case."[818]

It would be right to observe that any one of these orders could be made under the rules as they stand, having regard to what is said above about the existing scope of discretion. Lord Justice Jackson made it clear that his primary purpose here is to force a proper appraisal of cost against value to meet a test which, under the present rules, is one of proportionality. We emphasize the reference to the

818 Jackson Report at p. 372.

present rules because another part of Lord Justice Jackson's report examines, in learned but lucid style, whether the proportionality test is the right one to apply. The alternative test is one of "necessity," with the suggestion that the costs recoverable between parties should turn on whether the work done and claimed for was really necessary for justice to be achieved. Although this is not narrowly a disclosure point, the potential impact of such a change on, for example, the scope of the search is significant.

Given the express commendation of the practice and questionnaire referred to in the preceding section, it may appear to some that the Rule Committee's reluctance to adopt them is something of a rebuff to Lord Justice Jackson. After all, the obvious implication from what he said is that he would have made recommendations about procedure if the draft practice direction did not already provide adequate recommendations. If the Rule Committee proves too timid to implement the practice direction, then its fallback is to make its provisions and questionnaire usage merely matters of best practice. Given that the existing practice direction provisions have been ignored for over five years, this would scarcely be an adequate way of changing the culture.

Whatever the outcome of the deliberations of the Rule Committee's subcommittee, it is already clear that the Lord Justice Jackson's report has had significant influence on e-disclosure. Until its provisions are adopted, it remains of persuasive value only, but because so much of it is designed primarily to emphasize existing obligations, its effect must be counted as considerable.

Recent UK E-Disclosure Cases

Nichia Corp v. Argos Ltd[819]

The principles described by Lord Justice Jacob in paragraphs 46 to 54 of Nichia have been created in subsequent cases. Some quotations will suffice to give the flavour of it. It is wrong just to disclose a mass of background documents which do not really take the case one way or another. And there is a real vice in doing so: it compels the mass reading by the lawyers on the other side, and is followed usually by the importation of the documents into the whole case thereafter–hence trial bundles, most of which are never looked at. For it is the downstream costs caused by over-disclosure which so often are so substantial and so pointless. It can even be said, in cases of massive over-disclosure, that there is a real risk that the really important documents will get overlooked–where does a wise man hide a leaf?

"Perfect justice" in one sense involves a tribunal examining every conceivable aspect of a dispute. All relevant witness and all relevant documents need to be considered. And each party must be given a full opportunity of considering everything and challenging anything it wishes. No stone, however small, should remain unturned.

But a system which sought such "perfect justice" in every case would actually defeat justice. The cost and time involved would make it impossible to decide all but the most vastly funded cases. The cost of nearly every case would be greater than what it is about. Life is too short to investigate everything in that way. Subsequent cases have involved more specific reliance on particular rules, but the paragraphs in Nichia from which these extracts come remain the best summary of the principles.

819 [2007] EWCA Civ 741 (19 July 2007).

Digicel (St Lucia) v. Cable & Wireless[820]

The importance of *Digicel* has been described above. It is important not just for its conclusion, but for the workmanlike summary of best practices for disclosure and incidentally, , for its recital of the steps taken by each party illuminating what is involved in handling large volumes of documents. The importance of the practice direction is described in paragraph 47 in these terms:

> This case provides an opportunity for the Court to emphasize something mentioned in Part 31 Practice Direction which the parties in the present case disregarded. Paragraph 2A.2 of the Practice Direction states that the parties should at an early stage in the litigation discuss issues that may arise regarding searches for electronic documents. Paragraph 2A.5 of the PD states that where keyword searches are used they should be agreed as far as possible between the parties. Neither side paid attention to this advice. In this application the focus is upon the steps taken by the defendants. They did not discuss the issues that might arise regarding searches for electronic documents and they used key word searches which they had not agreed in advance or attempted to agree in advance with the Claimants.
>
> The result is that the unilateral decisions made by the defendants' solicitors are now under challenge and need to be scrutinized by the Court. If the Court takes the view that the Defendants' solicitors' key word searches were inadequate when they were first carried out and that a wider search should have been carried out, the defendants' solicitors' unilateral action has exposed the defendants to the risk that the court may require the exercise of searching to be done a second time, with the overall cost of two searches being significantly higher than the cost of a wider search carried out on the first occasion.

The judge also gave a reminder of why proper searches for electronic documents are important as a matter of evidence. He said in paragraph 46:

> It must be remembered that what is generally required by an order for standard disclosure is "a reasonable search" for relevant documents. Thus, the rules do not require that no stone should be left unturned. This may mean that a relevant document, even "a smoking gun" is not found. This attitude is justified by considerations of proportionality. This point is well made by Jacob LJ in *Nichia Corporation v. Argos Limited* [2007] EWCA Civ 741 at [50] to [52].

This paragraph has particular resonance in the light of two at least of the cases that we will discuss below, *Earles v Barclays*, which stressed the primacy of contemporaneous documents, and the *Ofsted*

820 [2008] EWCH 2522 (Ch) (23 October 2008).

case, where the documents produced at a late stage included prior drafts of the report on which the central issues turned.

Earles v. Barclays Bank Plc[821]

Earles, decided by His Honour Judge Simon Brown QC, is important chiefly for the criticism made by the judge of the defendants and its lawyers for the failure to disclose documents central to the issues. The claim concerned transfers between accounts of £265,000, and the central issue was whether the bank had authority to make such transfers. The judgment drew attention to the relevant rules and the lawyers' duty to know and comply with them (the relevant passage, with its reference to "gross incompetence," is quoted at the beginning of this paper) but emphasized still more the fact that time and money had actually been wasted because of the need to examine witnesses on points which would have been disposed of quickly and easily with the documents had been available. Some key language from this opinion includes:

> As regards disclosure, the bank failed to give disclosure of the Transfer Sheets referred to in paragraph 53 of the witness statement of Katharine Shelley. They were clearly relevant under the narrow test of CPR 31.6 to the primary issue in the case. The very fact that they were referred to in the carefully crafted witness statement proves that and it ought to have been obvious to the Defendants lawyers. Their absence made the task of the Court immeasurably harder to the extent that it considered lengthy submission as to whether or to draw adverse inferences against the Bank itself. I am satisfied that it was a decision of the legal team on the erroneous grounds of disproportionality.

The judgment is important also for its summary of the primacy of documentary evidence in circumstances where witnesses are unlikely to be able to remember what happened.

> It is not realistic to expect any human beings to recall with any reliability what they said 3 years ago about run of the mill business transactions. Therefore it is crucial to follow the guidance of these very eminent jurists and in particular those emphasized regarding the analysis of contemporaneous documents; objective facts and documents; witnesses motives and overall probabilities.

Lastly, the *Earles* judgment raised interesting points about the duty to preserve documents, an area which is less advanced in English law than in the US Although the defendants were successful, the costs awarded to them were substantially reduced as a result of their conduct in relation to disclosure.

821 [2009] EWCH 2500 (Mercantile) (08 October 2009).

Goodale v. The Ministry of Justice[822]

This is a judgment of Senior Master Whitaker, and provides a textbook example of the approach that a case-management judge should take when the only thing known about the document populations is that they are potentially very large. The Ministry approached the case management conference asserting that they did not intend to give disclosure of any electronic documents–not that they did not have any, not that they had none which were relevant, not that they had weighed the costs against the value in any real sense, but merely that they did not intend to disclose them. Since the point at issue (the government's policy in dealing with opiate-dependent prisoners) necessarily involved evidence of treatment across a wide range of people and places, as well as matters of policy, it was inevitable that such an approach would be deemed unacceptable by the senior master.

The chief significance of the judgment is that the Senior Master ordered the use of the ESI questionnaire in the event that the parties needed to come back to court. The questionnaire was, as it remains, a draft under consideration by the Rule Committee, and its use is a good example of a judge taking a hands-on and pragmatic approach to helping the parties to satisfy their obligations to the court.

The judgment is important, however, beyond the fact that it was the first public appearance of the questionnaire. Two things in particular stand out: an order for a staged and iterative approach to identifying the scope of the problem before making final decisions, and the recommendation that technology be used to reduce the volumes to a manageable size. The first of these points is illustrated by this quotation:

> It seems to me that the proper way of going about this in respect of the individuals is that the limited searches that could be run on the MEDS system should be run but without the actual physical review and production of those documents in the first place. We need to know how many documents each of the 31 terms are going to turn up to establish whether any may require a degree of fine-tuning. We also need to know the total number of documents that respond to this collection of search terms (acknowledging that the same documents may respond to more than one search term in many cases). There is probably going to be some question over whether all the 31 key words are necessary, because what little bit of sampling that has been done seems to reveal, that quite a few of them produce nil returns anyway. We shall see whether that is the case in respect of Palmer, Bradshaw and Piper as well as Marteau when those searches are run.

What Master Whitaker said about technology is an illustration of what Lord Justice Jackson said about the need for judges to know something of the available technology:

822 [2009] EWHC B41 (QB) (05 November 2009).

> At the moment we are just staring into open space as to what the volume of the documents produced by a search is going to be. I suspect that in the long run this crude search will not throw up more than a few hundred thousand documents. If that is the case, then this is a prime candidate for the application of software that providers now have, which can de-duplicate that material and render it down to a more sensible size and search it by computer to produce a manageable corpus for human review – which is of course the most expensive part of the exercise. Indeed, when it comes to review, I am aware of software that will effectively score each document as to its likely relevance and which will enable a prioritisation of categories within the entire document set.

Vector Investments v. Williams[823]

Although not an e-disclosure case, *Vector Investments v. Williams* provides another example of a successful party losing a proportion of the costs which would otherwise be recoverable--in this case £20,000--because of the manner in which it gave disclosure. The defects in that case involved duplication, lack of order, and the inclusion of documents that were irrelevant to the issues. The application of these principles to electronic documents is obvious.

Shoesmith, R (on the application of) v. OFSTED & Ors[824]

The Shoesmith case attracted attention because the underlying story was a matter of deep public interest. Sharon Shoesmith was Head of Children's Services at the London Borough of Haringey when a child known as Baby P died at the hands of those with whom he lived. A report was prepared by Ofsted, the regulating authority, for submission to Ed Balls, the Secretary of State for Education. Shoesmith was summarily dismissed by the Minister immediately on the publication of the report. Her application was for judicial review of the decision to dismiss her, and the report itself was obviously of critical importance, not least because of the suggestion that the "right" result was needed by Ed Balls in order to justify the dismissal.

After closing speeches but before judgment, Ofsted confessed that it had found nearly 2,000 pages of documents which should have been disclosed. When finally produced, these proved to include 17 earlier drafts of the report. Shoesmith's lawyers made much of the fact that each succeeding draft moved closer to blaming Shoesmith personally for the shortcomings of her department and the death of Baby P. The suggestion of foul play in the conduct of the dismissal procedures was reinforced by the existence of an Ofsted memo ordering staff to delete emails containing the words "Baby P" and "Haringey." That order was apparently rescinded on the day it was given, but it is not known whether anyone had acted on it in the interim and it hardly indicates the right institutional spirit where the duties to the court are concerned.

Whatever effect the disclosure defects have on the finding, the case is important in illustrating the

823 [2009] EWCH 3601 (TCC) (05 November 2009).

824 [2009] EWCH B35 (Admin) (10 November 2009).

reputational disadvantages of improper disclosure, for drawing public attention to the importance of a proper collection appropriate to the circumstances, and, not least, for illuminating the cost implications of a failure to comply with the rules the first time around.

Al-Sweady & Ors, R (on the application of) v. Secretary of State for Defence[825]

This judgment of the Court of Appeal should also bring home to lawyers the downside of getting it wrong. The case involved matters of public interest---the evidential point was as to whether a particular Iraqi died on the battlefield or in British custody--and concerned multiple defects in the disclosure given by the Treasury Solicitor on behalf the Ministry of Defence. These are not set out in what is a short judgment, but the key points for those responsible for disclosure include: the extreme importance of documents in judicial review cases where the respondent almost inevitably holds the documents that matter; the consequences in terms of costs (an interim order for payment of £1 million calculated on an indemnity basis was made); and the reputational issues--the Treasury Solicitor himself was "invited," along with the Provost Marshal of the Royal Military Police, to appear before the court to explain the disclosure defects, and a senior officer was described in terms which are likely to further his career, namely:

> If Colonel Giles continues to be put forward as a principal or even a significant witness in judicial review proceedings or if he is in any way responsible for disclosure, it is our view that any Court seized of those proceedings should approach his evidence with the greatest caution.

The key part of this judgment for the purpose of this paper's themes lies in a passage about a curious volte face made by the Treasury Solicitor. It had been said consistently on behalf of the Department that no further documents existed under a particular head. The judgment describes what happened next:

> Much to our surprise in the light of the Secretary of State's previous stance, it was then asserted for the first time that:- "the sheer volume of the material… together with the technical difficulties in framing meaningful search parameters, means that it would be impractical and disproportionate to conduct broad-based searches of the exchange servers themselves, and that to do so would be disproportionate."
>
> No reason has been put forward to explain why this response had not been made at any time since the original request which had been made more than eight months earlier on 16 October 2008. We conclude that the Secretary of State's agents had simply failed for no good reason during that lengthy period to carry out these critically important

825 [2009] EWCH 2387 (Admin) (02 October 2009).

> and obviously highly relevant searches and this failure in our view constitutes a serious breach of their duty to give proper disclosure.
>
> It must not be forgotten that Salmon J explained in Woods v Martins Bank [1959] 1 QB 55 at page 60 that "it cannot be too clearly understood that solicitors owe a duty to the court, as officers of the court, to go through the documents disclosed by their client to make sure, as far as possible, that no relevant documents have been omitted from their client's [list]". This duty requires a solicitor to take steps to ensure that their client knows what documents have to be disclosed.

If one needed confirmation that a more rigorous approach is needed to the early stages of electronic disclosure, including a questionnaire signed by the solicitor or his client, a case in which a party can veer from claiming that it holds no documents to being apparently overwhelmed by their volume certainly provides it.

West African Gas Pipeline Co. (WAPCo) v. Willbros Global Holdings, Inc. (WHG)[826]

In this international construction contract dispute, the court awarded costs against claimants WAPCo for ESI disclosure failures. Defendants WGH sought over £1.8m in claimed wasted costs incurred due to WAPCo's multiple failures. In assessing WGH's claims, Ramsey J. rejected several categories of costs sought, but found that failures in assembling WAPCo's disclosure, in de-duplication and in review by an outsourced provider in India resulted in wasted costs for WGH in the amount of £135,000 with a further application left open for consideration.

Phaestos Ltd. & Anor v. Ho[827]

Claimants in this matter sought a second extension of time to comply with the court-ordered disclosure timetable. In analyzing claimants' application, Akenhead, J. set out a detailed chronology and noted the situation was largely or wholly of claimants' own making, due to their "lack of urgency" and persistent underestimation of the effort required when it had been apparent from the beginning that the disclosure burden would significant and fall heavily on claimants' side.

As a practical matter, the court "reluctantly" granted an extension, but noted that failure to comply would result in claims and defenses to the Defendants' claims in these proceedings being struck out and the Defendants would be able to enter judgment in the full amount of the Counterclaims. Under these circumstances, costs were ordered on an indemnity (rather than standard) basis.

826 [2012] EWHC 396 (TCC) (27 Feb. 2012).
827 [2012] EWHC 1996 (TCC) (19 July 2012).

Australia

To facilitate the use of information technology in the traditional discovery process, the Federal Court of Australia issued Practice Note 17 in January 2009. The Practice Note, which has since been replaced as Practice Note CM 6, is the preeminent note on e-discovery released by the judiciary in Australia. While not a binding directive, CM 6 highlights several key issues in the application of e-discovery, and codifies the processes that the top-tier firms have been informally following over the last decade.

It is merely a framework of recommendations, and is limited in scope to matters before the Federal Court. It is the first court-wide framework on electronic document management, and has charted the future direction of the courts. Inevitably, all courts in Australia will move towards electronic document management, following the trends in America and the United Kingdom.

The new document-management protocols apply to all paper and electronic documents exchanged between the parties and delivered to the Court. The e-discovery threshold begins when more than five hundred discoverable electronic documents are involved.

The consistent theme throughout the amended Practice Note is a de facto requirement for large organizations to adopt a systemized internal process to address discovery requests. This theme of systemization is centered on three key concepts:

1. Early attention to electronic documents in order to be properly prepared at the Directions Hearing;
2. Accurately and quickly preserving and organizing potentially relevant evidence, including all associated metadata; and
3. Producing documents, when possible, in searchable electronic form.

The Court has released an attachment to CM 6, the Pre-Discovery Conference Checklist. This document outlines the expectations of the Court in regard to the discussion points at the Conference. Some key issues outlined in the checklist include:

1. The scope of discovery strategies for conducting a reasonable search for discoverable documents
2. The management of documents that are privileged
3. The establishment of a Document Management Protocol.

The express purpose of the amended Practice Note is to facilitate the use of technology to increase litigation efficiency. The Federal Court of Australia encourages legal practitioners to use policy, education and technology to ensure they perform document management activities during litigation efficiently and cost-effectively. In fact, the Court requires legal practitioners to be apprised of the basic capabilities of modern technology as it relates to the Practice Note.

CM 6 requires the parties at the Directions Hearing to discuss the proactive document-management policies in effect, the technology implemented, and the training of applicable employees responsible for document-management activities. Implementing a centralized internal e-discovery platform will facilitate this discussion and overall compliance.

Since each party bears the their own cost of compliance with the Practice Note, the Court expects practitioners to exercise diligence to ensure that any document-management activities performed on behalf of a client are conducted with quality, time, and cost-efficiency as priority considerations.

In light of the Practice Note's requirements, organizations would benefit by looking at "dual purpose" technology with additional capabilities (e.g., internal investigations and compliance audits), in order to realize substantial cost savings. Dual or multi-purpose technology would allow the organization to be able to amortize the cost over many different events and departments.

As a final note, we recommend you read a consultation paper released by the Australian Law Reform Commission (ALRC) for the Inquiry into Discovery of Documents in Federal Courts—Discovery in Federal Courts (ALRC CP 2, 2010). This paper provides key insights on Australian e-discovery trends for 2011.

Canada

Canada is a country where different legal cultures and languages coexist across a vast territory. For example, the main language is French in the province of Quebec, and civil law applies to the majority of civil and commercial matters brought before the courts.

Most organizations do business or have offices in Canada's two largest provinces, Ontario and Quebec, and accordingly there will be a need to deal with English and French documents when conducting discovery in Canada. The best approach often consists of utilizing a bilingual expert to strategize about how to identify and preserve relevant information.

Another important issue is the different set of rules in the province of Quebec, including those pertaining to discovery. Motions are generally presented in a common law province when the party seeking information does business in Quebec as well as in another province. Where the organization only does business in Quebec, however, the rules of civil procedure must be dealt with.

International evidence collection in Canada is based on the principle of comity.[828] Comity strikes a balance between different values: cooperation with other sovereign entities and protection of the requested country's citizens.[829] When requesting the assistance of Canadian courts to enforce letters of request, the principal implication is that Canadian courts will actually examine them, i.e., there is no "rubberstamping."[830] However, "comity dictates that a liberal approach should be taken to requests for judicial assistance, so long at least as there is more than ephemeral anchorage in our legislation to support them."[831]

Canada enacted the Personal Information Protection and Electronic Documents Act[832] in 2000. PIPEDA is the federal legislative response to growing concerns over the protection and use of personal

828 "A Primer on International eDiscovery in Canada," by Dominic Jaar, p.2.

829 Id.

830 Id.

831 States of America (District Court) v. Royal American Shows, Inc. ea t., [1982] 1 S.C.R. 414, 421, cited in Pamela D. Pengelley, "A Compelling Situation: Enforcing American Letters Rogatory in Canada," (2006) 85 Canadian Bar Review 345, 347.

832 S.C. 2000, c. 5 (hereinafter "PIPEDA").

information that is accumulated by both public and private organizations in the course of their day-to-day operations. The Act sets out rules governing how such information should be handled by the organizations that collect it, and under what circumstances it may be disclosed, either to third parties or to the individual who is the subject of the information.

See Addendum Article "A Primer on International eDiscovery in Canada" by Dominic Jaar.

See Addendum Article "Is Preservation an Obligation" by Dominic Jaar.

See Addendum Article "The Impact of Canadian Privacy Law on Discovery Procedures", by Dominic Jaar and Patrick Zeller.

US Court Decisions on Cross-Border Discovery

AccessData Corp. v. Alste Tech. GMBH[833]

In this international breach-of-contract action, the plaintiff, a US company, requested a reproduction of previously produced discovery in native format. The defendant, a German company, argued that compliance with the discovery requests would violate the German Data Protection Act (GDPA), subjecting the company to civil and criminal penalties under a German blocking statute. The defendant also claimed that its previous electronic production was in a "readily usable form" and reproduction would be unnecessarily burdensome.

Reviewing the GDPA, the court found nothing that barred discovery of personal information provided customer consent was obtained, and even if disclosure was prohibited under the GDPA, the US Supreme Court has held that blocking statutes do not deprive US courts of the power to compel production from a foreign party subject to its jurisdiction.[834] Addressing the production format dispute, the court determined that scanned PDF images are not readily usable as required by Fed.R.Civ.P. 26(b)(2)(E)(ii) and ordered the defendant to reproduce the requested documents in native form or in an electronically-generated "PDF" format.

In re Air Cargo Shipping Servs.

The plaintiff in this antitrust action moved to compel the defendant French airline to produce non-ESI records. The parties agreed that the records were relevant, that the records were subject to a French blocking statute, and that production would expose the defendant to prosecution in France. However, the records had already been produced to the Department of Justice and used in a criminal prosecution of the defendant. The Court granted the motion, but declined to proceed through the issuance of letters rogatory of the Hague Convention, noting the delay associated with that process.

In a subsequent decision, In re *Air Cargo Shipping Services Antitrust Litig.*,[835] the court addressed another defendant's argument that a South African blocking statute prohibited it from producing information. The court found, among other things, that the information sought was highly relevant,

833 2010 WL 318477 (D.Utah Jan. 21, 2010).

834 See Societe Nationale Industrielle Aerospatiale v. United States District Court, 482 U.S. 522 (1987).

835 2010 WL29876220 (E.D.N.Y. July 23, 2010).

that the discovery requests were specific, and that the United States had a fundamental interest in enforcing its antitrust laws through private litigation. The court dismissed any fear of South African prosecution as speculative because there was no evidence that the statute had ever been enforced and the defendant was itself a South African government agency. Accordingly, the court directed the parties to confer on a production schedule.

Enquip Tech. Group, Inc. v. Tycon Technoglass[836]

In this complex international business litigation, the defendants appealed an order of the trial court that held the European Union Data Protection Directive 95/46/EC ("Directive") did not limit discovery. The defendants argued that the trial court's ruling was a clear error, and that the exception provided in Article 26(1)(d), which permits the transfer of data when necessary to establish, exercise or defend legal claims, was inapplicable.

In response, the plaintiffs claimed that the defendants failed to meet the burden required to obtain a protective order because no effort was made to demonstrate the relevance of the Directive to any of the plaintiffs' specific discovery requests. Agreeing with the plaintiffs, the appellate court affirmed the trial court's ruling. In support of its opinion, the appellate court cited the trial court's reasoning that the defendants subjected themselves to Ohio law by doing business there, and that no reason existed to preclude response to discovery requests under the Ohio Rules of Civil Procedure.

836 2010 WL 53151 (Ohio Ct. of App., 2d Dist. Jan. 8, 2010).

Table of Articles

New electronic discovery rules boot up Friday 265
Legal Issues Raised by the Collection of Electronically Stored Information in Russia and China 267
Data Protection: Duty to disclose 278
Ethical Considerations in eDiscovery 281
Canadian Privacy Law: The Personal Information Protection and Electronic Documents Act (PIPEDA) 286
A Primer on International eDiscovery in Canada 299
Is Preservation an Obligation? 309
e-Discovery and Trade Secrets Law: Limitations on Discovery 312
CISO Profiles rise as their reach extends into Legal 320
Computer Forensics v. E-Discovery 322
Bringing Legal and IT Together at Nationwide Insurance 327
The Risks and Costs of Custodian Self-Collection 329
Planning and Paying for eDiscovery - and Responding to It 330
Privilege and Spoilation in the Courts 332
Edmund Sautter 334
Standoff Between EU Data Protection and U.S. eDiscovery Requires Difficult Compromises for Both Sides 335
EU Data Protection Versus U.S. eDiscovery 337
Judge Simon Brown Discusses Growing Impact of Electronic Disclosure in the U.K. 340
Judge Scheindlin States Litigants, Including the Government, Must Demonstrate Ability to Search and Assess ESI 342
The E-Discovery Toolbox: What You Should Look for in a Unified E-Discovery Solution 344
At Liberty Mutual, E-Discovery is a Team Effort 347
Master European Data Privacy Laws 349
Reduce Your Risk of E-Discovery Sanctions by 80 Percent 351
Victor Stanley II: New Landmark E-Discovery Sanction Decision 353
Voice of the Corporation: The 30(b)(6) Witness 355
Recent eDiscovery Developments in Australia and the U.K. 359
Legal Must Stay Actively Involved in Selecting eDiscovery Solutions 361
Seyfarth Shaw's Scott Carlson Provides Insight into How Clients are Handling eDiscovery 362
Understanding Legal Hold Technology; Email Archiving for eDiscovery? 364
Recent Court Ruling Underscores Importance of File Metadata Preservation 366
Bringing eDiscovery Processing In-House 367
The Keyword vs. Concept Search Debate 370
New Decision Holds Attorneys to Reasonable Inquires 371
Verizon Continues Its Goal of Using Technology to Become Self-Reliant in the eDiscovery Process 373
Selecting the Right eDiscovery Solution; Preserve in Place vs. Collect to Preserve 375
eDiscovery Spoliation Sanction Milestone: Monetary Sanction Imposed on an In-House Counsel 377
eDiscovery and the Cloud; Judges Pushing Companies to Insource eDiscovery? 378
Protecting Privilege with FRE 502 380
It's Time to Bridge the Gap Between eDiscovery, Internal Investigations, Audit and Compliance 383
Judge Andrew Peck on Keywords, Cooperation, Privacy and What Sherlock Holmes Teaches About eDiscovery 385

Best Practices for Public Sector eDiscovery Collection 387
UK e-Disclosure Turning Point: The Corporate Focus on Cost-Effective Collection and Processing of E-Mail and Electronic Documents for Litigation and Regulatory Purposes 397
What's New in EnCase eDiscovery Version 5.....414
The Place for EnCase® eDiscovery in Electronic Disclosure for Major Corporations in UK Courts 417
Obtaining German Works Council Approval to Collect Employee E-mail and Electronic Documents 438
Using EnCase® Enterprise Solutions to Enhance Data Protection Compliance in Corporate Investigations..... 446
Seeking a Balance in the Discovery Equation: Pre-trial Disclosure/Discovery in UK and US Civil Litigation of European-Based Data..... 459
eDisclosure after Jackson: Developements in electronic Disclosure in England & Wales (with an Update on US eDiscovery law) 472

Articles

New electronic discovery rules boot up Friday

by Steve Lash

Copyright November 30, 2006 by Chicago Daily Law Bulletin. Reprinted with permission.

WASHINGTON — Pretrial discovery officially enters the digital age Friday as new Federal Rules of Civil Procedure provisionsgo into effect detailing the obligations and protections for litigants whose computer-generated documents are soughtby their opposing parties.

Chief among these obligations is the duty to disclose the existence of saved computer files that are responsive to the opposing side's document request but would be extremely burdensome or expensive to retrieve Top among the protections is the ability of a litigant to retrieve from the other side a privileged computer document that was inadvertently sent in response to a discovery request.

The new "electronic discovery" provisions of the federal rules also generally protect litigants from sanctions for failing to comply with discovery requests if their computer programs routinely delete the types of information subsequently sought by the opposing party. For example, a litigant would not be punished for not having provided e-mail communications if the documents had been deleted from a computer that routinely purges e-mails after a certain number of days.

Chicago attorney Paul E. Freehling, a veteran federal court litigator, predicted Thursday that the e-discovery provisions will not increase litigation costs. But the new rules will be a wakeup call for lawyers who have not entered the computer age with regard to discovery requests.

"Every litigation lawyer must read and understand these rules," said Freehling, a partner at Seyfarth Shaw LLP. The rules "certainly brought the subject [of e-discovery] to the top of the pile."

The federal judiciary adopted the new rules, with Congress' silent acceptance, in recognition that gone are the days when companies warehoused the thousands of pages of internal memos, reports and financial records that traditionally form the basis for litigation and pre-trial discovery. This information now is routinely stored in personal computers that can hold 60 gigabytes of data, or 60 stacks of paper 85 feet tall, said the Administrative Office of the U.S. Courts, the judiciary's datacollection arm, in announcing the new provisions.

Computer networks at large corporations can hold the equivalent of 500 million typewritten pages, the administrative office said. While storing the mountain of data has become easier for companies, the ability of their lawyers to sort through the computer programs to respond to discovery requests has ironically become more difficult, time consuming and expensive, the office added.

The coming of the new federal rules has accelerated the trend of corporate law departments teaming up with the companies' information technology personnel to decide where data are stored on computer networks and how the data can be retrieved in the event of a discovery request, industry

observers say. The pending e-discovery rules have spurred a high tech industry of companies that provide computer software to help corporate law departments and outside counsel respond to discovery requests in this digital age.

Pasadena, Calif.-based Guidance Software Inc., for example, markets its EnCase Enterprise eDiscovery Suite software to corporate legal departments.

The new e-discovery rules have helped make sales of the software brisk and the marketing department's job easier, said Patrick Burke, assistant general counsel for Guidance Software. "They [legal departments] are reaching out to us," he said.

In light of the new e-discovery rules, Corporate general counsels know they must have a "defensible process" for compiling electronic information, Burke said. EnCode provides such a process by enabling the attorneys to find via keyword searches information stored on company computers, he added.

Burke did not disclose the cost of the software but said it is priced at standard rates depending on the company's size.

Chicago-based Impact Forensics, a computer consulting firm, has recently augmented its electronic-discovery services amid increased demand from law firms for high-tech assistance, the company stated in a recent news release. The expansion includes "a new forensics lab with significant investments in new electronic discovery technologies," company president Jeffrey Hartman said in the release. Hartman did not respond to a telephone message Thursday seeking additional comment.

The new federal rules, recognizing that the cost of upgrading computer equipment is expensive, permits attorneys to decline a request for the electronic documents if they can show that the cost and expense of retrieving and sending them electronically is prohibitive. The burden would then shift to the requesting party to prove to a judge that the documents are essential to its case.

The rules, noting that an electronic transmission of a massive amount of documents might inadvertently contain privileged material, generally allow attorneys to retrieve the privileged information from the requesting party.

While the new rules will bring uniformity to electronic discovery in federal courts, states remain a patchwork of 50 separate civil-procedure standards. However, the Conference of [state] Chief Justices in August approved model guidelines for states to adopt in an effort to achieve national uniformity.

The state model is similar to the new federal rules. For example, privileged documents inadvertently sent electronically to the opposing side would generally be required to be returned and not used at trial.

"Inadvertent disclosure of privileged information is sometimes unavoidable because of the large amounts of information that are often involved in electronic discovery, and the time and cost required to screen this voluminous material for attorney work product and other privileged materials," states an explanatory comment accompanying the guidelines. As a result, attorneys in most cases should not be penalized for these inadvertent transmissions and the material should be returned, the comment adds.

The Judicial Conference of the United States, the federal judiciary's policy making body, earlier this year recommended the new Federal Rules of Civil Procedure provisions, which the Supreme Court then approved. Congress did not vote to change or reject the new provisions, clearing the way for them to go into effect on Friday.

Legal Issues Raised by the Collection of Electronically Stored Information in Russia and China

by Patrick E. Zeller[837]
Vice President and Deputy General Counsel, Guidance Software, USA
&
Patrick Burke
Senior Director and Assistant General Counsel, Guidance Software, USA
Copyright Vol. 3, No. 12, Summer 2010, 1, by International In-house Counsel Journal. Reprinted with permission.

Collections of electronically stored information ("ESI") around the world often implicate local law including restrictions protecting the privacy rights of the individuals from whom data is collected. Collections of ESI in Russia and the People's Republic of China ("PRC") present legal issues not faced in other jurisdictions. This article describes some of the legal and procedural challenges faced when collecting ESI in Russia and the PRC for delivery outside those two countries.

Privacy Concerns for Collections in Russia

The primary legal obligations in Russia are with regard to employee privacy protections and related obligations to give notice to, and register with, government agencies when collecting personal data.

While Russia has certain protections for individuals' privacy, the law in this area – and its enforcement – are not as well developed as in the European Union, and allow for some latitude in data collection and export from Russia. Russian law assigns individuals a right to privacy as to certain personal information. The Constitution of the Russian Federation recognizes rights of privacy, data protection and secrecy of communications. Article 23 provides that everyone shall have the right to privacy, personal and family secrets and to protection of one's honor and good name. Constitution of the Russian Federation, 1993, Art. 23. Constitution of the Russian Federation, 1993, Art. 23. Everyone shall have the right to privacy of correspondence, telephone communications, mail, cables and other communications. *Id.* Any restriction of this right shall be allowed only under a court order of a court of law. *Id.* Russia is a member of the Council of Europe (CoE) and has signed and ratified the CoE Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108), ratified Dec. 19, 2005.

On January 26, 2007, the Federal Law "On Personal Data", No. 152-FZ, became effective in Russia. This law applies in all cases when (1) personal data (2) is processed (3) by operators of personal data. Personal data for individuals has a broad definition but focuses on such specific types of data as income, education and home addresses. Personal data is broadly defined to include "any information related to an individual…or information on the basis of which an individual may be identified." Examples include surname, birthdate, address, family status, income and education. Oleg Shuminov and Julia

837 Patrick E Zeller is a Vice President and Deputy General Counsel, and Patrick Burke is a Senior Director and Assistant General Counsel, at Guidance Software's Chicago and New York offices, respectively. For further information, Zeller can be reached at patrick.zeller@guidancesoftware.com, Burke at r patrick.burke@guidancesoftware.com. This article does not replace legal advice; it is strongly advised to check with local counsel before undertaking collections in Russia or the PRC.

Borozdna, *Data Protection: Russian's Law on Personal Data,* 5 PVLR 1679 (Dec. 4, 2006). Those who collect, process and transfer such information – referred to under Russian law as "processing operators" -- must protect the confidentiality of personal data unless it was sanitized or publicly available. Federal Law No. 152-FZ, Art. 7. Processing is defined as "operations with personal data, including collection, systematization, accumulation, storage, verification (renewal, modification), use, dissemination (including transfer), defacing, blockage, destruction." An "operator" is defined under this law as a 'legal entity, natural person or state (municipal) body engaged in processing personal data.' Id. at Article 3.

Until a case-specific legal analysis is conducted by your local counsel to determine whether an assignment calls upon you to act as an operator, it is a best practice to proceed under the assumption that you are acting as an operator, and take appropriate precautions.

A data protection violator may be subject to disciplinary, civil, administrative or criminal liability. In particular, the Criminal Code of the Russian Federation provides a penalty for violation of the immunity of private life, violation of secrecy of communications and infringement of home inviolability, as well as liability for unauthorized access to legally protected computer information. The Administrative Code of the Russian Federation also establishes liability for disclosure of information if access to it is restricted by federal laws. According to the Civil Code of the Russian Federation, if an individual suffers physical or moral damages by violation of his or her non-property rights or any other non-material welfare rights, as well as in other cases provided by the law, a court can force the person invading privacy to provide financial compensation.

Further case-specific legal and factual inquiry would be required to determine whether – in any particular case and under Russian law – you may be acting as "operators", and if the ESI being collected may qualify as "personal data". Until the determination is made that ESI collected does not contain personal data, it is a best practice to proceed as though personal data is involved.

Consent of the Individual May Be Required Under Russian Law for Personal Information to be Collected, Processed or Transferred

If personal data is involved the law may require that the employee consent to the collection, processing and transfer of his or her ESI. Consent is required when "directly provided by law" in situations such as the transborder transfer of personal data and processing of special categories of personal data relating to such issues as health or nationality. Federal Law on Personal Data, No. 152-FZ, Articles 10 and 12 (2006). Although there are exceptions (discussed *infra*) to consent, based on several interpretations of this law, it is fair to say that business emails should be considered as a source of personal information as defined in this law. Personal data is related to the confidential information, therefore, a person's consent is necessary in order to disclose such person's personal data to third parties. It appears that if personal data is excluded from e-mails, and the remaining information is not related to any type of confidential information as defined in the applicable laws, there should be no special limitations. However, since the author-employees would be identified with e-mail contents, it is prudent to obtain consent from the company.

If the employer has notified its employees by policy or specific notice that their e-mail and documents are company property and can be accessed for business uses at any time, written consent can be made by the customer/company to our client. Written consent is prudent because in any dispute on this issue, the burden of proof to prove consent will be on the operator and Russian courts usually require documentation as evidence. Federal Law on Personal Data, No. 152-FZ, Article 9, Point 3 (2006).

Although the law does not provide a standard consent form, it lists six criteria which should be included in any written consent to processing personal data:

1. full name of individual giving consent with address, passport number, date of issue and issuing authority;
2. name and address of operator(s) to whom consent is given;
3. objective of personal data processing;
4. list of personal data that may be processed by operator;
5. list of operations to be performed with personal data, and general description of the personal data processing methods used by the operator; and
6. term of validity of the consent and the procedure for its revocation.

Fed. Law No. 152-FZ, Art. 22, Clause 3 (2006).

There are also some broad exceptions to the consent requirement which include:

1. personal data processed on the basis of federal law primarily aimed at supporting law enforcement activities;
2. personal data processed to perform an agreement to which such individual is a party. An example is if an employer needs the employee‘s personal data to perform the employment agreement like for travel arrangements for insurance purposes;
3. personal data processed for scientific or statistical purposes, and its sanitized;
4. personal data processes to protect life, health or important individual interests and it‘s not possible to obtain consent;
5. personal data processed to deliver mail or telecommunications customer settlements;
6. processed for professional activity of a journalist or for scientific, literature or other creative activity;
7. data subject to publication in compliance with federal laws such as state officials or candidates to elective state posts.

As a best practice, it should be assumed that *none* of these exceptions will be available to ESI collected. In most cases that will be the case.

Cross-Border Transfer of Data Collected in Russia

At this time, there does not appear to be any legal barrier to taking business data out of Russia -- as long as it does not contain "personal data" or implicate Russian Secrecy statutes. In terms of transferring collected ESI, Article 15 (5) of the Federal law "On Information" also provides that data can be transferred through data telecommunications networks without any limitations subject to the requirements to data distribution and protection of intellectual property established by Federal laws. Limitations of data transfer can be set only by special federal laws. The federal laws which impose data disclosure limitations are the Federal law "On state secret" No.5485-1 dated July 21, 1993; the Federal law "On commercial secret" No.98-FZ dated July 29, 2004 and the Federal law "On personal data" No.152-FZ dated July 27, 2006. According to Article 7 of the Federal law "On personal data" the operator should ensure for the confidentiality of received personal data with two exceptions: (i) in instances involving depersonalization of personal data and (ii) to publicly available personal data. Most importantly, the operator can process personal data only with a person's consent (Article 6), subject to certain exceptions. Thus, one must be prepared to "ensure for the confidentiality of received personal data" unless it can "depersonalize" the data or show it is "publically available" (likely impractical). It is unclear what "depersonalization" of data is permissible.

The federal law "On personal data" provides for the operator's obligation to make sure that a foreign state – recipient provides for an adequate protection of a person's personal data. The cross-border transfer of personal data may be prohibited or limited to protect constitutional order of the Russian Federation, morality, health, rights and legal interests of citizens, provision of national defense and state security. If the operator obtains a person's written consent, the cross-border transfer of the personal data may in some instances be permitted even if a foreign state - recipient does not arrange for an adequate protection of a person's personal data. Law No. 152-FZ, Article 12.

Registration and Notice Requirements for Collection of ESI in Russia

If "personal data" is collected from employees, then those collecting the ESI have an obligation to register with the Rosokhrankultura, the Russian Federal Service for Oversight of Mass Media, Communications and Protection of Cultural Heritage, obtaining consent in advance of any data processing project (including certain criteria in that consent), and in some situations providing notice to the individual "owner" of any "personal information". Federal Law No. 152-FZ, Article 22, Clauses 1 and 3, and Article 14, Clause 4. So, it an initial determination must be made whether the anticipated data collection activities would require registration.

The Federal Law requires data operators who actively collect and use "personal information" to notify the "regulator" before they start actual data. Federal Law No. 152-FZ, Art. 22, Clause 1. The regulatory Agency is the Rosokhrankultura, the Russian Federal Service for Oversight of Mass Media, Communications and Protection of Cultural Heritage. In particular, one of its functions is to exercise control over compliance of personal data processing with requirements of Russian legislation.

Pursuant to the Order of the President of the Russian Federation No.724 dated May 12, 2008, the

Federal Service for Supervision in the Sphere of Mass Communication, Communications and the Protection of Cultural Heritage was divided into two separate Federal services: (i) Federal Service for Supervision in the Sphere of Communications and Mass Communications ("Rossvyazkomnadzor") and (ii) Federal Service for the Monitoring of Compliance With Legislation in the Area of the Protection of Cultural Heritage ("Rosokhrankultury"). The official web-site of Rossvyazkomnadzor is www.rsoc.ru.

By August 2008 this Agency had registered more than 14,000 personal data operators. Sergei Blagov, *Russia Moves to Register Companies, Agencies that Collect, Use Personal Data,* 7 PVLR 1274 (Sept. 1, 2008). Vendors or their agents may wish to consider registering if there is any question that the e-mail and data filtering may not sufficiently cull out personal information as it is so broadly defined under Russian law. At the very least it is recommended that filtering steps be run on the collected data to filter out employee personal information and avoid regulatory confusion.

If the processing operation is collecting any "personal data" during the project which is not able to be filtered out, an operator should provide the individual, upon his or her request, with information about the term of processing their personal data and term of storage of that data. However, in some cases it is possible that obtaining a written company consent could override the need for such notice particularly because business e-mail and data may be defined to fall outside the statutory definition of "personal data." Again, it is a best practice to assume that employee consents will be required, until your local legal counsel has determined otherwise.

Collecting ESI in China

The People's Republic of China recognizes two legal systems co-existing inside its borders - the PRC legal system and the Hong Kong legal system that existed prior to the transfer of sovereignty from the United Kingdom to the PRC in 1997. Since that time, Hong Kong has acted as a Special Administrative Region of the PRC with its legal system separate and intact from the PRC system. Under both the PRC and Hong Kong systems of law, individual privacy rights are not given much protection and neither jurisdiction has yet enacted any laws that specifically regulate electronic discovery practices there. However, there are import requirements for technology that includes encryption software so depending on whether technology will be imported into China to accomplish the collection, processing and transfer of ESI, and whether or not it was previously licensed/approved, some import requirements may need to be addressed. It is recommended as a prudent practice that one obtain written consent and authorization from the company managers to collect and transport business data from both the PRC as well as Hong Kong.

Applicable People's Republic of China Law

There is no clear prohibition in Chinese privacy law on access to the data of employees of the Chinese company or a non-Chinese subsidiary, assuming that the employees have not been notified previously that the employer may access their computer or that the computer belongs to the company.

China lacks comprehensive privacy legislation, although it has some basic principles set forth in

the General Principles of Civil Law. This may change in the future because in 2005 a draft of Personal Data Protection Law was submitted to the State Council, China's executive branch for approval. For this reason, you should check with legal counsel on the status of this new law before undertaking a collection in the PRC.

Although regulations on computer systems contain prohibitions of the infringement of privacy, the principle is not detailed in those regulations or elsewhere. It is not unusual for searches to be undertaken on company computers without an employee's consent. Chinese labor arbitration tribunals have relied on such evidence in their decisions, which is an indication of the state of practice rather than law, because such decisions lack precedential value.

Consent Issue

While Chinese law does not appear at this time to regulate business data collection practices (although it is regulated in Hong Kong, see below), it is recommended that you obtain written consent from the company in advance of collection to minimize any exposure to liability, and avoid any potential legal ambiguities.

Technology Importing into China

Laws which relate to import and export are implicated if the client technology incorporates an encryption product, which is defined as "products for which the information is subject to protection or security authentication on the basis of encryption technologies, including encryption products made within and outside of China." Article 3, Measures for the Use of Encryption Products by Overseas Organizations and Individuals within China, March, 2007, State Encryption Management Bureau (a bureau under the State Security Ministry). Whenever a foreign organization or individual intends to use an encryption product within China, such person or entity is required to obtain a license for the import of such technology. Id. at Article 5. There are penalties for failure to comply with the licensing requirements.

In the last several years, the Chinese government has issued several regulations related to the import, use and sale of encryption products in China. This could affect anyone using such technology regardless of the way that search and collection products are taken into China. If the e-Discovery collection or processing software uses encryption you may have to disclose the nature of the product in the Customs declaration documents because earlier this year, a partial list of tariff classifications for encryption products was issued. As a consequence, importers and exporters of the products in question must use those tariff numbers in the Customs declaration forms, which means that Customs will require that the necessary license be presented. It has been reported that the Chinese authorities are likely to issue a comprehensive list of encryption products with PRC tariff numbers in the near future.

If your team takes a search and collection software that uses encryption into or out of China in their luggage, as a practical matter the Customs authorities at busy airports such as Beijing and

Shanghai are unlikely to question the item and stop its import or export. Additionally, the use of such software may also go unnoticed in a city such as Shanghai or Beijing, where thousands of companies are transmitting data abroad. The encrypted data transmission would be more noticeable if the Chinese subsidiary is located in a remote area with few other companies transmitting data abroad. Be aware that the Chinese authorities are authorized to monitor data transmissions abroad and are increasing their technical capabilities in this area.

Cross-Border Transfer of Collected Data

Although China has state secrecy legislation that would prevent state secrets from being exported from China, regardless of the form of transmission (by hand, mail, or data transmission), it is unlikely that such legislation would be applicable. The State Secrecy Law defines state secrets as "matters that have a vital bearing on state security and national interests and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time," Article 2, Law on Guarding State Secrets, September 5, 1998, and include a list of seven items such as: major state policy decisions, secrets related to national defense and the armed forces, and diplomatic activities. If the data in the network in question appear to be ordinary commercial data, it likely would not be classified as "state secrets" although that analysis needs to be undertaken for particular cases.

If your organization brings someone to China to perform the collection for a period of less than three months, that person would only need a valid business visa to perform the work. The visa requirements are set forth on the website of the PRC Embassy to the United States.

Applicable Hong Kong Law

In Hong Kong, the main sources of protection in relation to an individual's right of privacy over personal data are based on two legal sources: (1) the Personal Data (Privacy) Ordinance ("the Ordinance"); and (2) at common law. Section 4 of the Ordinance headed "Data protection principles" provides that a data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under the Ordinance. For these purposes:

- "personal data" is defined as any data (a) relating directly or indirectly to a living individual, (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and (c) in a form in which access to or processing or use of the data is practicable; and
- "data user" means a person who, either alone or jointly in common with other persons, controls the collection, holding, processing or use of that data.

According to Data Protection Principle 3 of the Ordinance, the use of personal data (which would include the transfer of such data) must be consistent with the purpose for which the data

were originally collected or directly related to it, otherwise the prior consent of the data subject, the employee, must be sought and obtained.

Data that relates to a living individual and from which it is possible to ascertain his or her identity is "personal data" for the purposes of the Ordinance. For example, information relating to an employee's salary or commencement and resignation dates would not, in and of themselves, fall within the definition of "personal data" under the Ordinance. However, if the names of the relevant employees are included with this information, the information would constitute personal data. Likewise, information in HR files, if they contain the names, addresses, identity numbers or other personal details, would likely be classified as personal data. Subject to certain limited exceptions, such information cannot be disclosed to a third party without the employee's consent. In sum, it is a best practice to proceed as though information collected would include personal data requiring consents.

Consent Required Only for Personal Data Collection in Hong Kong

Pursuant to the Code of Practice on Human Resource Management, issued by the Office of the Privacy Commissioner for Personal Data, where information constitutes employee-related data covered by the Ordinance, an employer should not use or disclose such data of an employee for any purpose other than the purpose directly related to the employment of the employee unless:

- the employee has consented to such other use or disclosure;
- the purpose is directly related to the purpose for which the data were collected;
- such use or disclosure is required by law or by statutory authorities; or
- there is an applicable exemption provided for under the Ordinance.

There is a section of the Ordinance, section 33, which prohibits the transfer of personal data to places outside Hong Kong except in some limited situations. However, while enacted, it is not yet in force so does not govern or apply to transferring personal data currently. It is recommended that you check with your local counsel to determine the updated status of this prohibition.

Nonetheless, it may be reasonable to conclude that as long as the employer put their employees on notice that any business email communications and documents are accessible and collectible as business data, this constitutes contractual consent and is an exception to the statutory definition of personal data. Such a conclusion should be made together with your local counsel.

This Ordinance was specifically enacted to protect the privacy of individuals in relation to personal data, but further protection is afforded at common law under broader doctrines such as the duty of confidentiality. The duty of confidentiality provides that any information given or received in confidence or for one (specific) purpose should not be used for another purpose or passed to a third party without the consent of the owner of or person imparting the confidential information. A third party which receives confidential information is liable to be restrained from disclosing or using information which he or she knows, or ought to know, is confidential. While the scope of protection may be broad, the relationship of confidentiality may be difficult to establish outside the

traditional professional and client relationship. The protection only applies to information which has the necessary quality of confidence, which has been imparted in confidence, and which has been used without authorization to the detriment of the party communicating it. *(Coco v AN Clark (Engineers) Ltd* [1969] RPC 41). An aggrieved party may apply to the Court for injunctive relief and, where appropriate, seek damages if an unlawful disclosure has been made.

It may be reasonable to conclude that at common law, all data and email generated by employees is business not personal data, and that the owner of all such data is the business, not individual employees. So as long as the company provides consent for any business data collection, it may meet the statutory requirements. Again, it is a best practice to assume that employee consent is required until your local counsel makes a different determination.

Cross-Border Transfer of Collected Data from Hong Kong

Hong Kong does not have any generic "blocking legislation" preventing the transmission of information abroad. However, there are two Hong Kong laws that make specific reference to national security and defense as grounds for prohibiting the transmission of certain information and other forms of exchange. These are the Official Secrets Ordinance, and the Trading with the Enemy Ordinance.

The Official Secrets Ordinance was enacted to prevent the unauthorized disclosure of official information. The phrase "official information" is construed widely and would cover information from public servants, government contractors, members of the security and intelligences services and any persons who receive such information in confidence. The type of information covered includes security and intelligence information, defense information, information relating to international relations and information relating to the commission of offences and criminal investigations. The unauthorized disclosure of official secrets may result in criminal sanctions.

The Trading with the Enemy Ordinance applies when the Hong Kong Chief Executive makes an order that a particular State is an enemy, defined as any State, or Sovereign of any State at war with the People's Republic of China. Upon such an order being made, most forms of exchange with the enemy State would be prohibited.

In addition to the above, the Protection of Trading Interests Ordinance ("PTIO") may be relevant. Section 4 of the PTIO concerns documents and information required by overseas courts and authorities. Under this provision, the Hong Kong Chief Executive has the power to order a person in Hong Kong not to comply with the requirement of an overseas court and authority if it appears that doing so would infringe the jurisdiction of Hong Kong or is made otherwise than for the purposes of civil or criminal proceedings.

Provided that the information being collected does not contravene any of the abovementioned ordinances, there should be nothing improper or unlawful if that information was then taken out of Hong Kong.

Bringing Special Technology to Perform Collection into Hong Kong

To the extent that search and collection technology utilizing encryption capability is brought into Hong Kong, this may implicate certain regulations if it encrypts data before it is transferred outside Hong Kong. One should determine whether the software and any related hardware have an ECCN number. If it does, it is likely that an import license may need to be obtained in Hong Kong. An import license is not required for Hong Kong if the device is not a controlled product. However, where the device has been "modified" such that it contains encryption software then it is likely to be classified as a controlled product and would require an import license in Hong Kong.

There is no control over encryption software that is subsequently remotely downloaded over the Internet, and not actually physically imported into Hong Kong (since the control relates only to products that are physically imported or exported). However, if the device with the encryption software is subsequently exported from Hong Kong, it would be considered to be a controlled product and an export license would be required at the time.

If you bring a team into Hong Kong to conduct the collection, It is possible that work visas may be required. There are also potential taxation issues as Hong Kong's tax system works on the basis of where the particular income is derived. To the extent that work is being conducted in Hong Kong, from which income is derived, it may be subject to taxation.

Conclusion

In overall terms, in order to generally reduce liability for collections in either Russia or the PRC (including Hong Kong), the following measures are recommended:

1. obtain written authorization from the Russian corporate entity for collection of its employee's ESI;
2. obtain executed consents from the individual employees to access their data and transfer it outside the employees' country, and the consent should overtly acknowledge that it may be turned over to third parties for litigation or regulatory purposes;
3. review the employee policies of the Russian or Chinese employer to ensure that employees are made aware that e-mail and work product can be accessed and collected, or if no policy exists, then notice is given prior to the collection;
4. ensure any technology or hardware imported into each country meets Russian or Chinese import standards, which may require a license if it has not been previously imported/approved for use; and
5. in Russia, the entity performing the collection, processing or transfer of the ESI out of Russia may need to register with the appropriate authority as a "processing operator" if there is any question that the ESI collected might include "personal data" as broadly defined there. It may be possible to conduct filtering of the data to screen out anything that would be considered "personal data" under Russian law so this registration requirement would become moot.

Given the political systems and Communist heritage in Russia and China, lawyers supervising the collection of ESI in these two countries would be well advised to engage local counsel and pay particular attention to local legal requirements.

Patrick Zeller is Vice President and Deputy General Counsel for Guidance Software Inc. where he performs in-house legal functions, supervises the legal and regulatory team, and works with corporate law departments of other companies seeking to implement defensible in-house eDiscovery processes in the US, Canada, UK, and Europe. He writes and speaks regularly on topics related to eDiscovery and digital evidence and the intersection between law and technology.

Prior to joining Guidance Software, Patrick practiced litigation at Seyfarth Shaw LLP where he co-chaired the firm's Electronic Discovery Practice Group. He practiced commercial litigation, with a strong emphasis on technology issues and electronic discovery.

Patrick has lectured extensively on Internet and high-tech crime at numerous law enforcement training venues nationwide, including the FBI Academy. He is widely regarded as one of the leading minds in technology and the law; his specialties include eDiscovery, internal investigations, computer intrusion, economic espionage, online fraud, intellectual property and trade secret issues.

Patrick is an Adjunct Professor and Distinguished Lecturer at The John Marshall Law School's Information Technology and Privacy Law LLM program, where he teaches the "eDiscovery, Computer Evidence and Computer Forensics" class. He also holds several certifications in computer forensics, is a member of the Sedona Conference and Chairs the Board of Directors for the American Association of Digital Forensics and eDiscovery (ASDFED).

Patrick Burke is Senior Director and Assistant General Counsel for Guidance Software, Inc. where he performs in-house legal functions and works with corporate law departments of other companies in the U.S. and Europe implementing defensible in-house eDiscovery processes. He serves on the Sedona Conference Working Groups 1 and 6.

Prior to joining Guidance, Patrick was a U.S. Associate in the commercial litigation department of Linklaters, the London-based Magic Circle law firm, where in addition to litigating cases he co-headed Linklater's firm-wide eDiscovery working group. Previously he was a litigation associate at Paul, Weiss, Rifkind, Wharton & Garrison and Seward & Kissel. He attended N.Y.U. School of Law and served as a Law Clerk to U.S. District Court Judge Glenn E. Mencer (W.D. Pa.).

Patrick speaks regularly at legal conferences on topics including eDiscovery law and best practices, privacy, European data protection, digital evidence and cybersecurity. He is regularly invited to organize and moderate panels of judges on both sides of the Atlantic, including conferences in New York, London, Brussels, Munich, Philadelphia, Las Vegas, Warsaw, Washington DC and elsewhere.

Guidance Software is recognized globally as the world leader in eDiscovery and other digital investigations.

Our EnCase® software solutions provide the foundation for corporate government and law enforcement organizations to conduct thorough and effective computer investigations of any kind, including intellectual property theft, incident response, compliance auditing and responding to eDiscovery requests—all while maintaining the forensic integrity of the data.

We also offer customized services in eDiscovery, incident response, computer forensics, evidence presentation and trial testimony, utilizing a team of former law enforcement professionals, eDiscovery and litigation support experts, information assurance specialists and project managers who have front-line, hands-on experience in all areas of digital investigations.

Guidance Software trains over 6,000 corporate, law enforcement and government professionals annually in the areas of computer forensics, enterprise forensics, eDiscovery, and computer incident response. Courses and materials are offered in a variety of languages in Guidance Software facilities worldwide, through partners and online.

Our customers are corporations and government agencies in a wide variety of industries, such as financial and insurance, technology, defense, energy, pharmaceutical, manufacturing and retail. More than 100 of the Fortune 500 and over half of the Fortune 50 use EnCase solutions, including: Allstate, Chevron, Ford, General Electric, Honeywell, Northrop Grumman, Pfizer, UnitedHealth Group and Viacom.

Guidance Software is recognized by industry analysts such as Gartner, Forrester and IDC as a worldwide leader in digital investigations.

Data Protection: Duty to disclose

by Patrick Burke

Copyright 07 July 2010 by legalweek.com. Reprinted with permission.

Patrick Burke looks at best practices for multinational companies when faced with contrasting privacy laws over electronically-stored data

Multinational companies with UK and US facilities find themselves in what is often a no-win situation when it comes to e-disclosure. On one hand, they are legally obligated to respond to discovery requests in cases before US courts that require the collection, review and production of electronically stored information (ESI) - email and other electronic documents - stored on the computers of their UK employees. On the other hand, they are faced with the fact that UK data protection laws disfavour the collection and transfer of ESI due to stringent protections of employee privacy.

US court rules require litigants to produce to their adversaries any documents, including all ESI relevant to subject matter of the action (or those requested that may be reasonably calculated to lead to the discovery of admissible evidence), in their possession, custody or control anywhere in the world. This can be a vast amount of ESI, significantly broader than the quantities typically collected and produced in UK disclosure.

The broad US e-disclosure requirements raise data protection issues that are a challenge to navigate but, as discussed below, there are suggested best practices and technologies for building processes best able to reduce the legal risks.

UK protections for personal data

The crux of the dilemma is the concept of 'personal data'. In the UK, personal data includes any email or electronic document that includes an employee's email address, name or other identifying information that can possibly be tied to that employee. In most cases, it must be assumed that data collected from employees' laptops, workstations or shared drives will fall within the definition of personal data.

This is why corporate counsel at multinational companies charged with meeting US e-disclosure obligations requiring ESI from the UK are expanding their understanding of the substantive UK privacy laws - beginning with the UK Data Protection Act 1998. Unfortunately, published decisions and regulatory guidance are scarce in this area. Data protection authorities have been unwilling to commit themselves in writing to clear statements of the restrictions applicable to e-disclosure, leaving multinationals vulnerable whenever ESI is collected in the UK and transferred to the US.

British data protection authorities have issued guidance documents, however, that allow for a balance between the legitimate business needs of the company and the privacy rights of employees. In June 2005 the Information Commissioner's Office issued the Employment Practices Code that includes a chapter on disclosure requests. This chapter provides some practical guidance, including that employees from whom ESI is collected should be so notified, and that the company should collect, transfer and produce no more of the employees' ESI than obliged.

Transferring ESI to the US

Even where ESI collection can be accomplished lawfully, the transfer of electronic data to the US from the UK faces restrictions. Lawyers most knowledgeable on the issue advise that, when possible, companies obtain written consent from employees from whom data is to be collected. Keep in mind, however, that the UK Information Commissioner's Office warns that a particular consent may not be adequate to overcome restrictions, especially if the employee might have had no real choice about providing it, and even a valid consent may be withdrawn in some circumstances. They therefore advise that organisations should not rely exclusively on consent to legitimise transfers. In their view, it is better to concentrate on ensuring that the company treats individuals fairly rather than on obtaining consent in isolation. The UK Information Commissioner's Office provides detailed guidance on international transfers of personal data.

Transfers of personal data from the UK to the US also can lawfully be accomplished through compliance with the US Department of Commerce's Safe Harbor programme, which the UK Information Commissioner's Officer considers to provide adequate protection. This may not, however, provide compliance if the ESI is then turned over to a third party in the course of the US litigation.

Tailoring technology to enhance data protection compliance

Data protection practitioners advise that companies' ESI collection protocols be customised in the UK to better respect the privacy rights of employees. Over the last several years, technology has been developed that allows companies to perform surgically targeted collections - collecting only those emails and electronic documents that meet relevant search criteria. Thus, non-relevant personal data is left uncollected. This technology not only enables companies to better respect the rights of employees, but enhances compliance with the requirement of the Employment Practices Code that only that ESI which the company is obliged to produce is even collected in the first place. This same technology also permits companies to utilise an audit capability that provides transparency as to ESI collected and verification that the company is not overstepping legal limits.

Another tactic is to scrub all personal data out of the ESI (ie remove email addresses, names, etc) before it is transferred out of the UK. Anonymising software exists to facilitate scrubbing; however, the approach should be cleared in advance with opposing counsel to be sure they will be satisfied receiving ESI from which all names and identifying information related to UK employees have been removed.

Applying savvy lawyering to the challenge

As the US and UK grapple with these issues, employing a conservative approach and smart lawyering with surgically targeted search technology can help multinationals achieve win-win resolutions. Savvy US litigators advise counsel to raise UK data protection issues with opposing counsel and the court early on in the litigation process, in order to set and manage expectations on the demand side. They also recommend negotiating protocols for security and privacy of all UK data produced in the case and having those provisions converted into a court order, which can be shown to UK employees and

data protection officials. Such protocols should also make provisions for the return of any ESI received from employees who later decide to revoke their consent to its transfer and production to litigation adversaries.

Other possible negotiated solutions include attorney review of the ESI by counsel for the requesting party in the UK, or obtaining agreements from the requesting party to receive the ESI after personal data has been scrubbed using anonymising software. Though it does not look as though we'll see a solution to the conflict between US disclosure obligations and UK data privacy laws any time soon, at this stage understanding the requirements of data protection authorities, choosing an approach that respects those requirements and selecting technology that meets legal obligations on both sides is the best recipe for success.

Patrick Burke is senior director and assistant general counsel at Guidance Software.

Ethical Considerations in eDiscovery

by Patrick Burke

Copyright December 20, 2006 by The Recorder. Reprinted with permission.

Sucessful e-discovery requires more than technology knowledge

With all of the attention directed to the new e-discovery amendments to the Federal Rules of Civil Procedure — which went into ef fect this month — there has been less focus on the related professional ethics obligations applicable to e-discovery practice. These ethical standards are drawn from rules such as the California Rules of Professional Conduct and the ABA's Model Rules of Professional Conduct. Familiarity with these standards is important not only for attorney compliance, but also for determining best practices for corporate law departments engaged in designing defensible e-discovery processes.

Now that the federal courts have adopted ediscovery standards, it is reasonable to expect further development of e-discovery ethics jurisprudence. Specifically, e-discovery practitioners may be required to be reasonably competent to advise clients on ediscovery matters, keep their clients informed, and safeguard client confidences and privileged communication. Fulfilling these duties while producing gigabytes of data to an adversay will be a challenge even for seasoned ediscovery experts. It's essential for both e-discovery neophytes and veterans to track how professional ethics standards are applied in the context of e-discovery, e-discovery best practices and the design of corporate e-discovery processes.

The keystone of e-discovery ethics likely will be the attorney's duty to act competently. Attorneys also are ethically obligated to keep their clients reasonably informed so as to enable informed consent about significant developments in the case being handled by the attorney on the client's behalf. Given the complex technological factors that drive preservation and collection of electronically stored information, competency will be a challenge for litigators, particularly those without significant e-discovery experience.

With so much at stake regarding e-discovery, clients will have even more reason to rely on their attorney's competency. As a result, expect ethics prosecutions in this area, as mistakes in preservation and collection can lead to allegations of spoliation and/or failure to comply with court discovery orders. Sanctions can include monetary fines, adverse inference instructions or entry of default judgments.

The ethical requirements are intended to protect the corporate client vis-a-vis the lawyers who advise it on e-discovery. Frequently, e-discovery-related advice comes from the company's outside trial counsel. But when a company's outside trial counsel faces discipline for ethical lapses related to that e-discovery advice, the corporate client could suffer potentially detrimental consequences in the case being litigated.

The Risk of Withdrawal of Trial Counsel.

One of the worst outcomes for corporate defendants is the loss of their outside trial team while a case is pending. This may occur if, during the course of litigation, the outsidelaw firm is charged with ethical violations related to the firm's supervision of the client's preservation and collection process. At this juncture, the outside law firm may be placed in a position where it is forced to defend itself against the ethical charge.

Consider the scenario in which a client resists or ignores outside counsel's recommendations with respect to the collection of electronic documents. If this resistance leads to an indefensible preservation or collection methodology, the outside lawyer may face allegations of unethical conduct for alleged "incompetence." The law firm's interest in testifying to clear itself of the ethical charge may then be adverse to the client corporation's interest in keeping such details privileged and confidential. The law firm's adverse interest then may require that it step aside as trial counsel (or that the court remove trial counsel from the case).

This predicament may further be compounded when an individual at the outside law firm also turns out to be the person most knowledgeable about the company's preservation and collection of electronically stored information, which in federal litigation could mean that that individual may be designated preservation and collection witness pursuant to Federal Rule 30(b)(6). If placed in the position of testifying on ediscovery matters, that witness may be obligated to disclose information relating to the representation of the client that would be detrimental to the corporation's position in the lawsuit, implicating the attorney's duty under ABA Model Rule 1.6(a) to protect a client's confidential information. Again, this may create an ethical conflict for the outside law firm that could lead to the firm's withdrawal and the client scrambling for new trial counsel (See ABA Model Rule 3.7 which prohibits lawyers from serving as advocates in trials in which "the lawyer is likely to be a necessary witness").

Structuring Defensible Processes to Avoid Disruption of Trial Counsel.

A corporate law department can structure its e-discovery processes so as to minimize the risk that it will lose its litigation team on the eve of trial as a result of an e-discovery problem, ethical allegation or adversity situation. One way to mitigate that risk is to bring the oversight of e-discovery preservation and collection processes in-house, including knowledgeable e-discovery counsel overseeing that process who either (i)belong to the corporate legal staff or (ii) are from a law firm other than the trial counsel, e.g., outside national e-discovery counsel that advises a company on a nationwide basis to ensure consistent practices in litigations across all jurisdictions.

Critical to the in-house approach is a strong alliance between legal and IT personnel to provide intelligent and efficient hands-on project management for each litigation, always keeping an eye on the corporation's interests in all of its current and future litigations.

Many companies already take it upon themselves to create in-house practice teams to respond to e-discovery obligations. The primary driver for creating inhouse e-discovery platforms is to reduce

cost and to align the company's e-discovery preservation and collection with its records management programs. Current technologies can make the in-house collection and preservation approach faster, cheaper and more defensible than outsourcing.

The effort to insulate outside trial counsel from e-discovery decision making must be paired with good communication between the corporate client and its trial counsel on the e-discovery preservation and collection process. The key is striking the correct balance between shielding trial counsel from ethical liability and keeping them informed enough that their supervision of the client's discovery responsibilities isn't considered inadequate. For example, trial counsel must not become so distanced from the client's discovery-related activities so as to be unable to effectively represent the client in negotiations with opposing parties, and before the court (See also Federal Rule 26(g), which imposes a duty to engage in pretrial discovery responsibly).

Designate Legal and Technical Contacts to Keep Trial Counsel Informed.

The bestpractice for keeping outside trial counsel informed on preservation and collection activities is to designate both legal and technical contacts with whom outside trial counsel should maintain open lines of communication. The legal contact can be either an inhouse e-discovery counsel or a designated outside lawyer from another law firm. The technical contact should be someone on the IT or litigation support staff responsible for internal preservation or collection processes.

Many corporations have engaged "national e-discovery counsel" who, although practicing at outside law firms, works intimately with the company's internal legal and IT personnel to develop and maintain defensible inhouse preservation and collection processes. National e-discovery counsel, whether internal or external, are tasked with ensuring that the corporation can demonstrate consistent ediscovery processes in all its litigations, which increases the legal defensibility of those processes. They also serve as a check against any particular trial team exerting pressure to short-cut or change preservation nd collection processes to the detriment of the company's effort to develop consistent processes.

The designated e-discovery technical contact person should almost certainly be on the corporation's staff, and would serve as a project manager for each litigation's preservation and collection efforts. The corporation should strongly consider designating this technical contact as the company's 30(b)(6) witness on e-discovery issues. This designation avoids the potential risk that arises when someone at the outside law firm becomes the person most knowledgeable about the client's e-discovery preservation and collection efforts and therefore de facto 30(b)(6) witness.

Overview of E-Discovery Ethics

The Duty to Act Competently With Respect to eDiscovery.

Most significant to eDiscovery ethics is the duty to act competently pursuant to ABA Model Rule 1.1 and California Rules of Professional Conduct 3-100. To practice without a solid grounding in eDiscovery rules, technology and best practices is to invite ethical challenges. There are a lot of

very good litigators who currently are not competent to offer counsel in this area. This raises the question of whether attorneys who need to get up to speed on eDiscovery can charge their clients for costs associated with their learning processes. ABA Model Rule 1.5 (Fees) and California Rules of Professional Conduct 4-200 require lawyers to charge only reasonable fees that take into account whether the lawyer had the skill required, meaning that they cannot charge their usual rate for time spent on work for which they are not reasonably skilled, in this case eDiscovery expertise.

The greatest difficulty comes when the lawyer must ensure that the client understands and complies with eDiscovery requirements and rulings. The lawyer's lack of competence may lead to noncompliance that will undermine the client's litigation position and threaten the lawyer's professional standing.

Duty to Keep the Client Reasonably Informed.

Closely related is the attorney's duty to keep the client reasonably informed, pursuant to Rule 3-500, which requires California lawyers to "keep a client reasonably informed about significant developments relating to the employment or representation ... ." Truly fulfilling this responsibility will be difficult for many litigators not intimately familiar with the detailed technology and processes required to maintain a defensible eDiscvery process. This is a duty eDiscovery practitioners must be able to demonstrate that they have met, along with the duty to obtain the client's informed consent before any significant eDiscovery decision in the case.

Serving the client competently and keeping the corporation reasonably informed so it can give informed consent requires that the legal team work closely with the IT team. Best practices call for the company to appoint a single in-house IT or litigation support person to serve as its 30(b (6) witness on eDiscovery matters with knowledge of the company's information systems. This person would serve as the key technical resource for the litigators at eDiscovery meet-and-confer conferences and in court proceedings going forward.

Obligation to Protect Client's Confidential and Privileged Information.

Privilege and confidentiality obligations loom larger in the eDiscovery area because it is relatively easy for the client's privileged and confidential information to be inadvertently produced to adversaries. ABA Model Rule 1.6 (Confidentiality of Information) and California Business & Professional Code §6068(e) obligate lawyers not to reveal clients' confidential information and to keep clients reasonably informed about the risk of inadvertent revelations of confidential information or privileged communications. These obligations can be best controlled when eDiscovery collection and preservation is conducted by in-house personnel who can apply consistent approaches from case to case.

Duty to Report Noncompliance with eDiscovery Processes.

Finally, in-house eDiscovery processes should include procedures for attorney reporting of noncompliance. Federal Rule 26(g) imposes a duty to engage in pretrial discovery responsibly. Ethical standards sometimes impose an obligation on a lawyer acting on behalf of an organization to report

noncompliance with eDiscovery obligations. See ABA Model Rule 1.13(b) (Organization as client") (If a lawyer 'knows' of intent to act or refusal to act in violation of law likely to result in 'substantial injury,' shall proceed as 'reasonably necessary' including referring to 'higher authority' and, if needed, to the 'highest authority' authorized to act.); See also ABA Model Rule 1.13(c) (authorizes a lawyer to reveal information under certain circumstances to prevent the injury).

When a lawyer cannot obtain cooperation from corporate employees in implementing eDiscovery processes, he or she must be prepared to move up the corporate chain of command in appropriate situations. See California Rules of Professional Conduct 3-600. In-house eDiscovery processes should make explicit provision for such reporting by counsel to avoid sanctions for failure to do so. This reporting process should be applicable to both in-house eDiscovery counsel and/or outside national eDiscovery counsel.

Patrick J. Burke is assistant general counsel at GuidanceSoftware Inc., prior to which he was a litigator at major firms including, most recently, the New York office of the London-based law firm Linklaters.

Canadian Privacy Law: The Personal Information Protection and Electronic Documents Act (PIPEDA)

by Dominic Jaar
Legal Counsel Ledjit Consulting, Inc. Canada
and
Patrick E. Zeller
Vice President & Deputy General Counsel, Guidance Software, Inc., United States

This white paper provides a general overview of the Personal Information Protection and Electronic Documents Act ("PIPEDA"), and discusses both the privacy requirements imposed by that Act as well as the rules governing the use of electronic documents that it sets out.

Overview

Introduction to PIPEDA

PIPEDA is the federal legislative response to growing concerns over the protection and use of personal information that is accumulated by both public and private organizations in the course of their day-to-day operations.[838] The Act sets out rules governing how such information should be handled by the organizations that collect it, and under what circumstances it may be disclosed, either to third parties or to the individual who is the subject of the information.

The Act contains two main parts. The first part sets out the rules governing the collection, retention and disclosure of personal information, as well as the remedies available in the event of a suspected breach. In essence, this part of the Act establishes a framework which attempts to balance the privacy rights of individuals with the needs of organizations to collect, use, and disclose personal information in the course of commercial activities. This part of the Act is discussed in sections I and II of this document.

The second part of the Act describes the circumstances in which electronic alternatives may be used to fulfill legal obligations, which, under federal laws, require the use of paper documents to record or communicate information or transactions. For example, this part includes provisions providing for the filing or retention of documents in electronic format, as well as the use of electronic documents as evidence in court proceedings. This part of the Act is discussed in section III of this document.

The enactment of PIPEDA was motivated not only by the government's concern with privacy issues within its borders, but also by privacy developments taking place in other countries with whom Canadians do business. For example, certain EU directives dealing with the protection of personal information impose restrictions on the flow of data into jurisdictions which do not have similar privacy protections in place. PIPEDA was therefore necessary to satisfy the "adequacy" requirement of EU privacy laws and avoid the creation of non-tariff barriers to trade with EU nations.[839]

838 Personal Information Protection and Electronic Documents Act ("PIPEDA"), 2000 S.C., ch. 5 (Can.).
839 Council Directive 95-468EC, art. 25, 1995 O.J. (L 281) 31-50.

Scope of PIPEDA

PIPEDA came into force on January 1, 2001 and was implemented in three stages. At each stage, the list of organizations required to comply with the privacy requirements of the Act expanded, with the final stage taking effect on January 1, 2004. The Act now applies to all organizations engaged in the collection, use, or disclosure of personal information in the course of any commercial activity within Canada. To better understand what this means, it is useful to refer to the definitions provided in the Act.

The term "**commercial activity**" means "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering, or leasing of donor, membership or other fundraising lists."[840] Early indications suggest that this term may be interpreted broadly. In one notable case, the Privacy Commissioner determined that a security ompany, Centurion[841], who installed surveillance cameras in a public intersection, monitored the cameras, and reported incidents to the local police free of charge in an effort to generate business was engaged in a "commercial activity" for the purposes of PIPEDA compliance.

The term "**organization**" covers everything from traditional "brick-and-mortar"-type businesses to e-commerce businesses and includes corporations, associations, partnerships, trade unions and persons.[842] The application of PIPEDA also extends to certain public and government entities, provided that they are not already subject to the Privacy Act.

The term "**personal information**" means any information about an identifiable ndividual, including, but not limited to: name, age, gender, race, marital status, home address, credit rating, medical history, criminal history, purchasing history, and even an image of a person.[843] Personal information also includes information that, combined with other information available to the organization, can identify an individual, such as a table of customer ID numbers. Personal information does not include the name, title, or business address or telephone number of an employee of an organization.[844]

The term "**record**" is defined broadly under PIPEDA, and includes "any correspondence, memorandum, machine-readable record, or any other documentary material, regardless of physical form or characteristics, and any copy thereof."[845] Businesses must "monitor all of their files, regardless of the form of storage which may contain personal information." In the Centurion case discussed above, the Privacy Commissioner determined that, although Centurion was not recording the surveillance camera images on a tape but was merely monitoring the cameras 24-hours a day, the images the camera displayed were "records" under PIPEDA.

Finally, the "**use**" of information is defined as the "treatment and handling of personal information within an organization." By contrast, "**disclosure**" refers to the transfer of data outside the organization.

---

840 PIPEDA, 2000 S.C., ch. 5, s. 2(1) (Can).

841 Federal Privacy Commissioner says "no" to Street Surveillance Camers (June 20, 2001), accessed at<http://www/priv.gc.ca/media/an/nt_010620_e.cfm>on May 7, 2009.

842 *Id.*

843 *Id.*

844 *Id.*

845 *Id.*

It should be noted that collection, use, and disclosure of personal information are considered to be distinct events for purposes of the Act.

Territorial Application

Although PIPEDA is federal legislation with the force of law in all jurisdictions across Canada, the Act also permits the Privacy Commissioner to exempt a province from the application of PIPEDA where that province has enacted "substantially similar" provincial privacy legislation. In such a case, it is the provincial legislation that regulates the privacy obligations of an organization, and PIPEDA has no application.

Currently, three jurisdictions have received exemptions from PIPEDA: Quebec, British Columbia, and Alberta. For the most part, the legislation in these provinces mirrors PIPEDA. However, any company engaging in personal information collection, use, or disclosure in any of these three provinces is strongly advised to consult the provincial legislation to ensure compliance with the specific privacy laws applicable in that jurisdiction.

This latter advice is particularly important for companies operating in Quebec, where privacy obligations are more onerous than under PIPEDA. The legislative regime in that province is composed of two separate statutes, one governing privacy issues (*An Act respecting the protection of personal information in the private sector*[846]) and a second dealing with the use of electronic documents (*An Act to establish a legal framework for information technology*[847]). Together, these two statutes establish a framework similar to the two parts of PIPEDA.

It should be noted, however, that organizations operating under the Quebec legislation are subject to more stringent requirements affecting not only the manner in which information must be recorded and stored and the protections that must be put in place by the organization, but also the manner and content of communications with the individual concerned by the information, his or her rights of access, and the limitations placed on use and disclosure. Organizations operating in Quebec should therefore avoid relying on their knowledge of PIPEDA in determining their policies and practices relating to that jurisdiction.

With respect to international entities, PIPEDA does not specify the minimum level of connection that a company must have with Canada in order to be subject to its provisions. No language in PIPEDA limits its application to businesses with a physical presence in Canada, nor are its provisions explicitly limited to personal information collection, use, or disclosure occurring solely within Canada. Furthermore, the Act was enacted by Parliament partially to protect personal information in cyberspace and e-commerce transactions. Therefore, it is likely that a foreign company operating only marginally in Canada – for example, by hosting a website available to Canadian citizens or entities – will be subject to PIPEDA.

846 R.S.Q. ch. P-39.1 (2006).
847 R.S.Q. ch. C-1.1 (2001).

Individual Rights

An individual who feels that his rights under PIPEDA have not been respected has several recourses which he or she may use to challenge a company's compliance with the Act:

- By complaining directly to the company;
- By filing a written complaint with the Privacy Commissioner of Canada;
- By applying for a hearing in Federal Court, but only after receiving the Privacy Commissioner's report.

Complaints with the Privacy Commissioner may be filed anonymously.

Role of the Privacy Commissioner

The Commissioner has the authority to receive, investigate, and resolve complaints brought within the framework of PIPEDA. If the Commissioner has reasonable grounds to believe that an organization is not in compliance with PIPEDA, the Commissioner has the authority to audit the company's personal information handling policies and practices.Such audits are expensive, time-consuming, and reach all levels of a company.

The Commissioner may also make recommendations on a company's privacy practices, and may demand to be notified within a specified time that the recommendation has been implemented. The Commissioner may publicize a company's non-compliance with PIPEDA, including publication of results of an audit in the yearly report to Parliament, if he deems that it is in the public interest to do so. The Commissioner may also seek remedies in the Federal Court.

The Federal Court

The Federal Court has jurisdiction to hear matters resulting from a complaint filed with or investigated by the Privacy Commissioner. If the Court is satisfied that a breach of the Act has occurred, it may order a company to revise its practices, or publish a notice of the actions it will take to rectify its non-compliance.

In addition, the Federal Court may award damages to the complainant, including damages for humiliation, and may impose fines of up to $100,000 on the company or its directors, officers, and employees.

Implementing Compliance

The Ten Basic Principles

The application of PIPEDA is guided by 10 principles for compliance, each of which serves to further the Act's essential theme: that organizations may not collect, use, or disclose personal information in the course of commercial activities without the informed consent of the individual who is the subject

of that information. All organizations that are subject to PIPEDA must implement policies that respect its guidelines.

Some of these 10 principles are mandatory, while others are only recommendations. The distinction turns on whether the term "shall" or "should" has been used in describing the principle. Taken together, these 10 principles outline a company's model for compliance with PIPEDA.

1. Accountability.

Every company is responsible for the data under its control, and must appoint an individual or individuals who are accountable for the organization's compliance. Every company that possesses personal information must implement and maintain policies and practices to ensure compliance, such as: establishing a policy protecting personal information, establishing a complaint process, training employees, and developing materials to explain the policies.

2. Identifying Purpose.

The company must identify the purpose for collecting the personal information at, or before, the time it collects it. A noteworthy Canadian case, *Eastmond v. Canadian Pacific Railway*,[848] explored PIPEDA's subsection 5(3) requirement that an organization may collect "personal information only for purposes that a reasonable person would consider appropriate in the circumstances." In *Eastmond*, the Privacy Commissioner applied a four-part test to determine whether the company's decision to conduct video surveillance in the mechanical facilities area in which employees worked was reasonable. The four-part test included whether: 1) the measure was demonstrably necessary to meet a specific need; 2) the measure was likely to be effective in meeting that need; 3) the loss of privacy was proportional to the benefit gained; and 4) whether there was a less privacy-invasive way of achieving the same end. Later, the Federal Court, on review, adopted the Commissioner's four-part test, and added another prong of analysis: if the purposes were reasonable in the circumstances, did the company violate its PIPEDA obligations by not obtaining the consent of its employees before collecting the information (i.e., operating the video cameras)?

3. Consent.

This is by far the most important of the 10 basic principles. A company may only collect, use, or dispose of personal information with the knowledge and consent of the individual. Valid consent requires the company to inform the individual of what personal information the company is collecting, the manner in which the company will use the information, and to whom the information will be disclosed. If the company later wishes to use the information for another purpose, it must first obtain the informed consent of the individual to use the information for the new purpose.

The form of the consent required depends on the sensitivity of the information and the reasonable

848 [2004] F.C. 852 (Fed. Ct. Can.).

expectations of the individual under the circumstances. Implied ("opt out") consent is sufficient in cases where the information is not particularly sensitive, an where the individual would likely expect the company to use the information for a given purpose (for example, an individual who subscribes to a magazine is likely to expect the magazine to use his personal information to send him magazines and renewal notices). Express ("opt-in") consent is required where the information is sensitive, and the individual would not reasonably expect the company to use the information for a given purpose. Consent may be obtained in a number of ways: by providing notice on an application form, by providing an opt-in or opt-out box, or even orally.

Consent may not be "coerced" in the manner that is allowed in the United States. A company may not condition the supply of a product or service on an individual consenting to the collection, use, or disclosure of information beyond what is required for the product or service itself. For example, in the U.S. it is common for marketers to induce customers to provide personal information, for example through a survey, in exchange for a benefit, such as a chance at winning a free product or service. This type of "consent" is insufficient for purposes of PIPEDA compliance.

There is no "grandfathering" of information collected prior to PIPEDA's enactment. If the company wishes to use or disclose information it collected prior to PIPEDA, it must obtain the necessary consent, unless an exception applies.

Consent may be withdrawn by the individual at any time, subject to legal or contractual obligations, and upon reasonable notice. The company must inform the individual of the consequences of withdrawing consent.

4. Limiting Collection.

A company may not collect more information than is necessary for the purposes identified, and information may not be collected by unfair or deceptive means.

5. Limiting Use, Disclosure, and Retention.

A company may not use or disclose personal information for any purposes other than those consented to by the individual. A company may not retain information longer than necessary for the purposes the individual consented to.

6. Accuracy.

A company in control of personal information must ensure that the information kept is accurate, complete, and up to date to minimize the possibility that inappropriate information is used to make decisions about the individual. However, a company is not mandated to routinely update information, unless the updates are needed for the purposes consented to. This principle presents a potential **legal Catch-22**, because a company may have to go back and gather more information to ensure accuracy, but then it is collecting the information for a different purpose than the one originally consented to.

7. Safeguards.

Companies must protect and keep safe the personal information in its control against loss, theft, unauthorized access, disclosure, copying, use and modification. Types of safeguards include physical measures (e.g., locks), organizational measures (e.g., security clearances, limiting access to those on a "need-to-know" basis), and technological measures (e.g., encryption, passwords).

8. Openness.

Companies must be open about their policies and practices on its management of personal information by making its policies readily available to the public in a form that is generally understandable. This can be achieved, for example, by posting its personal information management policies on its company website. The information posted must include: name or title, and address of the individual accountable for the organization's compliance and the individual responsible for inquiries or complaints, means of gaining access to the personal information held by the organization, description of the personal information held by the organization and a general account of its use, and a description of personal information made available to related organizations, such as subsidiaries.

9. Individual Access.

A company must allow individuals to know what information the company holds about them and to whom the information has been disclosed. A company must also allow an individual to access that information, and must allow the individual a procedure in which to challenge the accuracy of the information and have the information amended.

In limited circumstances, an organization may refuse an individual's request for access. These circumstances include a request for information that is prohibitively costly to provide or that contains information about other individuals, information that cannot be disclosed for legal, security or commercial proprietary reasons, and information that is subject to privilege. In all cases, the reason for the refusing access should be provided to the individual on request.

10. Challenging Compliance.

A company must establish and maintain a complaint process for receiving and resolving complaints about their personal information handling practices. The company must also make individuals with inquiries aware of this complaint process, and the process must be readily accessible and easy to use.

Transfers to Third Parties

As indicated by the 10 principles, consent is the golden rule under PIPEDA. Thus, an organization that wishes to transfer personal information to a third party, subsidiary, affiliate, or agent must obtain the prior informed consent of the individual(s) concerned. In addition, contractual protections must be

used to ensure that the third party is bound to provide a comparable level of security, and to use the information for the same purposes for which it was originally collected. Cross-border transfers are treated no differently from domestic transfers taking place wholly inside of Canada.

In the case of a transfer of personal information to an agent, the necessary contractual protections include: strict confidentiality provisions, specifications regarding how and when the information must be destroyed, disposed of, or returned, and a requirement that the third party refer requests for access or complaints back to the company. In the case of transferring personal information to a non-agent third party, necessary contractual provisions include: limitation to use only for the purposes consented to by the individual, and a requirement that the third party seek consent from the individual before any further disclosure occurs.

Exceptions: When Consent is Not Required

Despite the overriding importance ascribed to the principle of consent under PIPEDA, it is not without exceptions. The Act also recognizes that there may be circumstances where it would be unreasonable, impracticable or even counterproductive to require an organization to obtain consent to the collection, use and/or disclosure of protected information. Certain limited exceptions to the consent requirement have therefore been provided.

For example, collection and use of information without consent is permitted if it is clearly in the individual's best interests and his or her consent cannot be obtained in a timely way. An example of such circumstances is in the case of an emergency where the life, health or security of an individual is threatened.

Collection and use of information which is publicly available, or which is intended solely for journalistic, artistic, scholarly or literary purposes is also permitted without consent. This applies also to information used for statistical or scholarly study or research, provided that the information is used in a confidential manner, it is impracticable to obtain consent, and the Privacy Commissioner is informed prior to the use.

Perhaps most importantly, the Act also contains exceptions which permit the collection, use and disclosure of information for purposes related to the enforcement of laws, the obtaining of legal advice or assistance, or enforcement of the organization's rights. For example, consent is not required under any of the following circumstances:

- The information is sought for violations of agreements or the law, and seeking consent would compromise the accuracy of the information;
- The information is given to legal counsel for the organization;
- The information is given to the government for security, defense or law enforcement purposes;
- The information is used for purposes of debt collection;
- The information is used pursuant to a valid court order or law;
- An emergency, including an imminent breach of contract, demands disclosure

To date, there is limited guidance available from courts as to the interpretation that will be given to these exceptions. Some general guidance of a cautionary nature may be taken from one recent case, *Shred-Tech Corp. v. Viveen*.[849] That case dealt with a plaintiff who, in preparation for legal proceedings, had obtained copies of the defendant's phone records from an investigative agency without the defendant's consent or knowledge. The plaintiff's investigator also posed as a customer in the defendant's place of business and secretly made an audio and video recording The court granted the defendant's motion to be released from the deemed undertaking rule that applies to pre-trial disclosures in order to file a complaint with the Privacy Commissioner. This conclusion suggests that while PIPEDA does permit the collection of personal information in preparation for litigation, it nonetheless does not authorize collection by invasive or otherwise impermissible means, and cannot be invoked to shelter alleged violators from the consequences of such actions.

Another very interesting case, currently awaiting transfer to the Federal Court, may provide additional insight into the scope of protections mandated by PIPEDA in the context of legal proceedings. In *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada,*[850] State Farm seeks a declaration that PIPEDA does not apply to the disclosure of documents, privilege, or other privacy interests of a plaintiff who is suing a defendant insured by State Farm, or that, alternatively, the PIPEDA is ultra vires. The plaintiff in the original suit had filed a complaint with the Privacy Commissioner after State Farm refused to disclose to him the information about him that it had collected in the course of investigating the claims made in his action against State Farm's client. The Privacy Commissioner proceeded to investigate the plaintiff's complaint, which State Farm alleged it had no jurisdiction to do. It will be interesting to see how the Federal Court resolves these issues if and when the case is heard.

It is also useful to note that an organization who is not party to litigation may nonetheless be required to disclose personal information that it has compiled, where requested to do so by an interested party and authorized by a court. In *BMG Canada Inc. v. Doe,*[851] the Federal Court of Appeal ordered an internet service provider to disclose the identities of certain of its clients who were allegedly using its service to distribute songs over the internet in violation of copyright. In making this order, the Court commented that although "privacy rights are significant and they must be protected", in this case the need for protection was outweighed by the public interest in permitting copyright owners to identify and pursue infringers.

It goes without saying that in any case where use or disclosure of protected information takes place, either with or without consent, it should be done with caution and with appropriate safeguards to ensure that privacy rights are intruded upon as minimally as possible. In case of doubt, it is advisable to seek guidance from legal counsel, the Privacy Commissioner, or a court, as appropriate.

849 C346-05, [2006] O.J. 4893 (O.S.C.J. Dec. 5, 2006).

850 [2009] NBCA 5 (N.B.C.A. Jna. 22, 2009) (holding that the Federal Court was the appropriate forum to resolve the PIPEDA challenge).

851 [2005] 252 D.L.R. (4th) 342 (Fed. Ct. Can.).

Electronic Documents

In addition to the privacy rules set out in the first part of the Act, Part II of PIPEDA provides rules to establish the circumstances and conditions under which electronic documents may be used to fulfill requirements for the creation, filing or retention of paper records pursuant to federal laws.

This part of the Act has tended to receive less attention than the privacy rules since its impact on organizations was overshadowed by the initial rush to implement compliance policies which followed the enactment of PIPEDA. However, the importance and usefulness of the rules set out in Part II should not be underestimated. Organizations need to be aware of these rules, not only to ensure that they comply with the conditions they contain, but also to be able to take fullest advantage of the efficiencies and cost-savings that may be had by using electronic documents and data storage alternatives.

Document Retention

Part II of PIPEDA follows the federal laws that dictate document retention requirements. This aspect of the scheme affects both private and public organizations.

Document retention requirements include, for example, obligations for organizations or individuals to retain copies of information they have collected and/or filed pursuant to tax laws or labor and employment laws. Pursuant to PIPEDA, a requirement under federal law to retain a document for a certain period of time may be satisfied by retention of the document in electronic form, provided that certain safeguards concerning the authenticity of the document are respected.

These safeguards include:

- The retention of the document in the format in which it was made, sent or received, or in a format that does not change the information contained in the original electronic document;
- The readability or perceivability of the information in the electronic document by any person who is entitled to have access to it or require production of it;
- The retention of any information that identifies the origin and destination of the electronic document, and the date and time when it was sent or received.

Jurisdictional Issues

As noted, the electronic document provisions of PIPEDA apply only to dispositions set out in federal laws. Consequently, any stipulations arising from provincial laws – e.g., concerning document retention or methods of authenticating certain types of documents – are not affected by the provisions of PIPEDA. However, many Canadian provinces have enacted comparable legislation which provides for the use of electronic documents to fulfill requirements set out under provincial statutes. It is therefore advisable for organizations to consult the laws in effect in the province(s) where they do business to find out whether such legislation exists.

Impact of PIPEDA on Discovery Procedures

The increased emphasis on protecting privacy which is exemplified by PIPEDA and its provincial counterparts has, not surprisingly, added a new dimension to conflicts over disclosure of information during pre-trial discovery procedures. This conflict is also heightened by the proliferation of electronic forms of communication, documentation and data storage used in modern commerce and accorded a new legitimacy by legislation like Part II of PIPEDA.

With such vast quantities of information now stored electronically and accessible with a relative ease that did not exist in the pre-digital age, courts are beginning to grapple with questions about how much information should be discoverable, how it should be made available, and how privacy rights can remain protected at the same time. While the case law on these issues is still in its infancy, certain general tendencies may be discerned.

For one thing, courts seem, as a general rule, to appreciate the importance of protecting privacy rights, and are generally mindful of the need to avoid unnecessarily broad disclosure. In *Innovative Health Group Inc. v. Calgary Health Region*,[852] for example, the Alberta Court of Appeal overturned a lower court decision ordering a party to produce, in their entirety, its imaged hard drives, as well as files containing a combination of relevant and non-relevant personal information. In doing so, the Court commented at length about the importance of maintaining proportionality in electronic discovery, and concluded that judges should always "hear representations as to how information that is neither material nor relevant can be protected from exposure, and frame any production order in the least intrusive manner." A similar position was advocated by the Federal Court of Appeal in *BMG Canada Inc. v Doe,*[853] a case concerning disclosure by an ISP of the identities of alleged copyright infringers using its service.

Moreover, it is to be expected that parties seeking access to electronic data will have to demonstrate the relevance of the information before access will be permitted. Requests for disclosure which have the air of a fishing expedition, rather than a request for specific information, should be refused. This was the outcome in *Park v. Mullin,*[854] where the defendant's request for access to the plaintiff's computer, used for both personal and business purposes, was considered to be overbroad, insufficiently precise as to the type of information sought, and not in conformity with privacy concerns.

It is also interesting to note that when it comes to identifying what constitutes a "document" for discovery purposes, some courts have made a distinction between the electronic medium used to store information and the information itself. In the *Innovative Health Group* decision discussed above, the Court considered a computer hard drive to be akin to an "electronic filing cabinet" – that is, a physical repository containing individual documents that may or may not be relevant to the proceedings. The Court therefore found that the hard drive itself did not constitute a "document", such that its production to the opposing party was not appropriate.

As these examples from the case law suggest, courts appear to be approaching privacy issues at

852 [2008] 433 A.R. 312 (A.B.C.A. June 13, 2006).

853 [2005] 252 D.L.R. (4th) 342 (Fed. Ct. Can.).

854 04/0348 [2005] B.C.J. 2855 <B.C.S.C. Dec 30, 2005).

the discovery stage with some measure of caution and with an eye to providing the best measure of protection possible, without unduly obstructing the legitimate discovery of information which is relevant and material to the litigation. More judicial interpretation is needed to further define the ground rules that will govern the disclosure and protection of personal information in this context. It is hoped that the present document has provided some helpful insight into the rights, obligations, and issues that are at stake.

10 Privacy-Related Questions You Need Answers To in the Discovery Context

1. Where is the potentially relevant information located?
   a. Which laws apply?
   b. Which court has jurisdiction?
2. Is there personal information within the potentially relevant information?
3. Is there irrelevant personal information within the potentially relevant information?
   a. Can it be easily identified?
   b. Can you segregate it?
4. Can you extract or redact the irrelevant personal information?
5. Whose personal information is it?
   a. Is it possible to identify them?
6. Do you have their consent?
   a. Can you obtain their consent?
7. Are you supposed to possess this personal information?
8. Will the information cross jurisdictions?
9. Who has or will need access to or control over that information?
10. What steps will be taken to keep the information secure?

Dominic Jaar is an e-discovery and legal technology expert. He is the president and legal counsel of Ledjit Consulting and has recently been appointed as Chief Executive Officer of the Canadian Centre for Court Technology (www.linkedin.com/in/dominicjaar).

He speaks throughout North America (www.ledjit.com/conferences/) and is a prolific writer on many legal and technology issues. He is frequently quoted in the press as an expert on electronic information (www.claimid.com/dominicjaar).

Mr. Jaar is on the editorial board of Sedona Canada and was in charge of drafting the French version of The Sedona Canada Principles on E-discovery. He is also a member of The Sedona Conference's working groups 1 (USA) and 6 (International). Mr. Jaar is the co-president of the Montreal Bar Association Technology Advisory Liaison Committee with the Quebec courts and is the president of the Law Practice Management and Technology section of the Canadian Bar Association. He is on the ABA Techshow planning board and is a board member of the Canadian IT Association (www.it-can.ca). Furthermore, Mr Jaar is the founder and organizer of Leg@l.IT, Canada's premier conference on legal technologies (www.legalit.ca). Mr. Jaar is a member of Guidance Software's advisory board.

Prior to founding Ledjit, Dominic Jaar worked as a commercial litigator at Bell Canada's legal department. Besides pleading cases for Bell, he advised his clients on electronic discovery, electronic information management, compliance and retention policies. Prior to moving in-house, Mr. Jaar worked as a commercial litigator at Borden Ladner Gervais where he specialised in technology related matters. He is a member of the Quebec Bar. He graduated from Laval University after studying at Western University (Common Law) and Aix-Marseille III (International and European Law).

Ledjit Consulting was founded to help corporations and law firms better manage their information while acquiring the capacity to handle electronic discovery in-house. With a team of lawyers, IT specialists, project manager and paralegal, Ledjit supports its clients in the development of policies and procedures during all the information life cycle, the restructuring their IT infrastructure, the implementation of information management technologies and the identification, preservation, collection, processing, review, production and presentation of electronic evidence..

Dominic Jaar, President and Legal Counsel, Ledjit Consulting, Inc., DJaar@Ledjit.com

Patrick E. Zeller is Vice President and Deputy General Counsel for Guidance Software Inc. where he performs in-house legal functions, supervises the legal and regulatory team, and works with corporate law departments of other companies seeking to implement defensible in-house eDiscovery processes in the US, Canada, UK, and Europe. He writes and speaks regularly on topics related to eDiscovery and digital evidence and the intersection between law and technology.

Prior to joining Guidance Software, Mr. Zeller practiced litigation at Seyfarth Shaw LLP where he co-chaired the firm's Electronic Discovery Practice Group. He practiced commercial litigation, with a strong emphasis on technology issues and electronic discovery.

Mr. Zeller served as an Assistant Attorney General and Director of the Computer Crimes Institute for the State of Illinois where he prosecuted a wide variety of technology related crimes and supervised a multi-jurisdictional computer forensic laboratory. During this time, he was named a Computer Crimes Fellow by the United States Department of Justice and served as a trial attorney for the Department's Computer Crime and Intellectual Property Section, where he advised prosecutors and law enforcement agents on how to conduct Internet and high-tech criminal investigations.

He has lectured extensively on Internet and high-tech crime at numerous law enforcement training venues nationwide, including the FBI Academy. He is widely regarded as one of the leading minds in technology and the law; his specialties include eDiscovery, internal investigations, computer intrusion, economic espionage, online fraud, intellectual property and trade secret issues.

Mr. Zeller is an Adjunct Professor and Distinguished Lecturer at The John Marshall Law School's Information Technology and Privacy Law LLM program, where he teaches the "eDiscovery, Computer Evidence and Computer Forensics" class. He also holds several certifications in computer forensics, is a member of the Sedona Conference and presided over the Midwest Chapter of HTCIA High Technology Crimes Investigators Association in 2008 and is a member of the national steering committee of ASDFEDAmerican Society of Digital Forensics and eDiscovery.

Guidance Software was founded with a clear purpose: to develop solutions that search, identify, recover and deliver digital information in a forensically sound and cost-effective manner. Since our founding in 1997, we have moved into network-enabled investigations, enterprise-wide integration with other security technologies, and now, have powerful earch and collection capabilities for eDiscovery and other investigations. Yet we haven't strayed from our core competency and continue to be widely recognized for quality and value.

Patrick E. Zeller, Vice President & Deputy General Counsel, Guidance Software, Inc.
Patrick.Zeller@GuidanceSoftware.com

A Primer on International eDiscovery in Canada[855]

by Dominic Jaar
Copyright 2010 by Dominic Jaar. Reprinted with permission.

Introduction

"This perfect equality and absolute independence of sovereigns, and this common interest impelling them tomutual intercourse, and an interchange of good officeswith each other, have given rise to a class of cases inwhich every sovereign is understood to waive theexercise of a part of that complete exclusive territorialjurisdiction which has been stated to be the attribute of every nation."[856]

While "conventional" eDiscovery (or even papery discovery, for that matter) has its own set of rules, difficulties and caveats, the particularities of international eDiscovery are mainly due to the international part of the expression. International eDiscovery is, figuratively speaking, the mere act of crossing the border prior to the actual discovery process.

Canada is not part of the *Convention on the Taking of Evidence Abroad in Civil or Commercial Matters*[857]. Due to the fact that the Convention doesn't have "an adequate federal state clause[,] which would permit phased-in implementation of the Convention", and given the federal nature of Canada and the inherent difficulty in coordinating the legislative agendas of eleven jurisdictions, Canada can only give its support in principles to the Convention[858]. Canada is not part to the *Inter-American Convention on Letters Rogatory*[859], either. That is not to say that Canada is devoid of ways to obtain evidence within its border: private international law provides the necessary background for the applicable statutes and their construction.

The law of international evidence collection in Canada is based on the principle of comity, which acknowledges the necessity for a sovereign entity to exercise its sovereignty for the potential benefit of another country's citizen, in the greater interest of the community of nations. The Supreme Court of Canada had the occasion to define the term on referred to a 1895 case before the Supreme court of the United States, stating that:

> ""Comity" in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws"[860].

855 © 2010 Dominic Jaar

856 The Exchange v. McFaddon, 11 U.S. 7 Cranch 116 136-137 (1812) (US Supreme Court, Marshall J.), referred to in Zingre v. The Queen et al., [1981] 2 S.C.R. 392

857 Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters,

858 Charles Platto (ed.), *Obtaining Evidence in Another Jurisdiction in Business Disputes* (Boston: International Bar Association, Graham & Trotman, 1988) 25-26.

859 Text and general information on the treaty at <http://www.oas.org/juridico/english/sigs/B-36.html>.

860 *Hilton v. Guyot*, 159 U.S. 113 (1895), at pp. 163-64, as cited in *Morguard investments ltd. v. Desavoye*, [1990] 3 S.C.R. 1077

The principle of comity strikes a balance between different values: cooperation with other sovereign entities and protection of the requested country's citizens. Indeed, "what must underlie a modern system of private international law are principles of order and fairness, principles that ensure security of transactions with justice"[861]. By nature, these principles apply to either litigant. In the context of requesting the assistance of Canadian courts to enforce letters of request, the principal implication is that when examining the said letters, Canadian courts will actually *examine* them – there is no "rubberstamping". On the other hand, "comity dictates that a liberal approach should be taken to requests for judicial assistance, so long at least as there is more than ephemeral anchorage in our legislation to support them."[862]

Procedure for International Evidence Collection

The fact that Canada has not signed the international conventions pertaining to international evidence collection does not preclude any federated jurisdiction to have dispositions similar in effect within its statutes. In fact, the federal level and eight provinces have enacted such statutes[863] – only Prince Edwards Island and Newfoundland-and-Labrador have not[864]. The proper procedure for each jurisdiction is set out in the applicable law.

For instance, in Ontario, the Superior Court identified four requirements that must be met *before* the court exercises its discretion regarding a letter rogatory:

- the witness whose evidence is sought must be within the jurisdiction of the requested court;
- the foreign court must express its intention in obtaining the evidence, by commission, order or other process;
- the evidence sought must be in relation to a matter (the various acts differ in scope) pending before the foreign court; and
- the foreign court must be a court of competent jurisdiction.

The Ontario Superior court used this analysis grid on a number of cases[865]. These requirements

861 *Morguard investments ltd. v. De savoye*, [1990] 3 S.C.R. 1077

862 *States of America (District Court) v. Royal American Shows, Inc. et al.*, [1982] 1 S.C.R. 414, 421, cited in Pamela D. Pengelley, "A Compelling Situation: Enforcing American Letters Rogatory in Canada", (2006) 85 *Canadian Bar Review* 345, 347

863 *Canada Evidence Act*, R.S.C. (1985) ch. C-5, s. 43-51 (Federal) ; *Evidence Act*, R.S.B.C. 1996, c. 124, s. 53 (British Columbia) ; *Alberta Evidence Act*, R.S.A. 2000, c. A-18, s. 56 (Alberta) ; *Evidence Act*, S.S. 2006, c. E-11.2, s. 65 (Saskatchewan) ; *Manitoba Evidence Act*, C.C.S.M. c. E150, s. 82 (Manitoba) ; *Evidence Act*, R.S.O. 1990, c. E.23, s. 60 (Ontario) ; *Special Procedures Act,* R.S.Q. ch. P-27, s. 9-20 (Québec) ; *Evidence Act*, R.S.N.B. 1973, c. E-11, s. 30-32 (New Brunswick) ; *Evidence Act*, R.S.N.S. 1989, c. 154, s. 70-73 (Nova Scotia).

864 However, similar dispositions may be found in the Newfoundland-and-Labrador *Rules of the Supreme Court*, 1986, S.N.L. 1986, c. 42, Sch. D, r. 47.

865 *Germany (Federal Republic) v. Canadian Imperial Bank of Commerce*, 1997 CanLII 12091 (ON S.C.) ; *King v. KPMG and KPMG Investigation & Security Inc.*, 2003 CanLII 49333 (ON S.C.) ; *Scienton Technologies Inc. v. Canadian Imperial Bank of Commerce,* 2009 CanLII 29188 (ON S.C.).

are of procedural nature and the specifics are to be found in the governing law (see, for example, the federal *Canada Evidence Act*[866] and *Quebec's Special Procedure Act*[867]).

Regarding the second criteria, it has been said that "[t]he letters rogatory must constitute a formal request from a court in the United States to a Canadian court. A request from the United States Embassy or its consulates, for example, is not sufficient"[868].

The third criterion directly refers to the scope of the applicable law. Ontarian and federal acts have often been invoked side by side without real consequences because of the great similarities between the statutes. A constitutional argument may be made that the foreign component of the letters rogatory calls for the exclusive application of the federal act[869] instead of the provincial acts. A second aspect of the criteria is that the civil action must be commenced before the foreign court in order for it to ask for the assistance in obtaining evidence[870].

Finally, the fourth criterion on jurisdictional competence is two-sided. First, the requesting court's enabling statute must allow the court to issue such request, thus excluding private arbitrators. Secondly, the court must be able to exert sanctions to enforce its orders[871].

---

866 *Canada Evidence Act*, supra note 9, s. 46(1) : "If, on an application for that purpose, it is made to appear to any court or judge that any court or tribunal outside Canada, before which any civil, commercial or criminal matter is pending, is desirous of obtaining the testimony in relation to that matter of a party or witness within the jurisdiction of the first mentioned court, of the court to which the judge belongs or of the judge, the court or judge may, in its or their discretion, order the examination on oath on interrogatories, or otherwise, before any person or persons named in the order, of that party or witness accordingly, and by the same or any subsequent order may command the attendance of that party or witness for the purpose of being examined, and for the production of any writings or other documents mentioned in the order and of any other writings or documents relating to the matter in question that are in the possession or power of that party or witness."

867 *Special Procedure Act*, supra note 9, s. 9 : "When, upon petition to that effect, it is shown to the Superior Court or to one of the judges thereof, charged with the administration of justice in the district, that a court of any other Province of Canada, or of any other British possession, or of a foreign country, before which any civil or commercial case is pending, desires to have the evidence of and party or witness in the district, such court or judge may order that such party or witness may be examined under oath, either by means of question in writing or otherwise, before any person mentioned in the said order, and may summon, by the same or by a subsequent order, such party or witness to appear for examination, and may order him to produce any writing or document mentioned in the order, or any other writing or document relating to the matter, and which may be in his possession."

868 P.D. Pengelley, supra note 8, p. 350, citing Janet Walker (ed.), *Walker and Castel on Canadian Conflict of Laws*, 6th ed., looseleaf (Toronto: Lexis Nexis Inc., 2005) at para. 6.4.b..

869 Pengelley, supra note 8, p. 351, n. 31 identified an review article and two decisions to this position, while another is to the opposite effect, saying that the provincial statute applies to foreign civil matters.

870 ABA Section of Antitrust Law, *Obtaining Discovery Abroad* (Chicago, American Bar Association: 2005) p. 84 [hereinafter "*Obtaining Discovery Abroad*"].

871 Pengelley, supra note 8, p. 352. The author cites the case of *McCarthy v. United States Securities and Exchange Commission*, [1963] 2 O.R. 154 (C.A.), where the Ontario Court of Appeal refused to enforce an SEC letter of request. See also *Obtaining Discovery Abroad*, p. 84-86, where such attribute is called "mutuality of purpose" between the requesting tribunal and the Canadian court.

Evaluation criteria

In the exercise of its discretion on whether or not to assent to the letter of request, a court may refer to multiple criteria. These criteria relate to the content of the letter of request, where the requirements set out in the section above are procedural conditions.

In a 1996 decision, the Ontario Court (General Division) established a list of criteria to guide its decisional process:

1. "the evidence sought is relevant;
2. the evidence sought is necessary for trial and will be adduced at trial, if admissible;
3. the evidence is not otherwise obtainable;
4. the order sought is not contrary to public policy;
5. the documents sought are identified with reasonable specificity;
6. the order sought is not unduly burdensome, having in mind what the relevant witnesses would be required to do, and produce, were the action to be tried here."[872]

Being guidelines for the exercise of a discretionary power, this list is inherently nonlimitative Each element has to be proven before the requested court – generally by affidavits. Some remarks on these requirements are necessary, though[873].

> The requirement of the evidence being used for trial is not as strict as it may appear. In a 1981 decision, the Supreme Court was of the opinion that "In general, our courts will only order an examination for the purpose of gathering evidence to be used at a trial, but that is not to say that an order will never be made at the pre-trial stage. Section 43 [of the *Canada Evidence Act*] does ot make a distinction between pre-trial and trial proceedings. It merely speaks of the foreign court or tribunal "desiring" the testimony of an individual "in relation to" a matter pending before it. I do not think it would be wise to lay down an inflexible rule that admits of no excep-tions. The granting of an order for examination, being discretionary, will depend on the facts and particular circumstances of the individual case. The Court or judge must balance the possible infringement of Canadian sovereignty with the natural desire to assist the courts of justice of a foreign land. It may well be that, depending on the circumstances, a court would be prepared to order an examination even if the evidence were to be used for pre-trial proceedings."[874]

872 *Fecht c. Deloitte & Touche* (1996), 28 O.R. (3d) 188, 194 (Ont. Ct. Gen. Div.) aff'd (1997), 32 O.R. (3d) 417 (C.A.), citing Friction Division Products Inc. v. E. I. Du Pont de Nemours & Co. (No. 2) (1985), 56 O.R. (2d) 722, 732 (Ont. High Ct.), cited in P.D. Pengelley, supra note 8.

873 A more detailed study of these requirements can be found in P. D. Pengelley, supra note 8.

874 *Zingre v. The Queen et al.*, [1981] 2 S.C.R. 392

However, the requirements regarding the relevance and specificity of the requested evidence and the burdensomeness of the order sought may be worth of attention on the part of parties from the United States. Indeed, the threshold for discovery production is generally higher in Canada: "documents which are merely potentially relevant are not properly the subject of Letters Rogatory."[875] As for the level of specificity required, although it may be difficult to determine a precise threshold, it was found that a request for "all documents pertaining to Coopers & Lybrand's audit of Rapid Data's fiscal year 1972 (ending June 30, 1972) financial statement, that refer or relates to the valuation of Rapid Data's inventory for the 1972 fiscal year" was sufficiently specific, given that it was "unlikely that a significantly more exact identification could have been achieved"[876]. Finally, the burdensomeness is assessed by comparison to the burden the witness would have faced if the action was brought in the requested forum. This burden may be mitigated if sufficient resources (time and money) are offered in compensation. "Thus, foreign request for production of evidence may be wide but this does not necessarily make the request unreasonably or unduly onerous"[877].

Legal limitations on discovery

Privacy Laws

In the wake of European Directive 95/46 on the protection of personal data[878], Canada enacted the *Personal Information Protection and Electronic Documents Act*[879] in 2000. Canada's PIPEDA is now fully into effect – its coming into force was sectorial and gradually encompassed health and employee records[880]. This law was drafted and enacted to offer an "adequate protection" in regards of the Directive 95/46. The recognition by the European Commission insures that personal information may freely flow from Europe to Canada without companies having to enter into specific agreements regarding to personal data protection or adding such dispositions in their contracts. The functioning is different from the Safe Harbours agreement between the European Union and the United States, but both regimes are to the same effect in creating a trusted sharing area for personal information. Consequently, information headed out of Canada must be provided adequate protection – be it by being sent to a country for which the EU has determined that data protection meets the Directive 95/46 level of protection, or otherwise, i.e. contractually. This is further established in Principle 4.1.3 of Schedule 1, which states that:

875 *Taft v. Siemens Electric, Ltd.* (2000), 45 C.P.C. (4th) 147 (Ont. Sup. Ct. 2000) para. 15, cited in *Ludmer v. Ludmer,* 2009 QCCA 1414 (CanLII) (application for leave before the Supreme Court dismissed).

876 *Clarkson & Co. v. Rockwell International Corp.* (1979), 11 C.P.C. 228 (Ont. H. Ct.), cited in *Obtaining Discovery Abroad*, supra note 16

877 P.D. Pengelley, supra note 8, p. 371

878 Directive 95/46/CE of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, online, <http://eurlex. europa.eu/Notice.do?mode=dbl&lng1=fr,en&val=307229> (hereinafter "Directive 95/46")

879 S.C. 2000, c. 5 (hereinafter "PIPEDA")

880 PIPEDA, s. 30.

> "[a]n organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party". (our italics)

Blocking Statutes

Blocking statutes are different from data privacy statutes in that they generally have a narrower application, carry more serious consequences and are enacted on the basis of specific national interests.

The main federal blocking statute is the *Foreign Extraterritorial Measures Act*[881]. It was enacted in 1984. Contrary to the first Canadian blocking regulations that were in response to a far-reaching United States law regarding uranium trade, in 1976, the *Foreign Extraterritorial Measures Act* is a permanent and general blocking statute[882]. It sets out the framework within which the government may block the circulation of information outside of Canada. Section 3 thus allows the Attorney General of Canada to make an order when "a foreign tribunal is exercising jurisdiction […] in a manner that […] is likely to adversely affect significant Canadian interests in relation to international trade or commerce […] or is likely to infringe Canadian sovereignty". The only order[883] taken under this aw is regarding the United States's *Cuban Assets Control Regulations*[884].

Ten years after the enactment of an Ontarian law to the same effect[885], Quebec enacted the *Business Concerns Records Act*[886], in response to the perceived extraterritorial reach of United States anti-trust legislation. The act applies to "any account, balance sheet, statement of receipts and expenditure, profit and loss statement, statement of assets and liabilities, inventory, report and any other writing or material forming part of the records or archives of a business concern"[887]. Section 2 of the act states that

> "no person shall, pursuant to or under any requirement issued by any legislative, judicial or administrative authority outside Québec, remove or cause to be removed, or send or cause to be sent, from any place in Québec to a place outside Québec, any document or résumé or digest of any document relating to any concern."

The Supreme Court of Canada had the occasion to review this act in *Hunt v. T&N plc*[888], where a British Columbia citizen asked the court to obtain evidence from the Quebec companies he was suing in British Columbia, whom objected on the basis of the above-mentioned statute. The limitations

881 R.S.C. 1985, c. F-29
882 ABA Section of Antitrust Law, *Obtaining Discovery Abroad* (Chicago, American Bar Association : 2005) p. 101-103.
883 *Foreign Extraterritorial Measures (United States) Order*, 1992, SOR/92-584
884 Code of Federal Regulations, Title 31, Part 515
885 Business Records Protection Act, R.S.O. 1990, c. B.19
886 R.S.Q. c. D-12
887 Id., s. 1 "document".
888 [1993] 4 S.C.R. 289

on the circulation of business records were found unconstitutional on the ground that they violated the division of powers between the provinces and the federal governments, and, generally, "the demands of the structural requirements of the Canadian Constitution"[889] The Supreme court goes on to underline the (im)practical consequences of the statue : "If constitutionally permissible, this approach would effectively immunize the business concerns located in Quebec and Ontario from ever having to produce documents sought for the purposes of litigation in other provinces."[890] The law was thus declared inapplicable to other provinces. The Court was however careful not to decide on the applicability of the law to requests emanating from outside of Canada[891].

Impacts on Electronic Discovery

Reviewing the abovementioned criteria, the practitioner is struck by the many challenges posed by the very nature of the electronic documents. For instance, how does one deal with the requirement that the evidence sought must be located within the jurisdiction of the requested court? In the electronic world, while a company may be headquartered or have a place of business in one location, its servers, and therefore its documents, may reside in a different jurisdiction. This situation is further exacerbated by the advent of cloud computing which can create situations where it is nearly impossible to precisely identify the location of the data.

Other challenges posed by electronic documents with respect to the abovementioned criteria are identified here and commented on as follows:

1. the variety of formats and the capacity of different formats to be different types of documents: In order for the documents sought to be "identified with reasonable specificity", the existing caselaw required that its format (e.g. paper, analogic tape, etc.) or type (e.g. contract, letter, fax, etc.), or both, be mentioned. That was relatively easy to achieve in the "paper world". One can only imagine the shopping list which would be appended to any demand in order to be as specific in the e-world. Fortunately, the use of the word "reasonably" enables the practitioner to liberally interpret the criteria. Accordingly, a list of the period covered, individuals and organisations involved, topics and matters discussed in the documents should satisfy the courts. This information would offer the opportunity for the producing party to make a proportionality and/or reasonable accessibility argument.

889 Id.

890 Id.

891 However, given some remarks by the Court and the evolution of international trade since the Hunt decision, the Quebec law, as it is now written, may well be declared ineffective at the international level, too : "Everybody realizes that the whole point of blocking statutes is not to keep documents in the province, but rather to prevent compliance, and so the success of litigation outside the province that that province finds objectionable. This is no doubt part of sovereign right, but it certainly runs counter to comity. In the political realm it leads to strict retaliatory laws and power struggles. And it discourages international commerce and efficient allocation and conduct of litigation. It has similar effects on the interprovincial level, effects that offend against the basic structure of the Canadian federation."

2. The contextualization of electronic information
   While paper evidence often required testimony to contextualize their existence and content, electronic documents can often be contextualized by themselves, via metadata, or by other electronic information. However, the volume of documents required to understand one particular document clashes with the requirement that "the evidence sought be necessary for trial and be adduced at trial". In other words, in an electronic context, a broadening of this requirement might be necessary to provide the parties and the courts with the necessary context for the documents adduced at trial.

3. The remote accessibility of e-documents
   The necessity for the evidence not to be otherwise obtainable raises an important number of questions. Technology substantially shrunk the notions of space and time by enabling people to gain access to information hosted on remote servers and networks. Accordingly, one can wonder if the ability of a party to remotely access documents prevents it from soliciting the support of the courts to gain access to them. In other words, does the fact that it is possible, thanks to technology, to pose certain acts create an obligation to do them?

4. The poor or inexistent information management
   To us, the most important question that remain to be dealt with by the courts at this stage relates to the requirement that "the order sought not be unduly burdensome,having in mind what the relevant witnesses would be required to do, and produce, were the action to be tried here." Since most organisations are still in a transitional phase, slowly migrating from a paper-based to a server-based environment, while having a foot in the paper and the other one in the paperless world, courts will need to look at their capacity to cost-efficiently access to their documents. In fact, whatt hey will need to look at to objectively assess the burden and its undue nature is the capabilitises of the organisation to find relevant documents compared to what can be expected from similar organisations. Eventually, courts will likely have fairly high expectations, particularly from sophisticated organisations, since proper information management is certainly a normal cost of doing business in the information era.

Canadian Challenges for Foreign Lawyers[892]

Canada is one of these interesting countries where different legal cultures and languages coexist on a vast territory. The clearest example of this situation is the province of Quebec where the main language is French and where civil law applies to the majority of civil and commercial matters brought before the courts.

892 For more details see Stephen Mason, *Electronic Evidence,* Second Edition, Butterworths Law, 2010, pp. 194 and followings.

Language

Since most organisations do business or have offices in Canada's largest provinces, i.e. Ontario and Quebec, when conducting discovery in Canada, chances are you will need to deal with English and French documents. This reality raises a number of practical challenges along the path of the EDRM[893], some of which are included in the following overview:

Identification and Preservation

In order to identify and preserve relevant documents, it is necessary for counsel to identify, amongst other things, the custodians, data sources and document formats. However, in order to achieve that goal, it is often necessary to have in-depth discussions with key players, in the different business units or departments, including the IT group. Unfortunately, many multinational organisations have employees within these units that do not speak English which already generate an important challenge for the lawyers in charge of the case. Under such circumstances, many will think that it is sufficient to rely on Google Translate or a translator to translate, for example, the litigation hold memo to the foreign language. However, such an approach sets aside the fact that much is lost in translation: remember when you were playing Chinese whispers?

Accordingly, the best approach often consists in bringing a bilingual expert to the table to strategize about how best to approach the daunting tasks or identifying and preserving relevant information.

Processing

Besides the technical challenges relating to Unicode, the main challenge faced at the processing stage is the identification of keyword in foreign language: no the dictionary is not enough. As is the case in English, to search and filter appropriately,it is necessary to know the slang and buzzwords used within the organisation within a particular jurisdiction. Furthermore, when it comes to deduplication, most software are unable to identify duplicates, or should we say near duplicates, in a foreign language. Accordingly, a corporate policy that exists in 5 different languages will likely need to be reviewed by 5 different reviewers, with the inherent delays and costs, but perhaps most importantly, risks of divergent relevancy or privilege call.

Review and Analysis

With respect to this phase, we would reiterate the comments made regarding identification, i.e. that translation is no solution. In fact, in many cases, the culture of a jurisdiction is quite important in assessing the relevancy of certain information. Therefore, we recommend that local reviewers be used, under the supervision of a bilingual senior reviewer who ensured the quality control of the English version. This will substantially reduce the risks of incoherent calls.

893 www.edrm.net

Presentation

Based on the best evidence rule, it is always interesting to see litigators, as I witnessed it, argue over the interpretation of a document that was generated from a translation of the original… While recognizing that proportionality may not justify having an interpreter, or even better bilingual lawyers and judges, present during a trial, it is certainly necessary to rely on the original to discuss its relevancy or to interpret it.

Civil vs Common Law

Another important issue facing practitioners is the necessity to deal with different set of rules, including those pertaining to discovery, in the province of Quebec. However, given these differences, experience shows that motions are generally presented in a common law province whenever the party from which one is seeking information does business in Quebec as well as in another province. However, in the instances where the organisation from which one seeks information does business only Quebec, then the rules of civil procedure must be dealt with.While influenced by the common law, the discovery rules are quite different in that relevance is interpreted in a much narrower fashion than in common law jurisdictions. However, as previously mentioned, in the context of a letter of request, the standard of relevance applied by the courts is much narrower and resembles Quebec's. Accordingly, while civil law may appear to be an important challenge, it can often be dealt with fairly easily.

Conclusion

Although the requirements towards letters of request are less strict than they were in the past, Canadian court will not simply "rubberstamp" the letters of requests presented to them. Careful consideration should be given to the drafting of thoserequests, as they could be subjected to judicial review by the Canadian court, with the help of the proposed witness[894]. This is even more important, considering that

> "[i]t is not uncommon for the requesting party to find itself in a situation in which the adverse party to the U.S. litigation does not oppose the application to issue a letter of request, the hearing before the U.S. court is therefore perfunctory, and Canadian counsel for the proposed witness is able, on the application to enforce, to argue that the determination of the U.S. court as to the necessity of the evidence should be given little or no weight"[895].

894 ABA Section of Antitrust Law, *Obtaining Discovery Abroad* (Chicago, American Bar Association : 2005) p. 91.
895 Id.

Is Preservation an Obligation?

by Dominic Jaar
A foreign perspective on Pension Committee

The Pension Committee opinion, aka "Zubulake Revisited: 6 years later", made a lot of noise in the US, mainly because 1) it was written by one of the e-discovery superstar judges (Shira A. Scheindlin), 2) it defines negligence, gross negligence, and willfulness in the discovery context and 3) it reviews the law governing the imposition of sanctions for a party's failure to produce relevant information. However, the most important lesson to be learned from this case has not been mentioned anywhere: many jurisdictions do not officially recognize the duty to preserve!

While recognizing that "Courts cannot and do not expect that any party can meet a standard of perfection", judge Scheindlin stresses that "the courts have a right to expect that litigants and counsel will take the necessary steps to ensure that relevant records are preserved when litigation is reasonably anticipated, and that such records are collected, reviewed, and produced to the opposing party." While this might seem to be a reasonable expectation for a US litigator or judge, it is an assumption that will, in many cases, be defeated by the reality of parties evolving mainly in civil law jurisdictions.

While we can all appreciate that parties suing in the US should apply the *When in Rome* idiom, the take away from this case is certainly that US litigators must be aware of the background and culture of the foreign clients they represent in the US. Otherwise, chances are that sanctions may be imposed against their clients or against them for not having advised their clients properly about the obligations they have in their jurisdiction. Could it be the case here?

Counseling foreign clients

Amongst the thirteen parties involved in this interlocutory proceeding, more than half are Quebec-based organizations. The province of Quebec (Canada) is a civil law jurisdiction which relies mainly on codified rules and explicit laws. While Quebec has codified many aspects of the common law rules of discovery, such as document production and examination on discovery, which otherwise do not exist in strictly civil law countries, it did not explicitly import the common law duty to preserve.

In Quebec, parties must only produce 1) documents that they intend to use at trial and 2) relevant documents requested by the opposing party. With respect to the latter, relevancy is interpreted fairly narrowly as meaning a document that has an evidentiary value in and of itself[896].

Accordingly, in reviewing the types of documents that "should" have been preserved and produced in the Pension case, most Quebec lawyers will tell you that they would not have been deemed relevant in Quebec. Therefore, unless the parties had been clearly instructed by their counsel that they had to preserve these documents and that they had failed to comply with the counsel's instructions, how could they have expected that these documents needed to be preserved, let alone produced?

According to Judge Scheidlin, plaintiff counsel's "instruction does not meet the standard for a

896 Westinghouse Canada, Inc. c. Arkwright Boston Manufacturers Mutual Insurance Company, 1993 Cal LII 4242 (QC C.A.) [http://www.canlii.org/fr/qc/qcca/doc/1993/1993canlii4242/1993canlii4242.html].

litigation hold. It does not direct employees to *preserve* all relevant records - both paper and electronic - nor does it create a mechanism for *collecting* the preserved records so that they can be searched by someone other than the employee. Rather, the directive places total reliance on the employee to search and select what that employee believed to be responsive records without any supervision from Counsel." While I do not share judge Scheindlin's view that a party must "create a mechanism for *collecting* the preserved records so that they can be searched by someone other than the employee" [this could be the topic of a complete article], relying on the preservation and production efforts she summarizes, I do share her view that the instruction did not seem to meet the standard. However, one can certainly ask, under such circumstances, why are the parties, and not the counsel, sanctioned? Furthermore, how could counsel objectively represent their clients for such a motion?

Ensuring the implementation of the opposing party's litigation hold

Besides blaming the plaintiffs' counsel, I am intrigued by the absence of any reference to a litigation hold letter being sent by the defendants to the plaintiff. While we can all appreciate that there is a common law duty to preserve, isn't it fair to expect parties in a litigation to clearly and in due course, i.e. while it is still time, to proactively identify document types and content they are expecting to be produced, or at least preserved? Wouldn't this be part of the collaborative culture sought by the FRCP and The Sedona Principles? If this is the case, as I hope, what is the impact of failing to send such a detailed litigation hold to the opposing party? Could we apply the rules covering the obligation of a party to mitigate its damages?

Exporting the duty to preserve

For US counsel representing or suing foreign organizations, there are a number of ways to prevent Zubulake from being re-revisited a number of years later:

As plaintiff counsel representing foreign interests, you should:

1. Inform your client, in writing, about the duty to preserve in the US and its scope in your particular case by identifying the targeted :
   a. Custodians
   b. Systems and technology
   c. Document types and formats
2. Provide an internal litigation hold memo detailing what custodians must do and how it should be done
3. Ensure your client understands, and audit compliance

As counsel defending against a foreign organization, you should:

1. Send a detailed litigation hold letter to the plaintiff and its US counsel
2. When there is no US counsel, the letter should summarize the expectations regarding preservation (perhaps appending the Pension Case?) or invite the party to seek legal advice from a US-savvy counsel
3. In some cases, and in some jurisdictions, it may be safer to seek a preservation order from a local court to ensure the execution of the final judgment in case of sanction

*** Dominic Jaar is a Quebec-based Canadian lawyer. He is the Associate Partner in charge of the Canadian e-discovery and information management services of KPMG, since the acquisition of his firm, Ledjit Consulting. Prior to founding his firm, he practiced as a commercial litigator in one of Canada's largest law firm and as an in-house counsel at Bell Canada. He is on the editorial board of Sedona Canada and a member of different working groups of The Sedona Conference.*

e-Discovery and Trade Secrets Law: Limitations on Discovery

by Scott A. Carlson and Patrick E. Zeller
Copyright Volume 2, Number 4, March/April 2010, by Landslide Magazine. Reprinted with permission.

Discovery requests can often seem to border on being overly intrusive and to go beyond the scope of the dispute. That intrusiveness, however, reaches a higher level when an opponent seeks to obtain information that may include trade secrets, proprietary content, or other sensitive information. Intrusiveness can peak when a party seeks discovery through the use of an inspection of another party's computer system, often through a request for a forensic image of a hard drive. In the trade secrets litigation context, this presents an extraordinary challenge. On one hand, the party requesting the inspection is often looking for its own trade secrets and related evidence located on its opponent's computers. But inevitably the opponent will say, "Wait a minute: *our* trade secrets are on there," and it will not want the computers inspected. Such is the tension faced when e-discovery law meets trade secrets law.

Forensic Inspections

Requests for inspections of computer systems or electronically stored information (ESI) arise in many ways. Some inspections simply seek access to a system to perform general searches for files. Others may be more intrusive and may request a forensic copy of a laptop hard drive or server. These forensic copies are typically a complete copy of the entire hard drive and are known by many names including mirror images, forensic images, complete images, bit-stream images, or bit-stream copies. All of these forensic copies cover the entire contents of the hard drive, including, generally: (1) the files created by a user (word processing files, e-mail, spreadsheets, etc.); (2) files that run the various applications, programs, and operating system on the computer, including log files, Internet history, etc.; and (3) information related to files that have been "deleted," including the potential recovery of partial or complete copies of deleted files.

These "deleted" files exist because of the manner in which computer operating systems store files. When files are deleted by a user, they are not removed from the hard drive; instead, the operating system simply no longer keeps track of them. Over time, these deleted files may be overwritten completely or in part because of the addition of new files and continued use of the computer involved. Often these "deleted" files are of interest in trade secrets and other types of litigation, and these files can only be obtained through a computer forensic examination.

Before the 2006 Amendments to the Federal Rules of Civil Procedure

Traditionally, most litigators thought of Rule 34 inspections as mechanisms to inspect property to perhaps photograph or take measurements at the site of an accident, for example. Alternatively, an inspection request might be used to allow expert to inspect a vehicle involved in an accident. In the earliest days of Rule 34, few would have contemplated "inspecting a computer hard drive." That being said, Rule 34 has long provided a mechanism for a party to obtain an inspection of certain iems,

including "data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form. . . ."[897]

Prior to the 2006 amendments to the Federal Rules of Civil Procedure, courts struggled with how to handle Rule 34 requests when it came to computer hard drives. When faced with Rule 34 inspections, a computer hard drive was typically viewed in one of two ways: (1) as simply a "tangible thing" and it was, therefore, subject to inspection under the plain language of the rule, or (2) it was the functional equivalent of a filing cabinet and should only be subject to inspection in limited circumstances.

For example, in *Advante Int'l Corp. v. Mintel Learning Tech.*,[898] the defendant Mintel accused the plaintiff Advante of withholding, concealing, or destroying evidence and filed a motion to compel for authorization to examine Advante's computer systems. The court began by noting that "electronic storage of information presents discovery issues not encountered in earlier times" but noted that it is well settled that "electronic evidence is no less discoverable than paper evidence."[899] The court acknowledged that inspection of hard drives may be appropriate in some cases but denied defendant Mintel's motion to compel.

> The mere fact that this case involves electronic data does not change the basic concepts or rules of the discovery process. Had Mintel made the same basic accusations in an earlier age, its claims of incomplete document production, inconsistencies, or even perjuring destruction of evidence, would not automatically entitle it to an order permitting it to enter Advante's offices to rummage through filing cabinets and desks. The relief Mintel is asking for here is no different and not more warranted.[900]

Also, defendant Mintel had not presented any concreteevidence of its allegations of discovery misconduct. Thus, the court denied the motion to compel.[901]

After the 2006 Amendments to the Federal Rulesof Civil Procedure

As part of the 2006 Amendments to the Federal Rules of Civil Procedure (the so-called e-discovery amendments), the Advisory Committee noted the inherent tensions associated with the inspection of hard drives containing ESI. Specifically, the Advisory Committee noted that

> [i]nspection or testing of certain types of electronically stored information of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents

897 Fed. R. Civ. P. 34.

898 2006 WL 1806151 (N.D. Cal. June 29, 2006).

899 *Id.* at 1.

900 *Id.*

901 Later, after Mintel presented evidence that some e-mails had been tampered with, the court granted Mintel's motion to examine Advante's systems, provided the parties agreed on a protocol for producing and disclosing any resulting information. Advante Int'l Corp. v. Mintel Learning Tech., 2006 WL 3371576 (N.D. Cal. Nov. 21, 2006).

> and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from the inspection or testing such system.[902]

Essentially, one cannot substitute a request for documents with a request for an inspection that would allow a party to send in an expert to routinely perform its own searches for documents. Put another way, courts should proceed with caution when considering providing a party with a right to the electronic equivalent of rifling through its opponent's office file cabinets—which is often the electronic equivalent of rooms full of file cabinets that contain both relevant and irrelevant information.

That being said, trade secrets cases are among those that often *do* require an inspection of a hard drive. The reason is that often it is not just the particular word processing document or e-mail that is important to a trade secrets case. Instead, trade secrets cases typically are won or lost on evidence about "how" a particular computer was used, not "what" documents are on it. For example, a forensic inspection may produce evidence that a CD had been burned on a particular day and that system logs show files containing trade secrets were copied onto a CD and deleted from the original laptop. Or it may show that an employee, just prior to quitting to join a competitor, utilized his company laptop to upload his former employer's proprietary information onto a thumb drive, USB drive, or another computer network. In other cases the inspection may show that sensitive information was copied from company servers to a company laptop but then quickly deleted to give the appearance the files were never downloaded and never existed on the laptop. All of these types of evidence, as well a plethora of other kinds of evidence, can be obtained through a forensic examination of an opponent's computer hard drive and may be the most critical evidence in a case.

Limiting Discovery and Protecting Trade Secrets and Other Information During Inspection

Courts and parties are continually seeking to strike a balance between the need for discovery of ESI and the need to protect against unnecessary access to irrelevant but often proprietary and sensitive information, including trade secrets. As the type of information and the technology involved change from case to case, so must the balance of discovery and protection change. Focusing only on technology, the balance struck in allowing access to a single workstation may change when that workstation is connected to a large network. Concerns associated with the inspection of a single hard drive may be dramatically different than those associated with the inspection of a server. Additional issues may arise when a party wants to look at a hard drive that is also the entry point for a person to utilize social networking sites, personal e-mail, or information contained in "the cloud" of remote computer systems.[903]

---

902 Fed. R. Civ. P.34, Advisory Comm. Notes.

903 Defining "the cloud" is well outside the scope of this article and would take a book to explain. However, in the broadest terms "the cloud" refers to a shift in the concept of computer storage from local controlled servers to storage places on the Internet ("in the cloud") that are accessed through a web browser with the user not knowing precisely where his or her data are stored.

Regardless of the technologies or the requests, courts and parties are often dissatisfied with a simple granting or denying of a particular request. Instead, a proper balancing of interests often leads to defined limitations on an inspection request. None of the limitations identified below are perfect solutions, and each must be considered based upon the facts in any particular case. These limitations hopefully do, however, provide a starting point for crafting the appropriate limitations for any particular matter given both the technology at issue and the information sought.

Protective Orders

Perhaps the simplest, and also perhaps the most dissatisfying, limitation on an inspection is the protective order. Parties can simply be told, "Don't worry; we'll enter a protective order and then whatever the inspector finds will be protected." While protective orders are common and sometimes are effective, they are inherently limited because of their focus on what one "does" with the information found, as opposed to "access" to the information in the first place. But courts are highly motivated to move in this direction—the idea of a protective order is simple and judges understand them. And in many cases, there is no way to place limitations on the scope of an inspection: allyou can do is put in place a protective order.

Independent Experts

Some courts have sought to limit inspections through the use of an independent expert. The precise application of this approach can and has varied widely in different cases, but it has certain common elements. First, it contemplates an expert who is engaged by and reports to the court, as opposed to the parties. Second, it necessarily requires a fairly precise notion of what the expert will be searching for. Third, it requires a considerable amount of the court's time and attention in managing the inspection and sometimes even involves the review of material and providing the results to the parties; these factors can cause courts to contemplate the appointment of a special master. The demands associated with the use of an independent expert are not often easily met or recognize at the time the independent expert is appointed.

Probably the most cited case supporting the use of a courtappointed forensic expert is *Playboy Enterprises, Inc. v. Welles.*[904] In that case, the court accepted the notion that e-mail messages might be able to be recovered through the inspection of a forensic image of the defendant's computer.[905] The court's order indicated that it would appoint an expert, that the expert would sign a protective order, and that any disclosure as a result of reviewing the information on the hard drive would not waive the attorney-client privilege if that privilege applied to the disclosed material.[906] The expert would image the hard drive and search for e-mails that could be recovered, which would then be provided to defendant's counsel to review for further production.[907]

904 60 F.Supp. 2d 1050 (S.D. Ca., 1999).
905 *Id*. at 1054.
906 *Id*. at 1055.
907 *Id*.

Limiting Inspection

Another method courts and parties have used to constrain access to electronic records is to attempt to "limit" or "define" the scope of an inspection. In some cases, a requesting party has been required to revise its request to specify a narrower and less intrusive request. Under pressure from a court, a litigant can sometimes fashion a particular search protocol that truly focuses on the relevant information.

For example, in *MSC Software Corp. v. Altair Engineering, Inc.*,[908] plaintiff MSC asked an individual defendant to produce "all hard drives, thumb drives, or USB drives from any and all personal (non-Altair) computers for inspection and imaging."[909] Notwithstanding the broad request, what MSC was actually seeking was the contents of a specific folder from the defendant's computers that might have been contained on these hard drives, thumb drives, or USB devices.[910] The individual defendant provided MSC the contents of the folder but would not give MSC access to the drive itself because it contained confidential information.[911]The court found that forensic imaging was inappropriate due to the sensitive nature of the case and MSC's overly broad discovery request.[912] The court did allow, however, a limited inspection in which defendant Altair's expert was to examine the hard drive for the folder itself and then provide the results designated as "Attorney's Eyes Only."[913]

Yet another example arose in *Sterle v. Elizabeth Arden, Inc.*[914] In that case, plaintiff Sterle sued defendant Arden alleging wrongful termination in violation of the Age Discrimination in Employment Act of 1967 (ADEA).[915] Plaintiff sought production of certain employee ranking reports that counsel for Arden had claimed could not be located.[916] In light of the failure to locate the records, the court issued an inspection order for a forensic computer consultant to inspect the defendant's computers.[917] The parties disagreed over how the consultant was to conduct the inspection and, when the consultant arrived to conduct the inspection, he was denied access to many areas of the computer system.[918] Counsel for Arden then filed a motion for a protective order to prevent the inspection of the defendant's computer system based largely on a theory that the plaintiff's attorney's instructions to the consultant threatened Arden's private or privileged information.[919] The court rejected this argument and found that Arden had not established good cause for a protective order, as the inspection order was drafted so that relevant information could be found and content and time limits were imposed

908 2008 U.S. Dist. Lexis 105570 (E.D. Mich. Dec. 22, 2008).
909 *Id.* at 21.
910 *Id.* at 21-22.
911 *Id.* at 22.
912 *Id.*
913 *Id.*
914 2008 WL 961216 (D.Conn. Apr. 9, 2008).
915 *Id* at 1.
916 *Id.*
917 *Id.*
918 *Id.* at 3.
919 *Id.* at 6.

to limit the inspection to searches for the missing reports and only for the year prior to the plaintiff's termination.[920]

Defined Court-Ordered Searches

If there are limits that can be imposed to properly balance the interests of the parties, it is important to make clear what the protocol is that will be used. In some instances, an appropriate balance might lead to a court ordering a party to conduct a particular search of its own computers and to provide the search results to its opponent. This approach has some appeal in cases where the disclosure of the underlying information is particularly problematic and the material sought can be clearly identified.

For example, in *Daimler Truck North America, LLC v. Younessi,*[921] plaintiff Daimler sued a former executive for breach of the duty of loyalty, breach of a confidentiality contract, and common law duty not to convert confidential and proprietary information. Daimler had requested to search Cascadia's computers for communications between Younessi (defendant and former employee) and Hebe (former CEO of both Daimler and Cascadia).[922] Cascadia asserted that the subpoena calling for this search was unduly burdensome and would require disclosing trade secrets to a competitor.[923] Upon balancing Cascadia's interest in maintaining its trade secrets against Daimler's interest in prosecuting its case, the court determined that discovery was warranted and denied Cascadia's motion to quash in part.[924] The court looked to *Playboy Enterprises, Inc. v. Welles*[925] for guidance on how to handle the search and protect Cascadia's trade secrets. The court ordered Cascadia to search its *own* computers, rather than to produce them for copying, because Daimler was a direct competitor and Cascadia was a third party to the suit.[926]

Special Considerations for Subpoenas

As noted in the Daimler case above, inspections for ESI can be obtained through the use of a Rule 45 subpoena. However, as with any subpoena, in addition to the general tension associated with inspections, inspections of nonparties should raise heightened concerns for the burdens placed on the nonparties. The 2006 Advisory Committee Notes to Rule 45 provide as follows:

> Rule 45(a)(1)(B) is also amended, as is Rule 34(a), to provide that a subpoena is available to permit testing and sampling as well as inspection and copying. As in Rule 34, this change recognizes that on occasion the opportunity to perform testing or sampling may be important, both for documents and for electronically stored information. Because

920 *Id.*
921 2008 WL 4791654 (E.D. Pa. Nov. 3, 2008).
922 *Id.* at 1.
923 *Id.*
924 *Id.* at 2.
925 60 F.Supp. 2d 1050 (S.D. Cal. 1999).
926 *Younessi,* 2008 WL 2519845, at 4.

> testing or sampling ay present particular issues of burden or intrusion for the person served with the subpoena, however, the protective provisions of Rule 45(c) should be enforced with vigilance when such demands are made. Inspection or testing of certain types of electronically stored information or of a person's electronic information system may raise issues of confidentiality or privacy. The addition of sampling and testing to Rule 45(a) with regard to documents and electronically stored information is not meant to create a routine right of directaccess to a person's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.[927]

In *Integrated Service Solutions, Inc. v. Rodman,*[928] plaintiffIntegrated Service Solutions, Inc. (ISS) served nonparty VWR with a subpoena that included all VWR computers. In particular, ISS sought a VWR laptop that was assigned to defendant Dennis Rodman's wife while she worked for VWR and that Dennis Rodman used during the time.[929] VWR, one of ISS's competitors, voiced concerns over giving ISS "direct access" to its IT system, and over the subpoena's reach into VWR's confidential information.[930] Accordingly, VWR offered to conduct the search itself or have a third-party expert perform the search, and the parties agreed to have PricewaterhouseCoopers (PWC) conduct the search.[931] PWC performed the analysis based on an ISS "checklist" and billed ISS.[932] PWC submitted the search hits to VWR counsel, who concluded they were not relevant to the litigation.[933] VWR counsel informed ISS that the analysis was complete and that (1) there was no evidence of wiping on the drive, (2) most of the search terms did not result in hits, and (3) none of the hits were relevant to the litigation.[934]

As a result of what was apparently a sufficiently vague protocol, ISS then sought an order compelling VWR to produce a full report from PWC and provide direct access to the files identified in the search.[935] Ultimately, the court concluded the parties had not agreed that ISS would obtain the files regardless of relevance and found nothing to indicate bad faith or unreliability on VWR's part or to suggest that VWR was withholding relevant evidence.[936] Thus, the court denied ISS access to the files, stating, "[w]e will not require this nonparty, VWR, to permit ISS to thumb through an electronic file drawer to double-check VWR's document review on this point."[937] But the court did

927 Fed. R. Civ. P. 45, cmt. (2006).
928 2008 WL 4791654 (E.D. Pa. Nov. 3, 2008).
929 *Id.* at 2.
930 *Id.*
931 *Id.*
932 *Id.*
933 *Id.* at 3.
934 *Id.*
935 *Id.*
936 *Id.*
937 *Id.* at 4.

allow ISS to seek,through VWR, a report of the search from PWC "to confirm the search terms were applied properly."[938]

In *Gonzales v. Google, Inc.*,[939] a civil action had been filed against the U.S. attorney general challenging the constitutionality of the Child Online Protection Act. Thereafter the attorney general subpoenaed Google seeking all the URLs in its database and then, in a later version of the subpoena, just a sampling of the URLs.[940] The subpoena also initially sought all search queries entered on the search engine for 60 days, ut it was later narrowed to a one-week period. The purpose of the subpoena was to collect information for a study on the effectiveness of filtering and blocking software.[941] Among other concerns, Google objected that trade secrets would be disclosed. The court acknowledged that a statistically significant sample from Google's index "may permit competitors to estimate information about Google's indexing methods or Google's users."[942] The court determined that the government demonstrated a substantial need for the information from Google based on its market share but not for disclosure of both the URLs and search queries. Thus the court granted a otion to compel only as to the 50,000 URLs and issued a protective order for the information submitted by Google.[943]

Conclusion

Inspection of computer systems and electronically stored information is an important part of the civil discovery process. While the balancing of interests between the right to relevant information and the risk of disclosure of sensitive nonrelevant information is complex, the courts have sufficient flexibility to balance those interests. The difficulties lie n clearly identifying the information sought and understanding the technology involved to fashion appropriate limitations on discovery steps. Courts have limited time and resources, and parties will proceed optimally if they effectively define appropriate discovery limitations and, perhaps more importantly, clearly explain the material discovery and trade secret issues to courts overseeing discovery processes.

Scott A. Carlson is the founder and chair of Seyfarth Shaw's national e-discovery practice group. Mr. Carlson advises clients on a broad array of e-discovery and related issues, utilizing his experience as a litigator along with his technical background, which includes a B.S. in Computer Science and Mathematics. He can be reached at scarlson@seyfarth.com.

Patrick E. Zeller is vice president and deputy general counsel for Guidance Software, Inc. He writes and speaks regularly on topics related to e-discovery, digital vidence, and the intersection of law and technology. He can be reached at patrick.zeller@guidancesoftware.com. Mr. Carlson and Mr. Zeller are both adjunct professors at The John Marshall Law School, where they teach a course entitled E-Discovery, Computer Forensics, and Digital Evidence.

938 *Id.*
939 234 F.R.D. 674 (N.D. Cal. 2008).
940 *Id.* at 678.
941 *Id.* at 679.
942 *Id.* at 684.
943 *Id.* at 686-87.

CISO Profiles rise as their reach extends into Legal

by Patrick Burke, Assistant General Counsel at Guidance Software, Inc.
Copyright London City Security. Reprinted with permission.

With corporation's lawyers increasingly reliant on ready access to the company's digital information, CISOs who work closely with Legal find their roles expanded and their corporate profile raised.

Legal departments at major corporations are increasingly reliant on ready access to their companies' digital information. Without the ability to locate and collect large amounts of data\ that resides on the company's laptops, workstations and servers, a company's lawyers now find they are unable to effectively advise management on legal questions, defend the company in litigation, advise on the company's rights under contracts with other companies, investigate HR issues or satisfy regulators.

In short, the lawyers have developed a growing dependency on the Chief Information Security Officer ("CISO"). The CISO and the Information Security ("IS") team are the people with the authorisation, ability and tools to search the company's data, collect what the lawyers need, and deliver it to them in a usable format. Given the range of legal matters at issue – including some "bet the company" investigations or litigations at some companies – this dependency is expanding the mission of IS and raising the profile of CISOs.

The fit between Legal and IS is symbiotic, natural and nothing new. IS at most companies traditionally has included in-house investigatory capacities. IS investigators frequently investigate matters at the behest of the Legal and HR departments such as IP theft, fraud, sexual harassment or other illegalities. Typically IS investigators come from backgrounds in law enforcement and are practiced in handling electronic evidence with attention to the chain of custody required by courts.

What is different is the scope sheer amounts of data required for the wide range of legal matters, and the increase in data maintained overall by companies and their employees.

Employee laptops alone often hold 40 gigabytes of data on their hard drives, with newer models holding a multiple of that amount. The data on just a dozen of those computers can amount to a terabyte of potential evidence, which is the equivalent of over 60 million pages of hard copy information. Document requests from the FSA, OFT, SEC or European Competition Commission can run beyond gigabytes into terabytes of data. Legal's hunger for data can be even greater when it comes to major litigation or exchange of due diligence materials required in mergers and acquisitions.

Savvy CISOs leverage their access to corporate data into a strategic relationship with Legal. They do this by demonstrating they understand Legal's requirements and can deliver on them. The relationships are strongest with Legal when the CISO puts in place:

- Strong communication with Legal. Some companies form "working groups" that facilitate planning, coordination and trust. IS should select representatives who are not put off by lawyers or how they communicate.
- Technology capable of efficiently searching, locating and collecting data from every single server, workstation and laptop in the company. Enterprise-wide solutions that automate data collection (including metadata) usually also provide the logging and documentation

that may be crucial to the lawyers at a later date. Having a common platform to support electronic disclosure, regulatory collections, internal fraud investigations, computer security incident response, internal audit, and other key processes allows the company to dramatically reduce the cost per activity by amortising the cost of the platform over many different events, minimizing the employee training required, and reducing the amount of outsourcing to expensive consultants.

- Strong project management. Smart project management not only gets the job done efficiently, but keeps an eye on documentation in a way that reassures courts and regulators.
- Processes that are defensible and repeatable. Ad hoc approaches to data collection increase doubt and suspicion by lawyers, courts and regulators. Repeatable process increase IS's ability to ensure compliance with best practices, rules of evidence and data protection laws.

Each of these elements is best accomplished by IS staff rather than outsource bureaus. Yet company lawyers frequently will turn to their law firms or to outside consultants if they do not believe that IS has the expertise. Sometimes IS can contribute to the impression that it is not comfortable with an expanded role.

The arguments are compelling for a company's IS staff over outsourced alternatives. The strongest argument is the cost savings – in-house systemised processes efficient and cost effective. Common sense dictates that IS is better positioned to implement defensible and repeatable processes involving the company's data because they work with that data every day, rather than consultants who work on a project basis.

Assigning data search and collection to IS also makes sense because corporate information security professionals already are generally well-versed in computer investigations. Many have computer forensics training and tools and routinely access and investigate systems to identify and collect data for security and investigative reasons. Further, a systemised process executed with plugged-in enterprise tools and run by a well-trained internal team that is very familiar with the organisation's IT infrastructure and that works alongside corporate legal is generally more advantageous from a compliance standpoint.

Finally, IS already have existing reason to be equipped with software that enables keyword and time-frame searching of all the company's email as well as all electronic documents on the companies' laptops, workstations and servers.

The expanding data needs of Legal present CISOs with an opportunity to raise their profile and increase their authority and budget. They are best positioned to step into this role, but must capitalise on this opportunity by developing strong connections with Legal and implementing defensible and repeatable inhouse processes supported by strong project managers equipped with efficient enterprise search and collection software.

Computer Forensics v. E-Discovery

by John M. Patzakis and Patrick J. Burke
Copyright May 2008 by the New York Law Journal. Reprinted with permission

Computer forensics is the application of computer investigation techniques to collect, analyze and authenticate electronic evidence in a manner that meets even the high standards of proof in criminal prosecutions. Computer forensics investigations, typically involving one or a few hard drives, are about determining exactly what happened on a computer and who was responsible for it.

Electronic discovery is the process of identifying, preserving, reviewing and producing electronically stored information (ESI) relevant to a lawsuit. Unlike its techno-flashy forensics relative, e-discovery is generally a broader and more systemic effort to collect relevant ESI from multiple custodians and data sources within an organization.

On the other hand, routine e-discovery preservation still requires good faith efforts, where some aspects of traditional forensics such as maintaining a good chain of custody, metadata recovery and preservation, documentation and reporting and an overall defendable process are required. It is no surprise, then, that corporate counsel often struggle to determine the appropriate methodology for ESI preservation and collection.

Are full-disk images[944] of every custodian's hard drive necessary? What are the real risks of not employing proper processes? What are the benefits and proper role of computer forensics in the e-discovery collection equation? How can corporate counsel leverage internal computer forensics resources to reduce costs instead of increasing them?

Our company, Guidance Software, is the developer of EnCase, computer forensics software used by law enforcement and e-discovery consultants alike.[945] While Guidance did not invent full disk imaging, we believe the company was instrumental in commercializing the practice.

With that background, one would think we would encourage full disk imaging as standard protocol for e-discovery collections. However, that is not the case. We believe that full disk imaging for ediscovery purposes is used much too often, perhaps due to confusion among in-house lawyers and their outside counsel as to alternative options. In particular, technology exists for what we refer to as a hybrid model, which takes parts from both computer forensics and e-discovery methods and uses. It is that hybrid method that this article will describe.

Mitigate Risk or Reduce Costs?

In the context of e-discovery, computer forensics imaging and deep analysis may be necessary in some circumstances such as in the case of suspected spoliation, fraud or trade secret theft. However, routine

944 A full disk Image, also referred to as a "mirror image," is "an exact duplicate of the entire hard drive, and includes all the scattered clusters of the active and deleted files and the slack and free space." *U.S. v. Triumph Capital Group Inc.*, 211 F.R.O. 31,48 (D.Conn.2002).

945 See *Sanders v. State*, 191 S.W.3rd 272 (fex.App., 2006), cert. denied, 127 S.Ct. 1141 (court takes judicial notice of the reliability of EnCase, finding that "EnCase is a 'field standard' for forensic computer examination.").

full-disk imaging is unwarranted for e-discovery due to considerable costs and burden. Large-scale full disk imaging can be onerous because it is disruptive, time consuming and expensive.

It is very expensive because forensic disk-imaging involves manually copying every bit of data on the hard drive. This process generally requires extensive labor hours (travel, interviews and imaging with forensic tools) and also results in substantial over-collection. With e-discovery service providers charging processing costs up to $2,000 per gigabyte, it is not uncommon for service providers to tally $50,000 or more for the forensic collection and processing of a single hard drive.

However, many litigants choose this option out of fear of spoliation or other forms of discovery non~compliance. According to the 2007 Socha-Gelbmann 5th Annual Electronic Discovery Survey (Socha Consulting LLC & Gelbmann & Associates), computer forensics software tools were the ones most widely owned and utilized for e-discovery purposes by service providers who responded to the survey. One reason litigants and their counsel tend to overly rely on full disk imaging is the perception that no other defensible means of data collection is feasible. With hourly and processing costs as high as they are, many service providers do not discourage this practice either.

Nonetheless, there currently is no known case law requiring full-disk imaging as a routine means of collecting ESI for civil discovery. To the contrary, several recent decisions provide that forensic mirror image copies of computer hard drives are not generally required for e-discovery production.[946] These cases invoke the well established rule that the duty to preserve ESI only extends to relevant information.[947]

On the other end of the spectrum, some litigants, deterred by associated costs and burden of full disk imaging, press the preservation compliance envelope and exercise what they approximate to be the minimal effort required to pass the reasonableness test. A notable example of this is the surprisingly popular but very questionable practice of custodian self-collection.

While courts are clear that deep dive forensics analysis is the exception rather than the norm for e-discovery, ESI collection and preservation must, as noted above, incorporate a defensible process that accomplishes the objective of identifying, preserving and collecting relevant data, including metadata, and establishing a proper chain of custody. Among the several dozen published decisions involving the imposition of sanctions due to e-discovery errors and omissions, the clear majority of those involve ESI preservation failures. Preservation and collection is where most of the e-discovery risk lies.

To be sure, the practice of allowing custodians to identify, preserve, search and collect their own ESI has drawn extensive scrutiny from courts in the past two years. Oftentimes companies will merely

946 *Diepenhorst v. City of Battle Creek*, 2006 WL 1851243 at *3 (W.O. Mich. June 30, 2006 ("Imaging a hard drive results in the production of massive amounts of irrelevant, and perhaps privileged information."); *Balfour Beatty Rail Inc. v. Vaccarello*, 2007 WL 169628 (M.O. Fla. 2007) (Court rejects discovery request for production of caples of hard drives as overbroad and unwarranted).

947 *Zubulake v. UBS Warburg UC*, 220 F.R.O. 212, 217 (SONY 2004) (no duty exists to "preserve every shred of paper, every email or electronic document and every backup tape .... Such a rule would cripple large corporations.").

issue a written preservation notice to potential custodians, yet leave it to those individuals to self-comply. As evidenced by several recent decisions, this is a recipe for disaster.[948]

In fact, at least one court has determined that relying on custodian self-collection is not only negligent, but in fact facilitates spoliation. In *In re Hawaiian Airlines Inc,.*[949] the defendant Mesa Air Group sent a preservation hold notice to its CFO, who was a principal witness in the case. Instead of preserving evidence, the CFO responded to the notice by deleting files and wiping his laptops.

Ultimately, the court determined that Mesa Air Group could have taken reasonable steps to prevent or mitigate the CFO's spoliation, such as copying the data from his hard drives.

"Instead, Mesa shnply told Mr. Murnane to preserve all evidence and trusted him to comply."[950] The court further noted that "Because Mesa failed to take such steps, Mesa facilitated (the CFO's) misconduct."[951] Consequently, the company was sanctioned with an adverse inference instruction.

The Third, Hybrid Option

So with it being established that routine full disk imaging goes too far, yet custodian self collection is fraught with serious risk, what is the best course of action for large organizations?

Many have answered this question by adopting a hybrid network-based computer collection model that is scalable and targeted yet maintains basic computer forensics protocols and associated defensibility.

An effective enterprise-scale computer evidence and collection capability is one that can identify, search, preserve and collect relevant ESI belonging to identified custodians across the network in a targeted manner while preserving metadata and maintaining a solid chain of custody, and generating detailed reports. Such a process, an efficient intersection of computer forensics and IT expediency, addresses the data that needs to be collected in a highly defensible manner without resorting to the burdensome overcollection caused by full disk imaging. In fact, an effective e-discovery collection process is one that will both facilitate compliance while substantially reducing costs.

Divergence and Re-Convergence

Until recently, the use of computer forensics tools for e-discovery was generally limited to full disk imaging of computer systems and initial culling of files. Because traditional computer forensics analysis involved keyword searches and other analysis across the entire collected drive image (including

948 See *Samsung Electronics v. Rambus*, 439 F.Supp.2d 524, 565 (E.O. Va. 2006) ("[i]t is not sufficient .. .for a company merely to tell employees to 'save relevant documents' ... this sort of token effort will hardly ever suffice."); *Cache La Poudre Feeds, UC v. Land O'Lakes Inc*., 244 F.R.O. 614 (D.Colo. 2007) (Court faults Land O'Lakes for simply directing employees to produce relevant information, and then relying upon those same employees to exercise their discretion to determine what information to save); *Google Inc. v. Am. Blind & Wallpaper Factory Inc*., 2007 WL 1848665 (N.O. Cal. June 27, 2007) (Mere transmission of written hold notifications to custodians and tracking of their acknowledgements held insufficient):

949 2007 WL 3172642 (Bkrtcy. D.Hawaii Oct 30, 2007).

950 *In re Hawaiian Airlines,* supra, 2007 WL 3172642, at *5.

951 Id.

deleted files and slack space) e-discovery practitioners choose to perform the bulk of their processing and analysis work by exporting the forensically collected ESI into specialized e-discovery processing tools and attorney review platforms.

This key step represented a clear separation point from computer forensics and e-discovery. However, this route had its own limitations, as those e-discovery tools were not adept at preserving file metadata and native file formats, dealing with unique file types, or maintaining an automated chain of custody.

As a result, e-discovery support professionals adapted processing methodologies that required extensive manual data massaging, ad hoc exception handling, detailed quality assurance, and very skillful project management. For instance, importing ESI into an e-discovery processing tool typically requires "metadata extraction" which involves manually logging the corresponding file metadata into a database and then re-inserting the metadata into a load file as the ESI migrates from the processing to review stage. These onerous and manual efforts are mainly why e-discovery processing costs are so high. According to Forrester Research, processing represents the single highest element costs charged by e-discovery service vendors.[952]

To address this broken process, the more recent generations of computer forensics tools have evolved in two important ways.

First, forensic data collection no longer necessitates full disk imaging. The leading computer forensics technologies can now collect ESI over a corporate network on a file by file basis. This enables the responding party to search (including by keyword), filter and cull ESI at the point of collection and only retrieve what is potentially relevant.

While more narrowly tailored, the process is systemic and transparent as uniform search criteria are objectively applied across the data stores of all identified custodians, with detailed reporting for chain of custody and process documentation. Further, because core technology is computer forensics, file metadata and native formats are kept intact.

The second important recent advancement in computer forensics technology is the integration of processing functionality. Once ESI is collected, the same computer forensics tool is used to cull, filter, deduplicate and index the data for secondary searching. Finally an attorney review platform load file is generated on an automated basis by the same computer forensics platform. This important step is further streamlined by the new EDRM XML standard load file format collectively developed by the e-discovery industry.

This integration of targeted forensic file collection and traditional e-discovery processing is a major improvement that is resulting in a much more streamlinedand cost-effective capability for major organizations. Computer forensics practitioners within larger organizations are able to address the e-discovery process in a more holistic manner through the point of attorney review. Those organizations that adapt this approach are able to realize substantial cost savings as they are able to reduce or even eliminate expensive e-discovery outsourcing and processing costs. Better yet, at the

952 Barry Murphy, "Believe It-E-Discovery Technology Spending to Top $4.8 Billion by 2011," Forester Reasearch, Dec. 12, 2006.

same time those organizations do not compromise but in fact enhance the effectiveness and thus the defensibility of their internal e-discovery process.

Multiple Compliance Processes

Finally, when an organization establishes a network enabled computer forensics capability, another key benefit is that capability can be leveraged to address multiple priority compliance investigation requirements.

For instance, effective fraud and risk mitigation controls require effective internal investigation, which most often involves digital evidence. In fact, litigation may often arise from a matter that first involves an internal investigation. Addressing internal and perhaps Sarbanes-Oxley investigation requirements with the same platform to conduct e-discovery brings tremendous efficiencies and other advantages.

Identifying, mitigating and containing the leakage of customer privacy data, intellectual property and other confidential data is a major compliance concern amongst senior executives. With the same technology used to execute e-discovery searches and litigation holds, routine audits to search for social security numbers, credit card numbers or various forms of proprietary information can be performed on up to hundreds of desktops and servers in a single week. For this reason, many chief information officers are partnering with general counsels to co-sponsor the implementation of such a dual process.

In sum, the re-convergence of computer forensics and e-discovery is an important development Counsel no longer must choose between mitigating risk or mitigating cost when meeting e-discovery challenges. Further, this convergence brings tremendous strategic benefits. With a common platform to support civil discovery, internal Sarbanes-Oxley fraud investigations, and the auditing of confidential data, a company can dramatically reduce the cost per activity by amortizing the cost of the platform over many different events, minimizing the employee training required, and of course reducing the amount of expensive outsourcing.

John M. Patzakls is vice chairman and chief strategy officer, and Patrick J. Burke is assistant general counsel; with Guidance Software.

Bringing Legal and IT Together at Nationwide Insurance

Copyright Fall 2008 by Guidance Software, Inc.

Andrew Drake is the Assistant General Counsel in Nationwide Insurance's Corporate Litigation Discovery Management Unit. He advises and assists with data-related litigation and regulatory inquiries, including Electronic Discovery. Andrew also acts as a liaison between Nationwide's information technology partners, business units and law department on a variety of litigation-related matters. His ongoing goal is to bridge the very divergent ways that the business, IT group and legal team operate.

Q: What is your legal/IT background and experience?

A: I spent more than 12 years working in a variety of IT roles from systems administrator to IT project manager before obtaining a law degree and making the move to Nationwide's Office of the Chief Legal Officer. I would say without question that experience across different business units within a company is an incredibly valuable asset for a Corporate Counsel – you really get a nuts-and-bolts perspective on how the business works. A holistic operational perspective is incredibly important when it comes to the types of matters we get in the door, simply from the standpoint that a seemingly innocuous looking issue may have very different degrees of impact depending on what business units might be involved.

Q: How did you become involved in eDiscovery?

A: I became involved with Electronic Discovery issues primarily as a result of my IT project management responsibilities before working as a Corporate Counsel. At the time, I was used to a structured methodology of IT project or program delivery, which was very different from how attorneys approached eDiscovery. In my view, this is really starting to change, as litigators are recognizing that putting together large data compilations is not trivial and unless you and your IT partners organize it formally, the results are uneven and costs skyrocket. Easily the greatest challenge in this area of the law has to be how fast the landscape is changing and evolving. It is no mean feat to keep up with the opinions coming out every day that interpret the new Federal Rules of Civil Procedure, as well as the 50 states that may or may not be marching to their own drummer. This keeps things interesting.

Q: How long has your firm usedeDiscovery technology?

A: We've been using eDiscovery tools ofsome sort or another for 7 or 8 years, though the early tools and processes were much less sophisticated than what we use today. The early products were far from a "solution" and almost required as much work to use the output as they did to operate. The rapidly evolving case law I mentioned means we have to make an effort to understand the gaps of the tools we use and either develop a process around them, figure out how to extend the tools to fill the gap, or look for something else that will resolve our issues. It's an active process – you can't acquire something and then sit back and assume everything's going to fall into place. Corporate Counsel should be an integral part of deploying and using the tools; in theory, they should be able to explain in detail how

and why the tools work and what the support processes around the tools are to outside counsel or others of importance in a matter, perhaps a regulator. You can't just take the output and run.

Q: What type of eDiscovery solution did your firm use before implementing in-house technology?

A: Like many other companies, we initially used a combination of off-the-shelf products not necessarily designed for eDiscovery and manual processes to fill in the gaps. Most of these were utilities used for desktop or server management. Before the focus on Electronic Discovery, this was probably adequate for the volume and types of materials being furnished. All that being said, it was very labor intensive and would quickly drain our resources. Itessentially became a question of, "How many people do you have to throw at the problem? An army?" We didn't, and something had to give.

Q: What are the measureable benefits your irm has experienced after implementing an in-house eDiscovery program?

A: eDiscovery software is a component of an overall larger effort that enables you to be more proactive in addressing issues. Clearly, the largest measurable benefits have come from our ability to in-source functions that used to be performed by either third party experts r outside counsel. Cost is a huge driver, as is the need to deal with volume. However, I am acutely aware of the need to maintain efensibility along with cost control, so the process element of the long term eDiscovery program is very important. Again, Corporate Counsel should view themselves as an integral function of the IT portion of this program. It's definitely not something you can hand off.

Q: How do you plan on taking advantage of in-house eDiscovery to further your firm's business goals?

A: I wish I had a crystal ball as to what our litigation or regulatory landscape will look like in 12 24 months. We are definitely looking forward to the next round of states finalizing their Rules of Civil Procedure, since we operate in many jurisdictions. I can say that we will continue the push to be even more proactive than what we are today, both from the usage of our tools and capabilities– pushing more into our compliance function for example, but also as a more visible participant in the trade groups and thought groups generating some of the industry change that's going on. I don't think there's any better way to be represented at the table if you're dealing with change. Longer term, we'll probably need to look at staffing again, since you can obviously tell we consider the operations component another critical piece of the puzzle. Inevitably, a matter may come in that could affect the direction of where we go, but the general objective of getting better and better in our eDiscovery program execution will remain constant.

The Risks and Costs of Custodian Self-Collection

by Daniel Lim, Esq.
Copyright Fall 2008 by Guidance Software.

"To adequately address the challenges and potential consequences of custodian self-collection, in-house counsel should seek to develop an e-discovery process that preserves ESI in a systemized, repeatable and defensible manner. "

In the midst of ongoing litigation, should you trust potential witnesses to comply with eDiscovery requests and avoid sanctions for missing relevant ESI? Is it wise to assume that all custodians will properly follow a litigation hold or collect and preserve data without overlooking, altering, moving or deleting it during collection and preservation? The answer is an unequivocal no.

The risks of custodian self-collection include non-compliance, under-collection, metadata alteration or spoliation, inadequate documentation of chain of custody, authentication challenges and business disruption. While most attorneys acknowledge the potential pitfalls of custodian self-collection, many grossly underestimate the actual risks and costs involved.

Take a recent bankruptcy case involving Hawaiian airlines. A principal witness in the lawsuit received a legal hold notice and responded by deleting relevant evidence. The court issued an adverse inference instruction agains the company because it "simply told [the custodian] to preserve all evidence and trusted him to comply," rather than taking reasonable steps to prevent spoliation. The company was held to have facilitated the misconduct even though the custodian acted in bad faith. In re Hawaiian Airlines, Inc., 2007 WL 3172642 (Bkrtcy. D.Hawaii October 30, 2007).

Spoliation is only one of many critical issues corporations are experiencing with custodian self-collection. In the recent Qualcomm case, attorneys were sanctioned and referred to the state board on alleged ethics violations because a fact witness's computer contained relevant evidence that was not produced prior to trial. The critical electronic files were discovered just prior to the witness's trial testimony and had existed on the witness's computer for four years prior to trial. Qualcomm, Inc. v. Broadcom Corp., 2008 WL 66932 (S.D.Cal. 2008).

This clear trend in case law shows that companies are ill advised to rely on custodian self-collection. Simply having a litigation hold notice go out and acknowledged by the end user is not sufficient good faith to insulate the client and attorneys from sanctions. See Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614 (D. Colo. 2007); In re NTL, Inc. Securities Litigation, 244 F.R.D. 179 (S.D.N.Y. 2007); Wachtel v. HealthNet, 239 F.R.D. 81 (D.N.J. 2006).

Moreover, the sheer volume of ESI continues to increase, even for smaller cases. A single personal injury plaintiff can have volumes of potentially relevant data sources, not only through hardware such as cell phones, iPods and flash drives, but also through information stored on various internet sites that enable the sharing of pictures and video, chat rooms, blogs, social networking, etc.

To adequately address the challenges and potential consequences of custodian self-collection, in-house counsel should seek to develop an e-discovery process that preserves ESI in a systemized, repeatable and defensible manner. An eDiscovery process that uses enterprise search and collection tools for responsive data collection from all prospective custodians will assist counsel in limiting their organizations' exposure to spoliation sanctions and penalties while facilitating compliance with the Federal Rules of Civil Procedure.

Copyright Fall 2008 by Guidance Software.

How do I set up an eDiscoveryreadiness plan?

An effective discovery response plan requires organizations to proactively anticipate the type of discovery that could be initiated based on prior years and develop an offensive response strategy. The goal is to provide guidelines that will serve as an overall business process for computer investigations and eDiscovery. The three major steps are: forming a corporate eDiscovery response committee, creating an ESI roadmap and drafting a plan.

When forming the response committee, it is important to include members from all departments. This group will facilitate crosscompany collaboration and coordination, establish best practices, analyze spending and identify risks.

The ESI roadmap is the information blueprint that indicates where ESI is located within the company's firewalls. It will require a system wide assessment that must be continually updated. This information will be critical to the designated 30(b)(6) witness that provides sworn testimony on information management, records policies and eDiscovery issues.

The eDiscovery plan addresses the entire eDiscovery process (identification, preservation, collection, processing, review and production). It should identify deficiencies in terms of cost, risk and time in light of the FRCP. It should also provide best practice recommendations for human resources, processes and technology.

Can you spell out the different ways to pay for eDiscovery?

There are essentially three ways to pay for eDiscovery: companies can contract with outsourced vendors, purchase an in-house eDiscovery solution or pay for technology the same way they pay for outsourced vendors, on a pay-per-use basis.

Outsourcing part or all of the eDiscovery process has been the traditional approach. This solution makes the most sense for companies that do not have a lot of litigation except for the occasional large case. In this model, a third party vendor handles the preservation, collection, processing and sometimes first level review of potentially relevant ESI. The downside to this model is that outsourcing is the most expensive of these three options over the long run and can be hard to coordinate when there are multiple ongoing cases and vendors involved. Outsourcing costs are normally passed through as a litigation expense which has caused many insurance companies to scrutinize their bills and CFOs to request that general counsels find ways to keep costs down.

Purchasing the technology and bringing the eDiscovery process in-house is the trend among Fortune 500 companies and for any others that have ongoing litigation. By taking control of the search, collection and processing of ESI, companies are better able to control ongoing costs, protect valuable intellectual property, coordinate ongoing preservation and collection and reduce the risk of non compliance. Although purchasing technology may shift some costs that were traditionally an

expense to the capital budget, insurance companies have rewarded those companies with reduced premiums, in addition to substantial cost savings over the long run. Additionally, when a big case hits, it is easy to supplement those spikes by bringing in experienced vendors to assist in the process.

The pay-per-use or consumption model has gained popularity with companies that don't have the capital budget to buy technology or don't have enough ongoing litigation to justify the costs. Although this approach is more expensive in the long run than an outright purchase of the technology, it is less costly than outsourcing. It allows companies to realize the benefits of bringing the eDiscovery process in-house by essentially renting technology on a per case/per gigabyte basis. This approach also allows companies to develop a strong internal litigation response team ready to purchase technology as budget becomes available.

What is the workflow for a corporate eDiscovery response?

1. Assess the scope of the litigation by identifying legal issues, time periods, key individuals and the potential data collection universe.
2. Issue a litigation hold. Custodians are instructed to preserve, not collect or review any ESI. IT suspends tape rotation and other standard operating procedures applicable to the litigation hold.
3. Conduct a targeted collection of potentially relevant ESI from applicable data sources. The collection process should not alter the metadata of responsive ESI. Full forensic images of hard drives are only performed if there is an issue of fraud or data spoliation.
4. Potentially privileged ESI is identified using an agreed culling strategy and responsive ESI is made available for immediate attorney review. Generally, privilege logs should contain specific information about the documents claimed to be privileged (attorney-client and/or work product).
5. Perform additional keyword searches to process remaining ESI and reduce the data set. All duplicates are removed from responsive ESI.
6. Create a load file to transfer the responsive ESI to the review platform of your choice. The XML load file format is the most universally accepted by most vendors.
7. The production format, number of production sets, delivery deadlines and location are discussed and agreed upon with opposing counsel early in the eDiscovery life cycle to prevent production delays.

Privilege and Spoilation in the Courts

by Patrick Burke, Esq. and Kimberly Wong
Copyright Fall 2008 by Guidance Software.

Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 70 Fed.R.Serv.3d 1052 (D. Md. 2008).

This is Real eDiscovery's top pick for the most notable eDiscovery decision of 2008. It is viewed as a tutorial in various eDiscovery topics by one of the foremost jurists in U.S. eDiscovery law, Chief U. S. Magistrate Judge Paul W. Grimm of the District of Maryland.

This decision explores the practicality of defensible processes for collection, including keyword searching, review of electronic documents, clawback agreements and how privilege disputes should be handled within the context of eDiscovery. The decision touches on these issues from both the perspective of the guiding standards and precedents as well as from a nuts-and-bolts litigation level in terms of what will or will not be deemed reasonable.

Plaintiff Victor Stanley, Inc. sought a ruling from the Court that 165 electronic documents produced to it in discovery by the defendant Creative Pipe, Inc. should not be deemed exempt from discovery because, contrary to the defendant's argument, they were not in fact protected by attorney-client privilege and workproduct doctrine protection. The Court's decision agreed with the plaintiff that the defendant had waived its privilege and work-product doctrine protections.

Judge Grimm described how the defendant at first sought Court approval for a clawback agreement, citing the possibility of inadvertent disclosure of privileged/protected documents given the volume of electronic documents to be produced in a short amount of time. However, when the Court later extended the defendant's discovery deadline by four months, the defendant abandoned its request for a clawback agreement and committed instead to undertake a document-by-document privilege review.

After receiving the defendant's production, the plaintiff's counsel discovered documents produced to it that were potentially privileged or work-product protected and notified the defendant's counsel. The defendants asserted that the production was inadvertent and belatedly provided privilege logs purportedly identifying the documents that had been inadvertently produced.

Judge Grimm's decision is remarkable due to the degree to which he takes the reader into the factual details of the defendant's pre-production review, which included the defendant's failure to examine many documents beyond their title pages, failure to use proper software tools to search through text-searchable PDF files and failure to apply best practices such as document sampling to test the reliability of its keyword searches. The decision is rich with references to applicable standards and best practice guidelines, including case law, the Federal Rules of Civil Procedure and Evidence and the Sedona Conference Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-Discovery, 8 Sedona Conf. J. 189 (2007).

The Court analyzed the defendant's assertion of inadvertent waiver under both a "strict" and an "intermediate" test and concluded that, under either approach, the defendant's production of the 165 documents amounted to a waiver. The Court's analysis focused on the "reasonableness of the

precautions taken to prevent inadvertent disclosure," criticizing the defendant's failure to provide the court with the keywords used, the rationale for choosing them, the attorneys' qualifications to create an effective search and retrieval method, what type of keyword search was used and whether they tested the effectiveness of the method.

Ironically, as the Court points out, had the defendant not abandoned its initial request for a clawback agreement, the company would have likely been protected from its waiver of privilege.

Ingoglia v. Barnes & Noble College Booksellers, Inc., 48 A.D.3d 636 (2008).

How is electronic spoliation handled in state court? This New York appellate court decision demonstrates the Court's willingness to impose severe sanctions for failure to produce electronic documents that existed under the party's control at the time the duty to preserve arose. In this case, the court dismissed the plaintiff's complaint for defamation in its entirety based on New York's common-law doctrine of spoliation of evidence.

The spoliation at issue was discovered by the defendant's computer forensic expert, who determined that the plaintiff had installed a software application designed to permanently remove data from the computer's hard drive, and that even after the Court had issued an order for the production of the plaintiff's computer for inspection, various data were deleted. During that time, the plaintiff also deleted numerous files, images, folders and some internet usage history.

The defendant initially survived the motion to dismiss at the trial court level, but the Appellate Division, Second Department, reversed and granted dismissal of the complaint because the plaintiff violated the common-law doctrine of spoliation of evidence. The Appellate Division found that the defendant was severely prejudiced by the plaintiff's destruction of key evidence. Thus, the plaintiff's actions amounted to spoliation of evidence and the court dismissed the plaintiff's complaint pursuant to the plaintiff violating its statutory duty to disclose under section 3126 of the New York Civil Procedure Law & Rules.

Edmund Sautter

Copyright Fall 2009 by Guidance Software.

Edmund Sautter is a partner at global law firm Mayer Brown LLP, resident in its London office, and is currently seconded to Merrill Lynch's London law department. Below he responds to Real eDiscovery's "Ask the Experts" question:

Are there any practical steps that I can take to mitigate the burden of compliance with European Data Privacy rules, when giving discovery in the U.S.?

The obligation to observe the European Data Protection Directive, as implemented by the EU member states, is an increasingly high profile issue for those providing disclosure in proceedings outside the EU, in particular in countries like the U.S. which have, on the one hand, broad discovery rules and, on the other, a somewhat limited approach to privacy issues. The Directive has strict rules (with relatively limited derogations) prohibiting the collation, and transfer out of the EU, of personal data. The following suggestions may assist in moderating the effect of these tensions.

First, note that the Directive has been implemented by domestic legislation in each EU member state. The mode of implementation (and the approach of the respective Data Protection commissioners) has not been entirely uniform between the member states, so you should take advice in relation to each state where the relevant data resides. A particular approach in one state may not be replicated in its entirety in another. However, the definition of personal data is broad, which leads to the next point.

In negotiations with the other party, seek to restrict so far as possible the extent of the data searches that are required. Overly broad search terms generate large amounts of data, some of which is relevant, but (often) much of which is not. (I have personal experience of a case where agreed search terms resulted in a body of collected data of which less than 5 percent was actually relevant.) The wholesale transfer of such irrelevant material out of the EU (to the extent that it contains personal data) is likely to breach the Directive. Therefore, reduce the burden of in-country review prior to transfer by negotiating, if possible, restricted search terms, date ranges, custodians, and so on. Further, although there is often reluctance to conduct the relevance review in-country, this may be a more practical solution, given the likely extent of personal data, than seeking first to identify personal data with a view to redacting it prior to transfer for the relevance review.

Consider also whether consent is an appropriate way forward but be aware of its significant limitations. For instance, the consent of the author or recipient of an email only extends to the personal data of that person, and not the personal data of the other party to the email. Also such consent must be freely given and capable, without sanction, of being withdrawn.

Based in London, Edmund Sautter advises and represents banks and other financial institutions in disputes, contentious regulatory matters, and associated risk management issues. He is a member of the Sedona Conference Working Group on international and electronic information, discovery and disclosure.

Standoff Between EU Data Protection and U.S. eDiscovery Requires Difficult Compromises for Both Sides

by Patrick J. Burke, Esq.
Copyright Fall 2009 by Guidance Software.

Lawyers on both sides of the Atlantic can be passionate when discussing the EU data protection laws and their impact on U.S. eDiscovery. Most American lawyers are incredulous that Europeans do not accommodate the need of U.S. litigants to collect and produce electronic documents and email from Europe that are deemed necessary to support claims or defenses. And most European lawyers are equally incredulous that Americans expect they should be permitted to collect and produce those electronic documents without regard for employees' rights to keep such information private.

Underlying the standoff are fundamentally differing priorities—Americans tend to value the search for justice over the protection of individual privacy, while Europeans may reverse these priorities.

Each side has incentives to compromise. Lawyers representing American companies would prefer not to be sanctioned for failure to preserve and produce electronically stored information (ESI) and would benefit from a compromise acceptable to the U.S. courts and European privacy sensibilities. European corporations sued in U.S. courts would prefer not to risk adverse inference instructions and stiff sanctions for their failure to produce important evidence.

Where are the possible compromise points? Let's look at what makes an email protectable by the European data protection regime.

Each email contains the employee's email address which in and of itself is considered protected personal information because it connects the communication to a European citizen. European data protection officials have indicated, however, that they might find it acceptable to collect and transfer email to the U.S. if the email address is scrubbed away first. Of course, American litigators consider the email's author or recipient a crucial element of the evidence. But when a requesting party is hungry to receive useful evidence, and the producing party is anxious to avoid sanctions, each may be incented not to allow perfection to be the enemy of the good. Perhaps U.S. litigators can be partially satisfied with a key that establishes which emails were sent or received by "Executive A" or "Research Scientist X." While this would impinge on litigators' ability to depose the email's author or recipient, it would at least allow for the use of the email's content and place it in some broad context.

Collection approaches can also provide opportunities for compromise. Companies often pull all of an employee's ESI and then review or search them to find the relevant evidence that should be produced. European employees are uncomfortable with their companies' lawyers and agents possessing and reviewing all their ESI, even if only the relevant subset is produced to opposing counsel. The concern is compounded by the employees' inability to know when their email is being searched in this way. However, companies can employ technology to allay these concerns. Search technology can be employed to search employees' ESI and only collect that which contains certain keywords and falls within relevant timeframes. By surgically targeting only the most relevant ESI,

companies can provide employees with reassurance that truly personal electronic documents and communications are not being swept up, reviewed and disseminated.

Companies can also build trust with their employees through transparency of process and technology. Before implementing a collection approach, companies are well advised to sit down with employee representatives, unions and/or works councils to explain the techniques and privacy safeguards being employed. Such advance notice, and invitations for employee feedback, can go a long way. Once implemented, the actual carrying out of surgically targeted collections can be made transparent to employee representatives, who can receive notification each time the search technology is employed, including the search criteria used and which employees' data is searched. Such transparency provides employees with the opportunity to decide—on a case-by-case basis—whether, and to what extent, their privacy rights have been implicated.

Dispassionate examination of these process and technology alternatives may be the only way to bridge the gap between the U.S. emphasis on the search for justice and the European passion for privacy. They may offer the only common ground between sincerely-held, yet opposing, values.

EU Data Protection Versus U.S. eDiscovery

by Patrick J. Burke, Esq.
Copyright Fall 2009 by Guidance Software.

"The U.S. eDiscovery bar has sought to engage the European data protection authorities to consider a reconciliation between EU data protection and U.S. eDiscovery laws."

Multinational companies with U.S. and EU facilities find themselves in what seems like a no-win situation when it comes to eDiscovery.

On one hand, they are legally required to respond to discovery requests in cases before U.S. courts that require the collection, review and production of electronically stored information (ESI) created by European employees or stored on their computers. On the other hand, they are faced with the fact that EU law disfavors transferring email and other ESI due to stringent protections of employee privacy.

This is why corporate counsel at multinational companies are expanding their understanding of the substantive EU privacy laws— beginning with the 1996 EU Data Protection Directive and the enabling laws implementing it and extending to the blocking statutes and other applicable regulations in the 27 EU member states.

Unfortunately, published decisions and regulatory guidance are scarce in this area. Data protection authorities have been unwilling to commit themselves in writing to clear statements of the restrictions applicable to eDiscovery, leaving multinationals vulnerable whenever ESI is collected in the EU and transferred to the U.S. The U.S. data privacy bar counsels that the risks are broad and undefined but, as discussed below, there are suggested best practices for building processes best able to reduce the legal risks.

EU Protection of Personal Data

The crux of the dilemma is the EU concept of "personal data." In the EU, personal data includes any email or electronic document that includes an employee's email address, name or other identifying information that possibly can be tied to that employee. The stringency of these restrictions varies among the different EU member states and the determination of which member state's laws apply dictates the manner in which its lawyers should proceed. Companies in the U.K., for example, operate in a more forgiving legal environment than, say, in France.

Once counsel has determined the member state jurisdictions that apply, they can begin to get their arms around the applicable limitations on data collection. British data protection authorities, for example, have issued guidance documents that allow for a balance between the legitimate business needs of the company and the privacy rights of employees. French data protection regulators, on the other hand, offer no such balance of interests—leaving France among the most challenging European jurisdictions.

The Challenge of Transferring ESI to the U.S.

Even where ESI collection can be accomplished lawfully, the transfer of electronic data to the U.S. from any EU member state faces restrictions. Lawyers most knowledgeable on the issue advise that, when possible, companies obtain written consent from employees from whom data is to be collected. Keep in mind, however, that EU law requires that such consents be freely given and are capable of revocation at any time—and are viewed with skepticism due to the imbalance of power in the employment relationship. Data protection practitioners also advise that companies' ESI collection protocols be customized in the EU to better respect the privacy rights of employees and to adequately address the concerns of union or, in certain countries like Germany, works councils, whose function is to represent the best interest of employees.

Over the past several years, companies using EnCase® technology have been able to take advantage of its ability to perform surgically targeted collections—collecting only those emails and electronic documents that meet relevant search criteria—to respect the rights of employees. Non-relevant personal data is left uncollected. This same technology also permits companies to provide unions or works councils with an audit capability so that they can be sure the company is not overstepping its authority.

Another tactic is to scrub all personal data out of the ESI (i.e. remove email addresses, names, etc.) before it is transferred out of the EU. Anonomyzing software exists to facilitate scrubbing; however, the approach must be cleared in advance with opposing counsel to be sure they will be satisfied receiving ESI from which all names and identifying information related to European employees have been removed.

The U.S. eDiscovery bar has sought to engage the European data protection authorities to consider a reconciliation between EU data protection and U.S. eDiscovery laws.

In the past year, these efforts resulted in the opening of a dialogue with the European Commission's Article 29 Data Protection Working Party, which on February 11, 2009, published a document entitled, "Working Party 158," that was devoted exclusively to cross-border discovery issues.

The document invited "interested parties, courts in other jurisdictions and others to enter a dialogue with the [European Commission's] Article 29 Data Protection Working Party" on these issues. This document does not sketch out a solution to the data transfer dilemma, and in fact casts doubt on the use of employee consents as a way out of the problem, stating that it is "unlikely that in most cases consent would provide a good basis for processing."

The document concluded that "[r]elying on consent may… prove to be a 'false good solution,' simple at first glance but in reality complex and cumbersome."

Applying Savvy Lawyering to the Challenge

As the U.S. and EU grapple with these issues, employing a conservative approach and smart lawyering with surgically targeted search technology can help multinationals achieve "win-win" resolutions.

Savvy U.S. litigators advise counsel to raise EU data protection issues with opposing counsel and

the court early on in the litigation process, in order to set and manage expectations on the demand side. They also recommend negotiating protocols for security and privacy of all EU data produced in the case, and having those provisions converted into a court order which can be shown to European employees, works councils, and regulators. Such protocols should also make provisions for the return of any ESI received from employees who later decide to revoke their consent to its transfer and production.

Other possible negotiated solutions include attorney review of the ESI by counsel for the requesting party in the EU country of origin, or obtaining agreements from the requesting party to receive the ESI after personal data has been scrubbed using anonymizing software. Though it doesn't look as though we'll see a solution to the conflict between U.S. discovery obligations and the EU data privacy laws any time soon, at this stage, understanding the requirements of data protection authorities, choosing an approach that respects those requirements, and selecting technology that allows you to meet your obligations on both sides of the spectrum is the best recipe for success.

Though it doesn't look as though we'll see a solution to the conflict between U.S. discovery obligations and the EU data privacy laws any time soon, at this stage, understanding the requirements of data protection authorities, choosing an approach that respects those requirements, and selecting technology that allows you to meet your obligations on both sides of the spectrum is the best recipe for success.

Judge Simon Brown Discusses Growing Impact of Electronic Disclosure in the U.K.

Copyright Fall 2009 by Guidance Software.

His Honor Judge Simon Brown QC adjudicates mercantile cases at the Birmingham Civil Justice Centre. He is among the most outspoken U.K. judges on the topic of electronic disclosure in civil cases.

Q: How is it that you have become so involved in the debate and thinking behind the evolution of electronic disclosure in the U.K.?

A: As a Mercantile Court judge in Birmingham I increasingly encountered controversies in which electronic evidence was important to my fact-finding. Our courts implemented a new section 2A of the Practice Direction to Part 31 of the Civil Procedure Rules here. We have had the rules in place for quite some time now but, quite frankly, lawyers and the courts have not paid much attention to electronic documentation. I view it rather differently; judges ought to be very interested in electronic documents, particularly email. Often email, the smoking gun, is probably the key to the case if you are a fact-finding judge.

Since I began banging the electronic disclosure drum, I've actually had quite a number of cases that have been started in my court, and I've asked, "Why are you in front of me? This doesn't seem to be the usual case that comes in front of the court." And they've said, "You are keen on electronic disclosure and we believe we are going to have problems with the other side, and we believe you will help us sort them out or make us sort them out." In the main, though, certainly in my court when I ask if they have looked at the Practice Direction under 2A, I often get a rather odd look indeed. My experience was, originally, that the parties never discussed anything before they came to the case management conference, let alone electronic disclosure.

Q: How would you describe the current state of electronic disclosure in the U.K.?

A: It is implicit in the present rules that parties must be in a position to explain to their opponents and to the court what course they propose to adopt in relation to disclosure and what of the likely costs are. That places a premium on being able to identify potential sources and thence the costs of handling them, as quickly and cheaply as possible. These rules are quite clear. They say that prior to the first case management conference, the parties should, and the courts interpret that word as "must," discuss any issues that may arise regarding searches for, and the preservation of, electronic documents. In the U.S., you are completely swamped with electronic documentation, and certainly the reaction in the U.K., by members of the senior judiciary, has been: We do not want any of that here. Obviously, the court doesn't want to get involved in electronic disclosure processes, but it does want the parties to engage in those processes efficiently and in accordance with the rules. The rules provide for electronic disclosure to be done in such a manner that judges are given the tools to find the facts of the case with accuracy—and that's what you want from the judge.

Q: What are you doing now in the Birmingham courts?

A: In the Birmingham courts, we're going to get involved in case management with the allied cause of cost management. We are doing a pilot scheme. With the consent of the parties, we're going to have a breakdown, in which the judge will see how much parties are going to spend on a case. One question will be: "How many electronic documents have you got?" The purpose of this three-month trial is to see if it is worthwhile to do such an exercise.

I think, in the future, you will find a much more businesslike approach to electronic disclosure in the U.K. courts, particularly in the business courts. It is going to be managed more proactively by the judges.

Judge Scheindlin States Litigants, Including the Government, Must Demonstrate Ability to Search and Assess ESI

By Daniel Lim, Esq.
Copyright Fall 2009 by Guidance Software.

SEC v. Collins & Aikman Corp., No. 07 Civ. 2419, 2009 WL 94311 (S.D.N.Y. Jan.13, 2009)

Can the government succeed in a blanket refusal to produce emails on the grounds of privilege without conducting an assessment of its electronically stored information (ESI)? Judge Scheindlin, of Zubulake fame, has answered this question firmly—no.

In SEC v. Collins & Aikman Corp., the SEC investigated defendants for accounting fraud. Defendants sought production of emails from the SEC relating to its investigation and handling of other similar prosecutions. The SEC responded that nearly all responsive emails would be privileged, protected, or non-substantive. The SEC also objected that the requests were overbroad.

Judge Scheindlin was not satisfied with the SEC's blanket refusal to produce emails. She stressed the importance of parties, including the government, to stay updated on the technical ability to search and assess ESI, noting the ability to search and review email as "a routine aspect of modern discovery." SEC v. Collins, 2009 WL 94311 at *11. The SEC's sole assertion that the cost of a search for responsive ESI was too high did not suffice in objecting to discovery.

This opinion makes clear that even when a privilege applies to the majority of ESI, an effort must be made to document the cost or likelihood that a search would produce relevant, non-privileged material. Scheindlin observed that "[t]he concept of sampling to test both the cost and the yield is now part of the mainstream approach to electronic discovery." Id.

In the end, Judge Scheindlin directed the parties to meet and confer to negotiate a reasonable search protocol, "considering the use of appropriate search terms and appropriate limitations of subject matter and date…" Id. She also suggested applying the search protocol to a segment of the SEC's email to assess the likelihood of such terms in identifying relevant, non-privileged ESI.

Scheindlin's opinion is clear as to the government's obligation to respond to discovery requests for ESI: "When a government agency initiates litigation, it must be prepared to follow the same discovery rules that govern private parties…" Id. at *12.

This case illustrates the level of proof necessary to sustain traditional discovery objections. Rather than assert a myriad of objections without any actual early case assessment of data, i.e., prior to collection, objections must be supported by proof of potential costs and likelihood of success. Solutions, such as EnCase® eDiscovery, do just that, providing the technical capability to test search protocol on a sample of data prior to collection of the entire data set.

Delaware Court Issues Adverse Inference Instruction for Failure to Preserve PowerPoint

An ongoing debate in eDiscovery is whether organizations should seek to collect ESI for all litigation, or if self-collection and preserve-in-place approaches are defensible alternatives. The case law continues to counsel against preserve-in-place and self-collection.

In Beard Research, Inc. v. Kates, the court issued an adverse inference instruction and awarded attorney fees against defendants for a PowerPoint presentation left uncollected and eventually lost from a custodian's computer. The interesting wrinkle in this case was that the presentation was on a computer that was never even owned by the defendant corporation.

Kates had been employed by the plaintiff, Beard Research, and issued a laptop computer. When he resigned, the employee retained possession of the laptop. At his new employer, Kates used this same laptop to deliver a PowerPoint presentation to a defendant corporation's Board of Directors. Plaintiff alleged that the presentation contained its confidential intellectual property.

Shortly after plaintiff filed suit, the defendant corporation terminated Kates' employment, but left the computer in his possession. By the time a court order for production of the laptop was received, the computer had been wiped and re-formatted several times.

On motion for sanctions alleging spoliation, the Delaware court found that Kates and the corporate defendants failed in their preservation obligations. The court criticized the corporate defendants, as well as Kates, for not taking any steps to preserve relevant ESI from the computer. The court allowed plaintiffs an adverse inference instruction to the jury that the presentation lost from Kates' computer and shown to the defendant corporations included plaintiff's trade secrets.

Deciding to forgo collection relies on the assumption that a court will not fault an organization for lost evidence so long as it has placed the witness on notice of the litigation hold. Cases like Beard Research continue to debunk this assumption.

Corporations remain liable, even for terminated employees, if ESI is left uncollected from their original sources. Best practice is to secure evidence in a forensically-sound manner for every case, using the right technology.

The E-Discovery Toolbox: What You Should Look for in a Unified E-Discovery Solution

By Chad McManamy, Esq.
Copyright Fall 2010 by Guidance Software.

"With a unified technology, organizations have the ability to insource such capabilities as automated legal holds, pre-collection analytics, early case assessment and first-pass review."

Faced with the high costs of outsourcing e-discovery to vendors, consultants and outside counsel, organizations have no doubt considered insourcing some of the work. The decision of which e-discovery processes to bring in-house is based on various considerations. Setting aside the document review phase of the process, organizations look first to the most costly line items when deciding which processes to bring in-house first. In recent years, organizations have targeted collection and processing as two big-ticket items to bring in-house. In fact, Real eDiscovery's Winter 2009 feature article ("Bringing eDiscovery Processing In-House") addressed how organizations are attempting to move e-discovery collection and processing in-house and away from service providers[953].

In the short time since the article's publication, collection and processing have expanded such that organizations are continuing to insource more of the e-discovery workflow. This trend is a result of a number of factors, including: the increased sophistication and capacity of in-house e-discovery teams, the pressure to adapt to shrinking legal budgets and minimize risk during continuing difficult economic times, and the development of technology that facilitates an integrated, comprehensive solution to the increasingly complicated e-discovery process. The issue remains as to which of the processes to bring in-house. With a unified technology, organizations have the ability to insource such capabilities as automated legal holds, pre-collection analytics, early case assessment and first-pass review.

Litigation Hold

A litigation hold notice is a memo that notifies an organization's employees of their preservation obligations as custodians of potentially relevant documents to a lawsuit. For decades, the issuance of a paper memo to custodians and a follow-up interview were sufficient to meet a litigant's initial discovery obligation. Technology has created the need for a higher standard of care and a more robust process that can improve the accuracy of electronically stored information (ESI) collections, track and release the scores of litigation holds large organizations maintain, and standardize the process from the outset of a case.

In addition to the hold notice, organizations can combine technology solutions with standardized questionnaires and reporting functions to reduce costs further and minimize risk. The use of technology may also provide a defensible position, potentially protecting organizations from mistakes common in a manual process.

953 The article examined the intricacies of ESI processing and the role technology can play in reducing processing costs and risks for in-house e-discovery teams.

However, a technology-based legal hold notification solution still requires human contribution. Organizations considering automating this aspect of the e-discovery process should consider the risk of error inherent in stand-alone solutions. Specifically, errors that may occur during the transition from the issuance of the legal hold to the point at which ESI collection begins. An integrated solution that uses a single platform for both the legal hold and collection phases provides organizations with the most complete process.

Specifically, legal should look for a solution that uses the custodians placed on legal hold as the starting point to manage, track and report on the collection, preservation and processing of ESI. This means that litigation hold is no longer an independent process isolated from the other parts of e-discovery. Thus organizations reduce costs and minimize potential errors during collection. (See, The Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities LLC, 685 F. Supp 2d 456 (S.D.N.Y. Jan 15, 2010, amended May 28, 2010) "[t]he failure to issue a written legal hold constitutes gross negligence because that failure is likely to result in the destruction of relevant information."

Pre-collection Analytics

Many of a company's initial efforts to alert custodians and collect ESI are an attempt to establish a record of reasonableness. Given the prevalence of case law concerning sanctions for spoliation, organizations tend to err on the side of over-inclusiveness during this process. This means organizations may issue holds to potentially irrelevant custodians. The result is unnecessary expense. Technology that can perform pre-collection analysis of ESI from potential custodians can return relevant information early in the e-discovery process. This information can help guide the direction of the litigation. Specifically, counsel can use the results of this pre-collection analysis to—among other things—refine keyword lists, eliminate or expand custodian lists, estimate costs based on the volume of potential data to be collected, and assist in preparing a litigationspecific data map. Used in conjunction with an integrated legal hold notification process, organizations can recognize significant reductions in costs at the earliest stages of a lawsuit.

Early Case Assessment

The ability to analyze ESI traditionally required lengthy, expensive processing and document review. This typically moved any analysis of the documents' contents to the end of the discovery process. As the volume of ESI expands exponentially year-over-year, this workflow model is not only cost-prohibitive, but it also exposes an organization to unjustifiable risk. In-house legal departments should choose a solution that can analyze ESI at any point in the discovery process. Often generically referred to as early case assessment (ECA) in-house counsel typically had to wait until after processing to be able to analyze ESI. Now in-house counsel should expect that their e-discovery technology should allow analysis almost simultaneously with the collection, and even prior to collection. With ECA technology, in-house legal departments can view documents as they collect them and make strategic

decisions earlier about the company's legal exposure and defense strength. Furthermore, powerful indexing engines that allow faster keyword searching, term-hit highlighting and advanced search capabilities (e.g. Boolean) are enhancing ECA. ECA technology also can reduce the time it takes for counsel to uncover and manage "smoking gun" documents from months to only a few days.

First-Pass Review

What was once the exclusive domain of large-firm associates, the document review phase of e-discovery has undergone dramatic changes. With the latest technology, in-house legal departments can review and analyze documents before sending them to outside counsel. Retaining the documents internally until an organization has conducted initial review and analysis provides significant cost savings and reduces risk.

Counsel achieves these cost savings by having internal personnel review documents using keyword searching and content analysis. Instead of dumping every document collected on outside counsel to review, legal departments produce only a targeted production, thereby reducing review costs without exposing the company to spoliation risks.

Until recently, in-house counsel simply could not scale an internal team capable of reviewing the vast volume of potentially relevant ESI. Advances in technology have changed that paradigm.

In-house counsel should choose a solution that can manage a number of simultaneously occurring processes. For example, from a Web interface, in-house counsel should be able to run keyword searches against individual custodian collections to refine keyword lists for upcoming meet-and-confers with opposing counsel. The search results should not only provide metrics on the potential volumes of ESI, they should also allow counsel to view the actual documents. While eyeing the documents, attorneys should be able to apply user-definable issue tags and add attorney notes. If the keyword search returns an e-mail, the solution should make it possible to view the e-mail thread (i.e., parent-child relationship) and uncover previous or subsequent, related messages.

Looking Ahead

Technology solutions are evolving to assist organizations with meeting litigation's growing technical demands. The trend of insourcing more of the process will continue as organizations look to lower costs and reduce risk wherever possible. A mature, integrated technology with the core functionality of collection and preservation, ECA, legal hold and first-pass review should be a priority for organizations considering this approach.

A Scalable Solution

Whether your case concerns a handful of custodians or spans across the enterprise, EnCase eDiscovery's integrated technology enables counsel to run pre-collection analytics, issue and track litigation holds, view documents during collection, and index only potentially relevant documents. With this robust solution, organizations are now empowered with the option to bring the e-discovery process in-house.

At Liberty Mutual, E-Discovery is a Team Effort

Copyright Fall 2010 by Guidance Software.

Many organizations' law departments are looking for ways to bring the e-discovery process in-house to make it more defensible and less costly. This requires a close working relationship between legal and the IT personnel who understand the organization's network and how to reach data. Such partnerships between legal and IT have been successful at many companies and serve as models for organizations taking on the challenge.

Liberty Mutual is known for having a wellintegrated in-house e-discovery process. We asked Sean McSweeney, Deputy General Counsel, and Glenn O'Brien, Electronic Discovery Manager, to discuss their process and approaches from the legal and technical perspectives.

Q: What aspects of the e-discovery process do you handle in-house at Liberty Mutual?

A: In the context of the Electronic Discovery Reference Model, we have in-house capabilities to handle information management, identification, preservation, collection and processing. With respect to review and production, we typically collaborate with our outside counsel provider to determine the best approach.

Q: To what extent is the success of the Liberty Mutual e-discovery process a story of cooperation between legal and technical teams?

A: The cooperation between legal and technical teams was essential in establishing our process. Early in the project, we brought together all of the stakeholders, legal as well as all of the technical teams needed. The legal department explained the business need for establishing the process, and the various technical teams responded with what it would take to implement it. We then essentially created sub-projects with each of the technical teams in order to resolve issues and implement our processes.

Throughout this process, the legal team learned a great deal about system issues and gained a more thorough understanding of how the systems operate. At the same time, the technical teams developed a greater appreciation for the business process. The legal department continues to stay in constant contact with the various technical teams well after the implementation of the process.

Q: Can you describe the personnel and technology involved in the operation and governance of the e-discovery process?

A: We don't take a one-size-fits-all approach; therefore, the personnel and technology involved may change depending on the requirements of the matter. The personnel may include representatives from our legal staff, outside counsel, electronic discovery group, various internal IT organizations or outside vendors. Technology choices may range from broad, network-based collections to deep-dive forensic examinations.

Q: What role does EnCase eDiscovery software play in Liberty Mutual's e-discovery process?

A: Although we have several tools available to us, EnCase eDiscovery is the cornerstone of our process. It provides the means to collect data from a wide array of storage locations in a forensically sound manner. It also gives us the flexibility to acquire full forensic images on individual devices if the case warrants it.

Q: What are the primary advantages of maintaining a sophisticated in-house e-discovery process?

A: There are several advantages. First is the ability to be proactive. Bringing the process in-house affords us the opportunity to initiate the process and focus on the case rather than focusing on building a process and searching for vendors.

Second is repeatability. We spent a considerable amount of time installing the process. We worked out the issues with the various IT units so that we could execute the same process for each case. As a result, we only had to go through the learning curve once for all of our cases rather than each time for each case.

Third is cost. Paying for the software and implementation costs once was far less expensive than paying e-discovery-related expenses on individual matters.

"EnCase eDiscovery is the cornerstone of our process. It provides the means to collect data from a wide array of storage locations in a forensically sound manner."

Master European Data Privacy Laws

By Denise Backhouse, Esq.
Copyright Fall 2010 by Guidance Software.

Denise Backhouse is an associate in the eData Practice of Morgan, Lewis & Bockius, LLP. She counsels and defends clients primarily in the areas of securities and financial industry litigation and business and corporate disputes.

As telecommunications and globalization continue to accelerate the spread of digital information throughout the world, understanding European data privacy and protection laws becomes crucial.

Where can I go to find out about European Union (EU) data privacy protection laws and how they affect the discovery of European data in U.S. litigation?

As a preliminary matter, there is no one place to go for information about European data protection laws. However, an excellent starting place is the European Commission's Data Protection website.

National data protection laws are based on European Commission Directive 95/46 EC, which provides an overarching framework and minimum standards. Furthermore, the Directive encourages each state to interpret and enact its own version. The European Commission website provides the Directive in multiple languages and an overview of the statuses of the legislation in the 30 member states that make up the European Economic Area (EEA)—the 27 EU member states plus Iceland, Liechtenstein and Norway. There are also links to each of those statutes and their amendments (and, for Austria and Germany, to the laws enacted by the federated Länder or states) with English translations where available, with the caveat that translations are often "unofficial" and for informational purposes only.

The Article 29 Working Party is the independent EU advisory body on data protection and privacy set up under the Directive. Links to this group's published opinions interpreting key issues and concepts in data privacy law are organized by year and include the 1/2009 WP 158 on pre-trial discovery for cross-border civil litigation, which specifically addresses issues surrounding data processing and, to a lesser extent, transfer. In addition, the Commission's FAQs on transferring personal data out of Europe to third-party countries includes a step-by-step decision tree to assist with the analysis. Keep in mind that opinions of the Article 29 Working Party, though persuasive, are not binding on European national enforcement agencies.

National data privacy administration and enforcement authorities' websites also have useful information. For example, the French CNIL's website, available in English and Spanish, explains data privacy rights and obligations and includes topics and news items.

Among the blogs in this field, Chris Dale of the UK eDisclosure Information Project site provides timely analysis that manages to be both thoughtful and entertaining.

In addition to the national data protection acts and their related notices and other requirements, a host of other laws and issues can come into play. Labor laws, general and issue-specific "blocking" statutes, telecommunications laws, and regulations are among the many issues that you need to consider. The Sedona Conference® International Working Group WG6 has published two useful

papers providing a broader perspective, including the 8/2008 Framework for Analysis of Cross-Border Discovery Conflicts and the 9/2009 International Overview of Discovery Data Privacy and Disclosure Requirements, which give detailed information concerning the legal system and data privacy laws of 12 countries, including seven European countries. One of these is Switzerland, which, being outside of the EEA, is not represented on the Commission's site. The Sedona Conference lists these papers on its homepage under "Recent Publications" and requires users to provide their name and e-mail address to access them. Guidance Software has published a series of helpful white papers addressing EU data discovery issues, including "Seeking a Balance in the Discovery Equation," which provides an overview of European data protection laws and their implications for U.S. discovery, and several on UK and German data protection and compliance issues.

Finally, if you are dealing with an actual data protection matter, it is essential to consult local counsel in the EU member state(s) where the data at issue is located.

Reduce Your Risk of E-Discovery Sanctions by 80 Percent

By Patrick E. Zeller, Esq.
Copyright Fall 2010 by Guidance Software.

One of the most common questions I get from law students[954] and in-house counsel alike is "How do I reduce the risk of e-discovery sanctions?" My answer is simple: It's best to begin by collecting and preserving all potentially relevant electronically stored information (ESI) because that's how you eliminate 80 percent of the sanction risks.

The key aspect to the 2006 amendments to the Federal Rules of Civil Procedure (the "Rules") is the duty to preserve ESI. The Rules instruct parties to preserve, discuss and plan for ESI, in many cases before litigation actually begins. A party's failure to meet its duty of preservation will often result in sanctions, including payment of costs, adverse inference instructions, default judgments or dismissals.

To determine whether such sanctions are warranted, courts have used the following test: (1) whether the party had an obligation to preserve the evidence at the time it was destroyed; (2) whether the evidence was destroyed with a "culpable state of mind;" and (3) whether the destroyed evidence was "relevant" to the party's claim or defense.[955] Therefore, if a party has a defensible, repeatable process to collect and preserve potentially relevant information that prevents relevant evidence from getting destroyed once the duty to preserve arises, it will substantially reduce or eliminate its potential risk for sanctions. The most prevalent sanctionable conduct related to e-discovery is the failure to preserve ESI[956]

There are three key factors that are essential to building such a defensible and repeatable process. First, you need to bring the process in-house. By making it part of your corporate fabric, everyone in your legal and IT departments will know the process used to search, collect and preserve relevant ESI. This will give you several benefits. Having dedicated people searching and collecting your ESI will promote the use of the same process for each data collection. In addition, your employees will already have some expertise in searching and collecting data because they are part of the corporate culture, understanding your unique corporate language and the uniqueness of your data environment. Owning this process will also allow you to take control of the spiraling costs of an outsourced e-discovery process, enabling you to save millions of dollars annually.

It's important to keep in mind that whoever does your ESI searches and collections will need to testify, so ensure that they have the necessary training and certifications.[957]

Second, you need an in-house process with early case assessment (ECA) capabilities. Specifically, these ECA capabilities should allow you to test, search and sample keywords, file types, dates, times and other criteria before you collect data. A true pre-collection ECA capability also will allow your

954 Adjunct Professor and Distinguished Lecturer teaching Electronic Discovery, Digital Evidence, & Computer Forensics since 2006 at The John Marshall Law School.

955 Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 430 (S.D.N.Y. 2004) ("Zubulake V").

956 Sanctions for E-Discovery Violations: by the Number by, Dan H. Willoughby, Jr. and Rose Hunter Jones, Duke Law School Civil Litigation Conference, May 10-11, 2010 P.9 Warburg

957 Guidance Software offers well-established certifications for EnCE (EnCase Certified Examiner) and EnCEP (EnCase Certified E-Discovery Practitioner).

lawyers to collaborate with IT professionals to determine what data they truly need to collect, it will allow you to test and sample your environment, and it will better arm your lawyers for their meet-and-confer conference with opposing counsel.

Third, your in-house process needs to search, collect and preserve ESI without altering any metadata. Metadata includes things like blind copies on e-mail, formulas on Excel spreadsheets, track changes in documents and timestamps on files. Keep in mind that the creation dates and times and last-accessed dates and times are highly volatile. In fact, simply opening a file can alter them. Therefore, if your process depends on employees dragging and dropping relevant documents for custodian self-collection, it will alter potentially relevant metadata. The best process is a solution that can search for potentially relevant ESI and make a copy of that data while preserving all relevant metadata that's admissible in court. Once you properly preserve all potentially relevant ESI, you can use virtually any type of culling, review and production processes with little or no risk of spoliation. Also, a proper initial collection will let you retrieve any needed ESI or metadata from the originally collected data.

It's also critical that you issue a litigation hold or communication to potential data custodians informing them of the reason for the legal hold and explaining what they need to preserve. Recent cases emphasize the need for a written hold notice to ensure you preserve relevant ESI. "When the duty to preserve is triggered, it cannot be a defense to a spoliation claim that the party inadvertently failed to place a 'litigation hold' or 'off switch' on its document retention policy to stop the destruction of that evidence."[958] In fact, courts have found the failure to instigate a litigation hold to be grossly negligent.[959] Issuing a legal hold is a crucial first step because it will help prevent your employees from inadvertently deleting potentially relevant ESI.

Quickly issuing a legal hold combined with a defensible, repeatable in-house process to search, collect and preserve potentially relevant ESI as outlined above should allow you to eliminate 80 percent of your e-discovery sanction risks.

958 MOSAID Techs. Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 339 (D.N.J. 2004).

959 Green v. McClendon, No. 08 Civ. 8496, 2009 U.S. Dist. LEXIS 71860, at *18 (S.D.N.Y. Aug 13, 2009).

Victor Stanley II: New Landmark E-Discovery Sanction Decision

By John Blumenschein, Esq.
Copyright Fall 2010 by Guidance Software.

Victor Stanley, Inc. v. Creative Pipe, Inc., 2010 WL 3703696 (D.Md. Sept. 9, 2010)

Chief U.S. Magistrate Judge Paul W. Grimm has done it again, issuing another in a series of landmark e-discovery decisions. This time the decision focused on sanctions for spoliation of electronically stored information.

In *Victor Stanley, Inc. v. Creative Pipe, Inc.,* 2010 WL 3703696 (D.Md. Sept. 9, 2010) ("Victor Stanley II"), Judge Grimm wrote a 103-page virtual handbook on U.S. e-discovery spoliation sanctions law and issued a whopper of a sanction in what he characterized as the "most egregious example of spoliation that I have encountered in any case that I have handled or in any case described in the legion of spoliation cases I have read in nearly fourteen years on the bench." Specifically, he ruled that due to the intentional, bad-faith spoliation by Mark Pappas, president of defendant Creative Pipe, Inc., Pappas will be required to serve up to two years in prison if he fails immediately to pay the plaintiff's fees and costs related to its motions for spoliation of evidence. Given the years of e-discovery strife in this case (recall Judge Grimm's previous landmark decision in this litigation, now referred to as Victor Stanley I, 250 F.R.D. 251 (D. Md. 2008)), that will be one very large bill.

Aside from the two-year jail term sentence pursuant to the court's civil contempt powers, Judge Grimm's decision is also notable for its 12-page chart surveying spoliation sanctions across all the federal circuits. He notes in his decision that the disparate standards across the circuits, and sometimes even within circuits, cause "concern and anxiety" for organizations "because their activities—and vulnerability to being sued—often extend to multiple jurisdictions, yet they cannot look to any single standard to measure the appropriateness of their preservation activities, or their exposure or potential liability for failure to fulfill their preservation duties." He advised that counsel develop "safe" preservation policies by "design[ing] a policy that complies with the most demanding requirements of the toughest court to have spoken on the issue, despite the fact that the highest standard may impose burdens and expenses that are far greater than what is required in most other jurisdictions in which they do business or conduct activities." He also wrote that he hopes "this analysis will provide counsel with an analytical framework that may enable them to resolve preservation/spoliation issues with a greater level of comfort that their actions will not expose them to disproportionate costs or unpredictable outcomes of spoliation motions."

In addition, Judge Grimm pointed out that "the duty to preserve evidence relevant to litigation of a claim is a duty owed to the court, not to a party's adversary." He wrote that parties frequently forget this and engage in extensive discovery motion practice that not only places greater burdens and costs upon the parties but also directly interferes with the court's administration of justice by crowding dockets and "divert[ing] court time from other important duties—namely deciding cases on the merits."

Guidance Software Plays a Key Role in Case

Judge Grimm's decision repeatedly refers to the technical findings by plaintiff Victor Stanley's forensic expert, Andreas "Andy" Spruill of Guidance Software (publisher of *Real eDiscovery*). Using Guidance Software technology, Spruill handled many aspects of the forensic analysis discussed in the Victor Stanley II decision, including demonstrating that the defendant did not take any reasonable measures to put in place an effective litigation hold, uninstalled an external hard drive used as the backup device for Pappas' own computer and failed to preserve or produce the ESI likely written to that external hard drive before it was uninstalled. The court also relied upon Spruill's forensic analysis for findings that the defendant purposely deleted potentially relevant ESI after the preservation obligation came into effect, including the deletion of thousands of files followed immediately by the use of disk defragmentation software to render them unrecoverable. In addition the analysis demonstrated the defendant's failure to preserve or produce exchange server logs, the production of corrupted servers to plaintiffs and Pappas' likely personal involvement in spoliation.

Voice of the Corporation: The 30(b)(6) Witness

By Albert Barsocchini, Esq.
Copyright Spring 2009 by Guidance Software.

"Whether you are the party requesting the witness or the one producing the witness, it is key to pre-plan a strategy around your actions."

The volatility, malleability and dispersed nature of ESI have created new challenges to litigators trying to search, preserve, produce and authenticate this information. Therefore, it is important to inquire about the steps a corporate defendant or plaintiff took to identify, preserve, collect and produce documents relevant to the litigation. This requires detailed inquiry into a corporation's information management and retrieval systems to ensure that discovery was diligently completed in good faith. The target of this inquiry is the 30(b)(6) witness.

The 30(b)(6) witness has been around for some time. His or her role is to testify not on the facts of the case, but on a company's operations, such as its IT infrastructure or accounting practices. It is important to note that the 30(b)(6) witness's testimony represents the knowledge of the entity, not of the person being deposed. In the context of eDiscovery, this witness is often called to testify on the steps the corporation took to find and produce responsive documents to ensure discovery was diligently completed in good faith. In this context, the witness must be prepared to testify on such topics as location of ESI, access to ESI, how ESI is maintained and how this data was preserved for the subject litigation.

When opposing counsel request to depose a 30(b)(6) witness, the burden of identifying responsive witnesses lies with the organization. This rule streamlines the discovery process and facilitates meaningful deposition. Since the topics can vary greatly (including, qualifications and organizational structure, information systems, software and email, records management, alternative sources of electronic information, legacy systems, backup and restoration procedures, and the production of ESI in other lawsuits), it may take more than one witness to give meaningful testimony, especially for large corporations.

Rule 30(b)(6) and Designation of a Witness

The Advisory Committee on Civil Rules of the U.S. Courts explained that the Rule 30(b)(6) has three purposes:

- to reduce the difficulty a deposing lawyer encounters in determining, before the deposition, whether a particular employee or agent is the right person;
- to curb the practice of "bandying," where an entity's officers or managin agents are deposed in turn, but each denies knowledge of facts that are clearly known to people in the organization; and,
- to assist entities that find an unnecessarily large number of their officers and agents being deposed by a party uncertain of who in the organization has the relevant knowledge. The burden is therefore on the producing party to serve up the appropriate witness for deposition

depending upon the topical categories in a notice to produce. That is why the 30(b)(6) notice must designate "subjects" not "persons."

In addition, the witness not only has a duty to be knowledgeable on the subject matter of the inquiry, but also on subjects the entity should reasonably know as well. This means that, once designated as the so-called voice of the corporation, producing an unprepared witness is tantamount to a failure to appear sanctionable under rule 37(d). Many companies have lost the confidence of the court and discovery because of producing an unprepared witness. This introduces a number of new issues for the defendant to manage, sidetracking the defendant from focusing on the actual merits of the case.

Because the 30(b)(6) witness serves as a sort of storyteller for the company—detailing its policies and procedures—the need for and relevance of this witness becomes that much more important when a party has failed to produce any meaningful documents in response to a discovery request or appears to be uncooperative. This is because a compelling story could convince the court to spare a company from sanctions and other penalties. In order to reap the benefits of a knowledgeable 30(b)(6) witness in such instances, a company must thoroughly prep and groom the witness in advance.

Choosing the Right Approach

One of the key decisions a company needs to make when selecting its 30(b)(6) witness is whether to choose from its pool of internal personnel or to select an outside expert, as well as whether to rely on one or multiple witnesses to provide testimony.

This decision is complicated by the many challenges the witness faces. For example, large organizations are complex and decentralized with distributed IT networks. This makes it difficult for one person to be the key witness. On the other hand, small companies without IT departments usually rely on third-party vendors to provide expert testimony, which can be expensive over the long run. That is why it is so important to identify this witness before litigation begins and prepare them to meet the challenge. It is also important to note that this witness does not need personal knowledge or be the person most knowledgeable within the corporation. Rather, he or she only needs to possess institutional knowledge, i.e. all relevant information reasonably available to the corporation to adequately respond to the questions and categories identified in the notice, which often is no small task.

As mentioned, some companies opt to have an outside representative serve as their 30(b) (6) witness. However, doing so has its own set of problems. For example, keeping that witness up to date can present both a large cost and time burden. He or she also may not be available when needed. Yet, if your company outsources its IT departments in whole or part, designating someone from this third-party vendor as a 30(b)(6) witness is likely. That is why it is important to build in contractual provisions regarding the third-party 30(b)(6) witness, as well as preservation and production obligations and procedures when engaging the vendor.

Another area that impacts witness selection is international data protection laws. These laws

can severely impact a company's ability to conduct cross-border eDiscovery. In these instances, companies should opt for a witness who is prepared to discuss in detail the protocols and procedures for preservation and collection in countries with data protection laws. Topics may include cross-border investigative capabilities, safe harbor and binding corporate rules, etc. The testimony given may create collateral damage by providing evidence on whether the company was in compliance with applicable privacy laws.

30(b)(6) Strategies

Whether you are the party requesting the witness or the one producing the witness, it is key to pre-plan a strategy around your actions.

For parties producing the witness, selection and preparation of the witness is the linchpin that will determine success or failure of the outcome. Counsel should take great care in the preparation of each designated representative to ensure that he or she is fully prepared for the categories of inquiry contained in the notice, as well as any other relevant matters to the cause of action. Failure to prepare the corporation's designated representative fully could result in adverse testimony binding the corporation in the future.

However, since witness preparation is discoverable, be careful with what that witness is exposed to during preparation. For example, exposing a 30(b)(6) witness to privileged documents may create subjectmatter waiver of the specific privilege. Additionally, that witness may also become a fact witness besides a 30(b)(6) designee, which can cause additional problems. Also, for large corporations, it is wise to designate the same person as the 30(b)(6) witness for each request in order to battle harden them.

If you are the requesting party, be strategic with your use of a 30(b)(6) deposition in order not to lose credibility with the court and opposing counsel. Consider how you want the deposition to advance the merits of the case. Many lawyers draft sloppy requests by using boilerplate categories with little thought about the specifics of the case and asking for information that is designed more to harass than to find relevant information. The requesting party should also be prepared to make an appropriate motion for sanctions when the witness is nonresponsive, which may include such draconian measures as requesting expert access to the opposing party's network.

Furthermore, crafting the notice requires attention to details and balance because an overbroad notice will become susceptible to a motion to quash or strike. For example, some courts have stricken "but not limited to" language from deposition notice categories out of concern that language makes the topics overbroad. On the other hand, the witness may legitimately refuse to testify on topics that are not specified adequately or are overbroad in the notice.

When responding to a request, you must pay close attention to the 30(b)(6) topical categories in the notice and be prepared to address each one adequately. Failure to answer a specific category is sanctionable. To that end, counsel must be aggressive in clarifying the scope of categories. It is wise to use the meet and confer conference to define the scope and drive desired results. If all else fails, consider a protective order.

The bottom line is the requesting party must designate with reasonable particularity the topics on which the examination is requested, while the responding party must ensure that the designated witness is knowledgeable regarding the designated topics.

Some attorneys use the 30(b)(6) deposition as a cost-effective way to avoid more time-intensive discovery vehicles such as written interrogatories. On the other hand, others create extensive categories to draw out any time limitations on depositions. For example, FRCP 30(d)(1) states that unless otherwise stipulated or ordered by the court, a deposition is limited to one day of seven hours. The court must allow additional time, consistent with Rule 26(b)(2), if needed to fairly examine the deponent or if the deponent, another person, or any other circumstance impedes or delays the examination. Additionally, designating multiple witnesses to testify could have the consequence of allowing the requesting party seven hours per witness.

Companies should always consider the alternatives to 30(b)(6) deposition, such as written question and answers and informal reciprocal information exchange. Having a carefully drafted, canned response may be preferable to a live deposition if opposing counsel will cooperate. This is why it is important to think about the 30(b)(6) witness before litigation arises and create alternate game plans to negotiate with opposing counsel at the meet and confer conference.

In Conclusion

An effective, repeatable and defendable eDiscovery response plan requires an organization to proactively anticipate the type of discovery that could be initiated and develop an offensive strategy that employs both technology and human resources. Having the right witness and investing in defensible technology has always been the linchpin to the overall successful implementation of any litigation readiness plan. This witness is just as important as the technology used to identify, preserve, collect and process the ESI. To that end, eDiscovery has made the 30(b)(6) witness an invaluable tool for both the requesting and responding party.

"Having the right witness and investing in defensible technology has always been the linchpin to the overall successful implementation of any litigation readiness plan."

Recent eDiscovery Developments in Australia and the U.K.

By Chris Dale
Copyright Spring 2009 by Guidance Software.

In this issue of Real eDiscovery, guest columnist Chris Dale of the e-Disclosure Information Project analyzes twodevelopments, one from Australia and one from the U.K., which highlight some differences from U.S. norms.

New Australian Federal Court Practice Note No. 17

The new Federal Court Practice Note N o. 17 on the use of technology in the management of discovery and the conduct of litigation took effect on January 29, 2009. Its Related Materials include a Pre-Discovery Checklist, a Default and an Advanced Document Management Protocol and a Pre-Trial Checklist. The break-point beyond which the Advanced Protocol applies is 5,000 documents.

The Practice Note and its Related Materials provide a very detailed code which recognizes that electronic disclosure is a major cause of delay and expense, and tackles it in an extremely prescriptive manner. If it is enforced as is intended, the potential impact on litigation costs is considerable.

The Practice Note provides that an order may be expected requiring that discovery be given electronically and that the hearings be conducted in electronic format where "a significant number of the documents... have been created or are stored in an electronic format [and where] the use of technology in the management of documents... will facilitate the quick, inexpensive and efficient resolution of the matter." A "significant number" is defined a "in most cases, 200 or more."

The broad statements of purpose and expectation are supplemented by "observations." An example is that "Printing electronic documents for the purpose of discovery will generally be a waste of time and money." This approach is less prescriptive than any attempt to quantify or define, but leaves parties (and judges) with clear pointers as to what is appropriate. Parties are expected to have "discussed and agreed upon a practical and costeffective discovery plan" before the court makes any discovery order and must meet and confer about protocols for electronic exchange and "other issues." The use of an appropriate Document Management Protocol is mandatory, and it is here where the tone changes from generalized exhortation to detailed prescription. Structurally, that makes sense, not least because it is the detail which may need to be changed with experience, something the Practice Note expressly anticipates.

Apart from short references in the Pre-Discovery Checklist to the scope of discovery, a reasonable search and preservation of documents in their original format, there is almost nothing in the Practice Note about identification and collection, or about metadata. The detail goes mainly to the management and production of the documents and their use in court, and the focus is more on streamlining discovery as between the parties and with the court than on the front end of the process. That reflects the intended scope of the Practice Note—there are other sources, both statutory and in case law, which show that the Australian courts attach considerable significance to the manner of collection and the methods used.

BS 10008: The U.K.'s New Standards on Admissibility and Weight of Electronic Evidence

The U.K.'s approach to the quality of the evidence put before its civil courts is rather different than that which obtains in the U.S. It is not that the U.K. courts are lax about it—far from it—but they have fewer absolute standards as to what must be proved about data or documents. The courts are more interested in the weight which should be attached to a document than to pure questions of admissibility, and this is generally dealt with at trial. There are arguments that things should be otherwise. One is that the whole expense of trial might be avoided if there was more scope to argue admissibility points pre-trial. The counter-arguments include the risk of satellite litigation, the U.S. experience (which, rightly or wrongly, is not seen as a helpful path to follow), the fewness of cases which go to trial anyway, and the fact that summary judgment is available as a remedy where it can be said that an admissibility point makes a case unarguable. The other reason why more guidance on admissibility is helpful is that without a measuring pole, parties cannot assess what their strengths and weaknesses are in respect to documents with arguably doubtful pedigrees.

That pedigree is, of course, set long before litigation arises. Without any relevant statutory or case law definitions, an information manager finds little authority as to the courts' expectations as and when the data in his care is required as evidence.

To fill this gap, the British Standards Institute (BSI) released BS 10008: 2008 in November 2008. *Called Evidential weight and legal admissibility of electronic information*, it sets out in 30 pages the specification of requirements for planning, implementing, operating, monitoring and improving an organization's information management systems. Much of it seems obvious—you must have senior buy-in, you need a process, it must be tested—but there is clearly a need for it. Information managers will know much of it anyway, but it will give power to their elbow when they argue that IT systems and procedures should match generally accepted standards.

The BSI's output has no statutory force but, by setting out some standards, it helps a company measure itself against what others are doing. That in turn gives the court a yardstick when it has to consider questions of authenticity or chain of custody in weighing the evidential value of a document.

Legal Must Stay Actively Involved in Selecting eDiscovery Solutions

By Daniel Lim, Esq.
Copyright Spring 2009 by Guidance Software.

Many organizations have a committee of IT, Records Management, Information Security, and Legal professionals who are assigned the task of developing and improving eDiscovery processes. Typically, Legal is engaged in the initial stages of setting goals and requirements. However, once the task of evaluating, choosing, and implementing solutions begins, they often tend to disappear.

When this happens, organizations unknowingly embark on activities that result in unnecessary costs and delays. The danger of "scope creep" runs rampant, as narrowly-focused eDiscovery solutions projects become part of longer-term records management or compliance projects. The end-result is all too common: lots of time spent changing or re-arranging the proverbial haystacks of information sources, and scarce focus on determining ways to find and preserve the needles of relevant files within the existing haystacks.

Most organizations understand the need to invest in technologies that enable them to gather electronically stored information (ESI) quickly and efficiently, while preserving chain of custody and metadata. While a number of technologies appear to give similar messages of being able to meet these criteria, a world of difference exists in how they work, the time required for implementation, and overall effectiveness.

In a recent meeting with an organization's IT and Legal staff, I found that Legal asked IT to improve eDiscovery collection processes, with a mention of looking into email archiving solutions. IT then evaluated and invested in an archiving solution that was taking months to implement and complete. When I asked how the organization dealt with collecting ESI stored locally on computer hard drives for desktops or laptops, IT looked over at Legal and asked, "Is this something you need to acquire as well?" Legal looked back at IT and said, "Yes." Then, a moment of silence. Clearly, a disconnect existed between what Legal needed from a broader perspective for eDiscovery and the limited solution that IT had chosen.

Archiving and other records management initiatives are not a complete solution for eDiscovery. Discoverable ESI is much more than what exists in an archive, enterprise content management system, or other structured data source.

Moreover, eDiscovery is not simply extending an information management solution to manage more data sources. What's more important is to determine how best to collect and preserve ESI from existing sources for pending litigation— and information management solutions were not designed to do this.

The name of the game for eDiscovery is acquiring what is potentially relevant from reasonably accessible sources as quickly and efficiently as possible at the time an organization anticipates litigation and in a defensible manner. Legal, stay involved when your organization is choosing an eDiscovery solution! Your partners in IT need your input because you know the legal requirements. Also, your success depends on IT's ability to give you what you need, when you need it.

Seyfarth Shaw's Scott Carlson Provides Insight into How Clients are Handling eDiscovery

Copyright Spring 2009 by Guidance Software.

Scott Carlson is a partner and founder of Seyfarth Shaw's National eDiscovery Practice Group. Mr. Carlson provides clients practical solutions to eDiscovery and high technology issues through a combination of a strong technical background, including a B.S. in Computer Science and Mathematics, as well as significant litigation experience. Mr. Carlson and his group provide clients a wide range of eDiscovery services both from a litigation as well as an advisory services perspective. Mr. Carlson serves as National eDiscovery Counsel to companies throughout the United States.

Q: What do you hear most often from clients when working with them for the first time on an eDiscovery case or consulting project?

A: I frequently hear from companies that they just do not know where to start in developing a sound overall approach to eDiscovery issues. In that regard, I try to help clients assess where they are currently and come up with a plan that makes sense for them. In doing that, I try to take a close look at what kinds of litigation they regularly face, how much "pain" they currently feel with eDiscovery, what their IT landscape looks like, what in-house IT capabilities they currently have and whether their law department has a desire to take on more internal management of eDiscovery.

I find that through this assessment, companies can really focus on the portions of the eDiscovery process that will get them the "most bang for the buck." Sometimes developing some good written policies and practices are necessary. In other instances, modifying some IT policies will provide them real value. Sometimes software solutions make the most sense. The 80/20 rule is alive and well in eDiscovery. You need to take a good look at what you are doing now and focus on the 20 percent that yields the most results. And it doesn't have to be expensive. Sometimes, a change in IT policy, for example, can reduce IT costs and can also decrease eDiscovery risk.

Q: What is the most common misunderstanding about in-house eDiscovery that you've heard from clients?

A: The most common misunderstanding is the notion that someone can be "eDiscovery Compliant." There is no such thing, as the requirements to properly preserve and produce electronically stored information arise from common law and not from some particular statute that can be "complied with." There is no checklist that you can follow to correctly manage eDiscovery risks. Instead, as with any risk, companies must assess their exposure to the risk, identify how much risk they are willing to accept and determine the level of resources they are willing to expend to deal with the risk.

Q: At what point do you advise your clients to bring eDiscovery in house?

A: It depends. For more than five years, I have provided eDiscovery advice and counsel to clients all across the country, in different industries, with differing types and frequency of litigation and differing internal staffing of the law department. As I have worked with these various clients, it becomes clear

that there is no "one size fits all" approach. For some clients, it makes perfect sense to internalize a very large part of the eDiscovery process. For other clients, they may not have the desire or the culture that would make them successful at internalizing the process. So fundamentally, I suggest to clients that they look closely at each step of the eDiscovery process, understand the risks and costs associated with that step and make determinations about what steps, if any, it makes sense to internalize.

Q: If there was one thing you'd advise Corporate Counsel to do, what would that be?

A: Make your preservation process more rigorous through more formal preservation policies and practices. I believe that the frequency and severity of sanctions is on an increase and that we are far from seeing a plateau. The inherent difficulties and challenges associated with eDiscovery have not lessened over time. Sure, many people have become more sophisticated about the issues, but navigating them in a complex case remains a very difficult task. Many judges believe enough time has passed since the 2006 Amendments to the Federal Rules of Civil Procedure, and that there have been enough eDiscovery seminars that the problems just shouldn't be there anymore. Simply put, while the issues remain difficult, judges are often less patient and less forgiving in resolving eDiscovery disputes. Clients need to be ready to demonstrate to a court that they have a rigorous and thoughtful approach to eDiscovery—particularly on the preservation front.

"You need to take a good look at what you are doing now and focus on the 20 percent that yields the most results. And it doesn't have to be expensive. Sometimes, a change in IT policy, for example, can reduce IT costs and can also decrease eDiscovery risk."

Understanding Legal Hold Technology; Email Archiving for eDiscovery?

By Matthew Miller, Esq.
Copyright Spring 2009 by Guidance Software.

Are Email Archiving Solutions Suitable as eDiscovery Solutions?
– Vice President of Litigation, Consumer Packaged Goods, Fortune 1000

When an organization is evaluating solutions for internal eDiscovery processes, the right choice is a tool that can get the job done in a scalable and effective manner under tight deadlines, while providing legal defensibility. A defensible eDiscovery process is repeatable, systemized and meets legal requirements for proper handling and admissibility of computer evidence.

Though email archiving can be useful as a complement to other eDiscovery efforts, it is not a complete solution. An ideal eDiscovery solution identifies, collects, preserves, processes, reviews and produces relevant electronically stored information (ESI). Relevant information may be found in unmanaged, unstructured, semi-structured or structured data sources dispersed across networks on desktops, laptops, servers, share drives, removable storage media, and other devices.

As the name implies, email archiving is limited to the contents of an email system. Because these solutions work only with the set of emails that reside within the archive, search and collection capabilities do not extend to all data on the network. Using a solution that does not address all sources of relevant information can expose a business to significant legal risks. To protect yourself, you would likely need to either purchase more software or contract with a vendor for other tools capable of identifying potentially relevant information from all of your systems and devices beyond the email system. Obviously, this also adds to your organization's eDiscovery costs.

Some email archiving vendors may claim that their technology is a complete eDiscovery solution, satisfying requirements set forth in the FRCP. If you hear such a claim, please consider the following: email archiving systems were designed for email management purposes and therefore do not address content outside of the email system.

In short, email archiving can be a useful tool, but it is by no means a replacement for a complete eDiscovery software solution.

What Should I Look For in a Legal Hold Solution?
– Deputy General Counsel, Financial Services Company, Fortune 500

Applicable law requires preservation of potentially relevant information when litigation can reasonably be anticipated.

Organizations should therefore look for legal hold software that has the ability to actually enforce legal holds at the earliest outset of litigation. The software should address the duty to preserve relevant information through custodian identification, hold notification, questionnaires, document preservation and hold releases. Reports that track holds along with the collection and preservation of ESI are all needed to prove that organizations have satisfied their duties.

Many current legal hold solutions do not provide an integrated technical means to systematically collect and process custodian data subject to legal hold. Instead, they merely send and track emails to custodians while promoting custodian self-collection. In fact, custodian self-collection has drawn harsh scrutiny from the courts and presents risks such as non-compliance, spoliation, inadequate chain of custody, authentication challenges and business disruption. Also, certain legal hold solutions promote a "preserve-in-place" methodology that changes file permissions on a custodian's files so that a document cannot be altered. This poses two risks: first, if a user has administrative rights on their computer (and many do), the custodian can still delete the file; and second, it is unnecessaril intrusive to custodians, who have to make a copy of the so-called "preserved" file in order to modify it and make use of it in day-to-day business.

Using a process that is planned, systemized and scalable is ideal, as an ad-hoc, manual, custodian-reliant process can result in undue burden and expense. This can be accomplished by a tool that not only provides the notification, but also enables collection and preservation of relevant ESI in a forensically sound manner (including metadata) so the ESI cannot be destroyed by the employees.

Recent Court Ruling Underscores Importance of File Metadata Preservation

Copyright Winter 2009 by Guidance Software.

Influential U.S. District Court Issues Mandates Demonstrating that Metadata Preservation is Critical throughout the eDiscovery Process

In Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dep't of Homeland Sec., a United States District Court issued a definitive ruling providing that the U.S. Federal Rules of Civil Procedure require that metadata associated with emails and electronic files be preserved, maintained and produced in the course of legal discovery, particularly where the requesting party seeks its production in its initial request. This case reaffirms that the preservation of electronically stored information including its associated metadata throughout the eDiscovery process is critical, and that a party to litigation faces significant legal risk if they do not collect and maintain digital evidence with technology designed specifically for the task.

As eDiscovery best practices are delineated and ultimately determined by the courts, this case is particularly important as it dispels any uncertainty concerning the legal requirements for metadata preservation. In arriving at its decision, the Aguilar court cited recent case law, as well guidance from the influential Sedona Conference, who recently revised their statement of eDiscovery principles to emphasize the importance of metadata preservation in the course of discovery. The Aguilar court explained that file metadata is important to help establish the authenticity of electronically stored information, to enable accurate and effective search, sorting and analysis of the data, and also because the metadata itself has relevant evidentiary value.

The Aguilar decision underscores the importance of eDiscovery technology, such as EnCase® eDiscovery software, that preserves metadata throughout the eDiscovery process, including the processing stage. Most eDiscovery solutions fail to preserve file metadata at the collection and/or processing and early assessment stages. As a result, organizations risk significant legal exposure by producing electronically stored information with compromised metadata, or incur substantial increased cost by engaging in a time consuming, manual processing effort to reset the file metadata to its original, pre-collection state.

EnCase eDiscovery is unique in that it fully captures and preserves file metadata at the point of collection and then preserves the metadata in place throughout the eDiscovery workflow, including processing, analysis, and load file generation. Many other collection methods alter the metadata and nearly all processing and early case assessment technologies fail to keep file metadata intact. EnCase eDiscovery provides the dual benefit of reducing eDiscovery costs while reducing risk with a court-validated preservation process.

Bringing eDiscovery Processing In-House

By Patrick J. Burke, Esq.
Copyright Winter 2009 by Guidance Software.

"Done correctly, culling and filtering before the processing stage will allow you to achieve as much as 50% cost savings on the overall cost of eDiscovery, including attorney review and hosting."
– John Rosenthal Partner and Head of the eDiscovery Practice at Winston and Strawn, LLP

Processing is one of the most expensive—and least understood—aspects of eDiscovery. Until recently, corporate eDiscovery teams had little choice but to outsource processing to service providers.

But this has changed. Technology is available that enables in-house eDiscovery teams to perform eDiscovery processing themselves.

Processing takes electronically stored information (ESI) that has been collected, and filters and deduplicates the data to cull it down, performs various technical processes (including text extraction, decompression, decryption, and sometimes indexing), and converts all the data into a format suitable for review by attorneys.

A primary goal of processing is to reduce the data set down to just what is potentially responsive to litigators' needs. Keeping in mind that first-pass attorney review (for relevance, privilege and to identify hot documents) typically costs between $5 and $7 per document, there are significant savings in applying automated processes to cull out irrelevant data.

Some in-house eDiscovery solutions enable companies to cull the data down prior to the processing stage, at the point of collection. In fact, John Rosenthal, Partner and Head of the eDiscovery practice at Winston & Strawn LLP, states that organizations can achieve significant cost savings from culling during collection.

"Done correctly," says Rosenthal, "culling and filtering before the processing stage will allow you to achieve as much as 50% cost savings on the overall cost of eDiscovery, including attorney review and hosting."

So how does technology help reduce the total data volume for attorney review?

During the collection phase, some in-house solutions can search and collect for only email and particular user-created file types (e.g. Word, Excel, PowerPoint, etc.). This excludes known irrelevant file types (e.g. system files) and vastly reduces the volume of data collected. This type of software can also collect data that was created or modified within a particular timeframe, or only emails and/or electronic files containing certain keywords. During the processing phase, in-house technology takes the collected data (already at a smaller volume if culled at the point of collection) and filters it further by keywords, timeframes and file types.

Another important way to reduce the data set is through deduplication, which eliminates bit-by-bit identical versions of a document and leaves one copy for the attorneys to review while keeping track of which custodians also held duplicate copies of reviewed files.

"Anywhere from 10 to 20% of all collected files are often exact duplicates of one another," explains Rosenthal. "If you can extract these duplicates at the processing stage, you can save a tremendous amount of money."

Optional in the process is indexing, whereby the raw text of all the files is compiled into a comprehensive text index against which keyword searches can be performed. This stage is optional if you are using software that can perform effective keyword searches directly against the emails and files themselves, without generating an index. But sometimes it can be useful to pass a pre-created index for use in the attorney review stage.

Processing can also involve "hashing" all collected files. Hashing refers to a process that uses mathematical algorithms to create unique digital fingerprints for files or datasets to prove that they have been preserved without any changes. This is important because it is a means by which one can authenticate an electronic document by demonstrating that it has not been altered during the eDiscovery process.

"Hashing has become more important now that you see more and more native productions," observes Rosenthal. "With native productions, the hash value is the only way—at this point in time—that you can verify that the document produced and, later on, used at trial, is the same document and hasn't been changed."

The remaining features of processing focus on delivering the data to the chosen review platform in a format that will allow the attorneys to review it effectively.

The delivery to the review platform is accomplished by creating a load file, but before it is created, the in-house eDiscovery software extracts text from files, or data contained within zip files (or from zip files within zip files), decompresses data inside compressed files, and de-crypts encrypted data. It is important that the different components of the document, such as the text and metadata, are not only extracted,but that the proper relationships among those components (e.g., between an email message and its attachments) are maintained when passed along to the attorney review platform. With that accomplished, in-house software can create load files that comply with the new EDRM-standard XML load file format, as well as in Concordance, Summation or native file formats.

"You have to be careful here," explains Rosenthal, "because while a lot of commercial systems generally can deal with different review formats, not all of them can. One of the benefits I like about EnCase® eDiscovery is that its has the ability to not only process the documents, but also to put the documents into one of the three most common commercial attorney review formats, pretty much 99% of commercial platforms."

In-house eDiscovery teams collecting and processing their own ESI can choose whatever attorney review and hosting solution makes the most sense for that particular case. This can be particularly valuable when they use multiple law firms for litigation, as the different firms will have their own preferences for (and experience with) different hosting services and attorney review platforms.

In some cases, the preferred attorney review platform is one that does not call for any hosting fees at all. By eliminating service providers from the eDiscovery process, the in-house team has more options, provided that their in-house processing technology permits creation of load files that are compatible with each of the applicable review platforms.

The cost advantages of in-house processing are self-evident. Rather than pay premium rates to outsource vendors, companies can process for free if they invest in a perpetual license for in-house eDiscovery software. For companies that do not have the capital budget to do this, there is in-house

eDiscovery software that can be licensed on a pay-per-use basis (e.g. EnCase eDiscovery). Either way, companies will pay less than what is charged by outsourced vendors.

With a clearer understanding of the details of processing, corporate eDiscovery teams no longer need to rely on these services from outsource vendors. They can comfortably bring the process in house—and enjoy order of magnitude savings.

The Keyword vs. Concept Search Debate

By Albert Barsocchini, Esq.
Copyright Winter 2009 by Guidance Software.

As more and more organizations begin to investigate different in-house eDiscovery technologies, the debate regarding the validity of electronic discovery production based on a keyword search has become increasingly heated. Concept search vendors are now claiming that recent rulings on the use of keywords demonstrate that an eDiscovery production based on a keyword search is not as effective, reliable and defensible as other methods.

A closer look at the opinions, however, reveals that these rulings are being misinterpreted. Courts are not criticizing the effectiveness or reliability of keywords; rather, judges are simply pointing out the fact that lawyers must have a defensible and systemized process when conducting a keyword search.

For instance, In *Victor Stanley v. Creative Pipe Victor Stanley, Inc. v. Creative Pipe, Inc., —F.Supp.2d—, 2008 WL 2221841* Chief US Magistrate Paul W. Judge Grimm held that ignorance is not an excuse when using keywords to identify potentially relevant documents and privileged documents. He further states that because keyword search technology is prone to producing over- and under-inclusive results, attorneys using keyword searches should adopt one of two approaches. Either collaborate with the opposing party to agree on a keyword search methodology, or utilize keyword search best practices to demonstrate to the Court that they have taken reasonable measures to reduce over- and under-inclusiveness.

The use of concept search in ediscovery productions is relatively new, however in the eyes of the court, it is a "black box" technology, employing proprietary algorithms and formulas to search and cull electronically stored information (ESI). When vendors are asked to justify or explain these processes in court, they demur, claiming that they cannot provide a complete description of the company's technical processes for competitive reasons. As this technology cannot be explained, it is not transparent. Thus, the Court cannot adequately assess the reliability of concept search technology within the context of the case.

A keyword search is transparent because what you search for is what you get. If you search for the term "Pistachio," for example, you will get all instances of that term and nothing else. Therefore, explaining a keyword search to a judge is much easier than explaining how complex mathematical algorithms find all words similar to "Pistachio" across the company's network. Additionally, the newer concept search technologies tend to generate significantly more false positives than a keyword search; false positives increase data volumes, thereby increasing processing costs and attorney review time.

As an emerging technology, concept search has a lot of promise. It can be helpful for enhanced filtering during the processing phase with a large data set and categorizing documents for attorney review. That said, it needs more judicial exposure before becoming an established search tool in the eDiscovery toolbox.

A keyword search, when used properly (see sidebar) remains a highly defensible and effective culling strategy compared to a concept search. The important point to remember is that civil discovery is based on good faith and reasonableness… not Euclidean precision.

New Decision Holds Attorneys to Reasonable Inquires

By Patrick Burke, Esq.
Copyright Winter 2009 by Guidance Software.

Mancia v. Mayflower Textile Services Co., 253 F.R.D 354 (D. Md. 2008)

Chief Judge Grimm strikes again! In his October 15, 2008 decision in *Mancia v. Mayflower Textile Services Co.*, 253 F.R.D 354 (D. Md. October 15, 2008) (hereinafter "*Mancia*") Grimm sets out an impressive legal framework to support holding attorneys to more stringent obligations to make "reasonable inquiries" to ascertain whether requests, responses or objections are complete, correct and not for improper purposes. The decision also pulls together persuasive support for an increased duty to cooperate with adversaries.

Paul W. Grimm, the Chief U.S. Magistrate Judge for the District of Maryland, has written many of the most influential eDiscovery decisions of the past few years, most recently the *Victor Stanley v. Creative Pipe* decision that has quickly become the leading case on eDiscovery privilege waiver. He was assigned this Fair Labor Standards Act case—*Mancia*—in which the plaintiff employees alleged that the defendants failed to pay overtime and made illegal deductions from their wages—for the purpose of resolving all discovery disputes, which were plentiful. In the end, he found violations on both sides, faulting defendants' boilerplate objections and plaintiffs' extensive discovery requests. He did not, however, order monetary sanctions. Rather, he sent the parties back to the negotiation table, with a detailed roadmap on how to come to agreement on a reasonable scope for eDiscovery, develop factual support through reasonable inquiry for better particularized responses, requests and objections, and to cooperate with their adversaries.

The *Mancia* decision may someday be seen as a watershed decision, recognizing enhanced duties of "reasonable inquiry" and cooperation in the conduct of those attorneys who sign eDiscovery responses, requests and objections. Grimm throws a spotlight on the oft-ignored Rule 26(g), which he calls "[o]ne of the most important, but apparently least understood or followed, of the discovery rules…." 253 F.R.D. at 357. The rule requires that responses, requests and objections be signed by counsel to be effective.

This signature requirement is Judge Grimm's springboard into a newly recognized list of duties, as Rule 26(g) deems it a certification that "to the best of the person's knowledge, information and belief formed after a reasonable inquiry" the disclosure is complete and correct, and that the discovery request, response or objection is consistent with the rules, not interposed for an improper purpose, and is neither unreasonable nor unduly burdensome or expensive. Such a certification is not insignificant, and Judge Grimm argues that when such certifications cannot be supported by evidence that such "reasonable inquiry" was ever undertaken, that the courts should routinely sanction counsel and parties.

The *Mancia* decision will likely be remembered as a significant milestone in the evolution of the legal obligation for attorneys to behave cooperatively in eDiscovery matters. Judge Grimm first does this by showing that while the American jurisprudence systems encourages zealous advocacy,

it also always favors relaxing that advocacy during discovery. In making the case for a stronger duty to cooperate during the eDiscovery process, Judge Grimm lends his reputation and keen reasoning to the Sedona Conference's recent "Cooperation Proclamation", which launched a "national drive to promote open and forthright information sharing, dialogue (internal and external), training, and the development of practical tools to facilitate cooperative, collaborative, transparent discovery."

Judge Grimm's *Mancia* decision gives a huge lift to the Sedona Conference's Cooperation Proclamation. We may some day point to this decision and say "that is when the federal courts began routinely imposing sanctions for eDiscovery abuses and failure to cooperate."

Verizon Continues Its Goal of Using Technology to Become Self-Reliant in the eDiscovery Process

Copyright Winter 2009 by Guidance Software. Reprinted with permission.

Patrick Oot is Director of Electronic Discovery and Senior Litigation Counsel at Verizon in Washington, DC. Mr. Oot is considered one of the nation's leading experts on electronic discovery. He has extensive experience in commercial litigation, regulatory filings and antitrust matters, and is charged with advising Verizon's business units on electronic discovery while developing new technologies that increase cost-efficiency.

Q: How did you become involved in eDiscovery?

A: I was introduced to legal technology while working on a large contract dispute for Verizon Vice President and Head of Litigation, John Frantz. This was Verizon's first significant matter that required the engagement of an external eDiscovery service provider to process, manage and host large volumes of litigation data. That case triggered my interest in legal technology. Since I met him on that case in 2002, John has been a major champion of the electronic discovery program at Verizon. In 2005, John paired me with Jaideep Singh, Director of Electronic Discovery IT Strategy & Planning. While I primarily deal with vendors and outside counsel, Jaideep vets internal systems and uses his many years of experience in Verizon's IT group to navigate the collection and legal hold processes.

Q: What interests you about this specific area of law technology?

A: eDiscovery is the new frontier. The law is developing with every ruling. Decisions in the cases we work on today have significant influence on future cases to come. Electronic Discovery is the one area of law that is undoubtedly growing.

I think my most interesting work focuses upon our continued Federal Rules reform campaign. Anne Kershaw, Founder, Senior Attorney & Consultant, A. Kershaw, P.C. Attorneys & Consultants, and I jointly testified before the Federal Rulemaking Committee on the proposed Federal Rules of Evidence (FRE) 502. We educated the committee on the costs of privilege review in litigation and regulatory filings. Our testimony resulted in the enhanced protection of privilege for litigants on both sides of the "v." It also gave parties the ability to screen for privilege using advanced search technology (as a reasonable precaution to protect privilege under the new rule). President Bush signed the proposed rule into law this past September.

Q: What type of eDiscovery solution did your firm use before?

A: Last year, Verizon started using EnCase® Enterprise for its legal collection needs. Our team was extremely satisfied with the solution's collection process, especially in how it supports Verizon's continued effort to standardize collection practices between corporate, wireless and business.

In prior years, Verizon's eDiscovery team collected electronically stored information (ESI) using one of several methods. For most cases, we were using software internally developed by our desktop support team. The application allowed an operator to collect data over the network while the legal

team conducted a case interview of the employee over the phone; the process could best be described as a collection over a Webex connection. This internal application replaced outside attorneys and paralegals traveling to collect with external drives. Also, for a few cases, where deleted files might have been crucial to the case, our team took an in person bit-for-bit image of target drives. In person collection took significant time and travel, and needs were determined on a case by case basis.

Q: In your opinion, what is the ROI for pay-per-use in-house eDiscovery?

A: As Verizon's litigation volume increases, our security team requires the tools to respond to our collection needs more rapidly. Our litigation data volumes are increasing, while our headcount is not. Our team is looking to Pay-Per-Use EnCase eDiscovery to streamline our collection process and provide transparent response times to our in-house managing attorneys.

Q : What are your plans for the future?

A: Verizon Security and Verizon Electronic Discovery have jointly submitted a business case to corporate finance to fund the deployment of the software and hardware to continue our goal to become more self reliant in the EDRM process. Our business case clearly shows that buying licenses and hardware is more cost effective for Verizon than using service provider models.

"Our litigation data volumes are increasing, while our headcount is not. Our team is looking to Pay-Per-Use EnCase eDiscovery to streamline our collection process and provide transparent response times to our in-house managing attorneys."

Selecting the Right eDiscovery Solution; Preserve in Place vs. Collect to Preserve

By Michael Rhoden, Esq.
Copyright Winter 2009 by Guidance Software.

What are the basic characteristics/features/requirements for an eDiscovery solution that I should look for when considering such a product?
– Milan Chestovich, Senior Counsel, AK Steel

As you evaluate different in-house eDiscovery products, look for the following characteristics/features/requirements:

1. A solution that can handle legal hold notification, collection, preservation, processing, review and production within one comprehensive solution. This allows you to keep all collected data in one application, decreasing the risk of loss of data integrity that can occur when data is transferred from one application to another.
2. A solution that integrates litigation hold notification with collection and preservation. This gives your organization the ability to truly enforce the legal hold by collecting and preserving potentially relevant electronically stored information (ESI) at the same time that the hold is issued.
3. A solution that offers integrated processing capabilities. This enables your organization to have complete control over the processing phase and gives you a wide range of options for hosting and attorney review. You can choose an outsourced provider, or you can use popular platforms like Concordance or Summation to conduct the attorney review of documents.
4. A solution that preserves file metadata and the file itself inside a court approved digital evidence container. This helps to ensure that your eDiscovery production will not be challenged in court. It is important that the software's preservation technology has a proven track record for validation and approval in different jurisdictions, and if applicable, different countries.

Can you explain the distinction between the preserve-in-place and collect-to-preserve approaches, including how this might cause you to recommend one type of eDiscovery solution over a other?
– Senior Litigation Support Specialist, Fortune 500 Biotechnology Company

"Preserve in place" refers to preservation of archived data formats, such as back-up tapes, email archives and scanned document repositories—items that are not altered in the normal course of business. However, recently the term has been expanded to refer to "locking down" files currently in use wherever they are found, including files on custodians' computers. The risk and inconvenience of using "preserve in place" for documents currently in use by the custodian limits its usability for eDiscovery preservation.

"Preserve in place" does not actually collect files in a forensically defensible manner. Once a document is "locked down," the custodian must make a copy of the file to edit and use for business

purposes. If the file is on a computer of a custodian who is also an "administrator" on that computer, it may be possible to override the in-place preservation. In addition, leaving a file in place on a computer in the possession of a custodian exposes the data to greater risk of accidental or purposeful destruction. Finally, the metadata and unique hash value of the file may be altered when "locked down," rendering proof of chain of custody and duplicate identification difficult or impossible.

"Collect to preserve" is the method that data forensics and eDiscovery professionals use when preserving potentially relevant evidence. This method uses digital investigation or eDiscovery software to create a copy (which is an original under the Federal Rules of Evidence) of the target data (often filtered by keywords, dates, or other parameters). The software verifies the accuracy of that copy by generating a Hash or CRC value, then preserves the copy, along with its exact state and metadata, within a court approved file format. By quickly preserving data out of the stream of use in the regular course of business, you can minimize business disruption, the burden of "preserve in place" data management and the risk of spoliation. If you are collecting data for submission in court or for proof of compliance to regulators, use an eDiscovery solution that uses the "Collect to preserve" method.

eDiscovery Spoliation Sanction Milestone: Monetary Sanction Imposed on an In-House Counsel

By Patrick J. Burke, Esq.
Copyright Winter 2010 by Guidance Software.

Swofford v. Eslinger, 2009 WL 3818593 (M.D. Fla. Sept. 28, 2009)

It finally happened—a federal court has issued eDiscovery sanctions against an in-house counsel that was not an attorney of record or a party in a litigation. The decision comes from U.S. District Court Judge Mary S. Scriven of the Middle District of Florida in *Swofford v. Eslinger*. Robert and Sharon Swofford brought the lawsuit after Robert was shot seven times by deputies of the Seminole County Sheriff's Office (SCSO) who apparently believed Swofford was a car burglary suspect.

The sanctioned in-house counsel is David Lane, defendant SCSO's General Counsel, whom the Court found was "the sole lawyer responsible for responding to the preservation letters." Lane failed to ensure that email, electronic files and other potential evidence was preserved despite receiving two preservation letters, as well as a notice of intention to sue and a public records request for particular information including email communications related to the shooting investigation. Lane testified that the only action taken by anyone at the SCSO in response to the preservation letters was to forward copies to a half-dozen senior SCSO employees including the Sheriff. Otherwise, neither Lane nor the Sheriff nor the SCSO employees who received copies of the letters did *anything* to see that the SCSO complied with its obligation to preserve. This inaction continued even after plaintiffs filed their spoliation sanctions motion. Lane testified that he had not "ever read the Federal Rules of Civil Procedure to ascertain on even a rudimentary level what his and his client's obligations were in this regard." Judge Scriven concluded that "[n]othing other than bad faith can be inferred from the facts of this case."

Judge Scriven explained that she was imposing the sanctions against Lane "pursuant to both the Court's inherent authority and 28 U.S.C. §1927." The outside lawyers that litigated the case on behalf of the SCSO were not sanctioned "because there is no evidence to establish that any outside counsel contributed to or failed to prevent the spoliation…."

The Court ordered that adverse inference instructions be given to the jury with respect to the lost email and electronic documents. It also ordered that the defendants and Lane, each in their official capacity, shall reimburse plaintiffs for the costs, expenses and attorneys' fees reasonably incurred as a result of the sanctionable conduct. Plaintiffs claim to have incurred over $300,000 in costs and attorneys' fees to bring and prove the sanctions motion. The parties were ordered to attempt to stipulate to the proper amount of the monetary sanction and—if they are not able to reach agreement—the Court will hold an evidentiary hearing to resolve the issue.

eDiscovery and the Cloud; Judges Pushing Companies to Insource eDiscovery?

By Albert Barsocchini, Esq.
Copyright Winter 2010 by Guidance Software.

Nowadays, with people using online email services, how much could we discover from a local disk? – Dexter H.
Manager, Business Development and Technical Support
Infinity Forensics Limited of Singapore

Before probing the technical challenges of recovering electronically stored information (ESI) from online email services, a company lawyer first should determine whether their client in fact has a legal obligation under court rules to preserve such ESI stored in the cloud. (The "cloud" refers to the delivery of business applications and services through the Internet, usually accessed from a web browser.)

The general rule of law is that a company must produce all relevant or potentially relevant ESI in its possession, custody or control. When the company outsources its corporate email services and/or storage to an online email provider or a "cloud" computing application, courts likely will find that—while outside the company's possession or physical custody—employees' emails stored through the company's arrangements in an outsourced "cloud" nonetheless are within the company's legal control. See, e.g., *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008) For this reason, many companies insist in their contracts with these services that there be specific and detailed provisions regarding security, location, management, preservation obligations, eDiscovery collection protocols, and access to all the ESI.

The preservation obligation is far less certain with respect to ESI created and stored on employees' personal email or social media platforms such as Google, Facebook, Twitter or Yahoo. Companies generally cannot lawfully reach directly into an employee's personal online email or social network postings (although the situation may be different if the information is cached on a workplace computer, as described below). It is likely a court today would find an employer does not have an obligation to preserve ESI stored in the cloud on these individuallycontrolled platforms because the company has neither possession, custody, or control. For this reason, some companies' acceptable use policies ban or discourage employees from using any of these media for business communications.

The only exception may be an obligation to preserve any residual ESI that reasonably can be found somewhere in the possession, custody or control of the company. Forensic examination and collection of ESI will focus on any data artifact remaining on the end user's computer in the web cache. Forensic solutions such as EnCase are able to capture not only the surviving cached image of ESI, but also its metadata including when the data was created or last accessed.

I have been hearing that judges are starting to push companies to consider bringing eDiscovery in-house. How do judges view the issues?
– Anonymous

Companies of all sizes have been weighing whether to bring electronic discovery in-house and, if so, which specific functions or capabilities to bring in-house. The developing trend is that the judiciary now considers the legal hold, collection, and preservation functions core capabilities that corporations should have in-house.

For example, in October 2009 noted eDiscovery authority Ralph Losey published on his blog a video interview with Magistrate Judge Craig Shaffer and former Magistrate Judge Ron Hedges, in which the judges were quite emphatic:

> "The day is coming… I think judges are going to start saying 'Don't come to me, large organization, and tell me that you can't do this or that, when you really haven't tried to internalize it.'" – Former Magistrate Judge Hedges

> "You really, organization, need to start getting something developed in-house, and you can't rely, for example, on individuals to do self-collection anymore." – Former Magistrate Judge Hedges

> "I think the days are probably coming to an end where companies are simply going to bring in an outside vendor…" – Magistrate Judge Shaffer

They are by no means unique among the judiciary. The judicial decisions described below provide further insight on what to expect from courts on this topic.

In *Phillip M. Adams & Assocs., L.L.C. v. Dell, Inc.,* 2009 U.S. Dist. LEXIS 26964 (D. Utah Mar. 27, 2009) the Court found it unacceptable for a party to hide behind inadequate information management systems as the reason why it could not produce relevant documents. Similarly, in *Spieker v. Quest Cherokee, LLC*, 2009 WL 2168892 (D. Kan. July 21, 2009), the defendant was admonished by the Court for claiming that it did not have the in-house expertise to collect the requested ESI. "This court is aware of no case where a party has been excused from producing discovery because its employees 'have not previously been asked to search for and/or produce discovery materials'."

Finally, in a new decision (issued Jan. 15, 2010) by Judge Shira A. Scheindlin of the U.S. District Court for the Southern District of New York, *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities*, Case No. 05 Civ. 9016 (SAS) 2010, sanctions were issued against plaintiffs for, among other things, indefensible in-house eDiscovery processes and capabilities, including: (1) failure to issue timely, written litigation hold notices, and (2) careless and indifferent collection efforts. Judge Scheindlin noted that litigants "at a minimum… must act diligently and search thoroughly at the time they reasonably anticipate litigation."

These statements and opinions by judges in various districts highlight the emerging minimum standards for corporate litigants: if you want to avoid sanctions, you should have the capability to promptly execute litigation holds and ESI collections.

Protecting Privilege with FRE 502

By Patrick Oot, Esq. and John J. Rosenthal, Esq.
Copyright Winter 2010 by Guidance Software.

Patrick Oot is an experienced corporate attorney who currently serves as General Counsel and Co-founder of The Electronic Discovery Institute, a nonprofit organization dedicated to resolving litigation challenges by conducting studies of litigation processes for the benefit of the federal and state judiciary.

John J. Rosenthal counsels clients on electronic discovery and risk reduction from electronic discovery. He is Litigation Partner in the Washington, D.C., office of Winston & Strawn LLP and serves as Chairman of the firm's eDiscovery and Electronic Information Management Practice Group.

Over the past decade, the exponential growth of electronically stored information (ESI) being preserved has had an enormous impact on an organization's ability only to disclose the non-privileged and relevant evidence during litigation. The traditional "gold standard" of document review, whereby attorneys manually reviewed each page of ESI for privilege prior to production, did not result in a high level of precision due to the voluminous number of documents. The result was that privileged and non-relevant documents were being produced to opposing parties in litigation; this often resulted in the waiver of protections normally afforded a producing party. In addition, the cost and time consumed in this traditional approach were staggering and often disproportionate to the amount in controversy in a case. Certain studies have concluded that the sheer volume of ESI exceeds the ability for human accuracy and consistency when compared to results achieved by software programs tailored to filter and search the data.

The studies, among other factors, have helped raise concerns in the legal community and resulted in amendments to Federal Rule of Evidence 502 (Rule 502) in late 2008. The amendments to Rule 502 provide guidance as well as better legal protection for a claim of inadvertent waiver of privileged communications involving ESI. The amendments read as follows:

- 502(a) Severely limits the scope of subject matter waiver by confining waiver only to the information disclosed, unless fairness dictates otherwise;
- 502(b) Mandates non-waiver for intentionally disclosed documents when reasonable steps are taken to prevent disclosure and the producing party took reasonable steps to correct the error;
- 502(c) Limits the instances when a litigant can carry a disclosure in a state court proceeding to a federal proceeding;
- 502(d) Encourages the use of protective orders and mandates court ordered non-waiver for any other federal or state proceeding;
- 502(e) Encourages the use of protective orders by suggesting confidentiality agreements only bind the parties to them unless it is incorporated into a court order;
- 502(f) Binds state courts to a federal court's determination of non-waiver;
- 502(g) Defines attorney-client privilege and attorney work-product doctrine.

The amendments now provide a federal standard governing the impact that inadvertent disclosure has on the attorney-client privilege. Rule 502 recognizes and establishes a process for parties to secure protection and extend the consistent reach of federal waiver decisions to other forums.

The core protection Amended Rule 502 provides is a reduction of the risks associated with large volume ESI productions. This is accomplished by defining when a disclosure may be considered inadvertent, and if so, when it should not be considered a waiver of the privilege. See *FRE Rule 502(b)*. Further, the Advisory Committee Report to Amended Rule 502 includes a multi-prong test drawn from the common law, setting out factors which courts should consider when evaluating a claim of inadvertent disclosure. The factors include:

- the reasonableness of the precautions taken by the producing party;
- the amount of time the producing party took to notice and correct the error;
- the scope of discovery;
- the extent of discovery; and,
- the over-riding issue of fairness[960].

The Advisory Committee also suggests factors courts can use to determine the reasonableness of the precautions including:

- the number of documents the producing party had to review for the production;
- the time constraints for production;
- the producing party's use of software applications and linguistic tools in privilege screening; and,
- the implementation of an efficient prelitigation record management program[961].

Since Rule 502 was amended, many courts have relied upon the Rule to resist finding waiver when privileged electronic documents were disclosed. See *Coburn Group LLC v. White cap Investors LLC*, 2009 U.S. Dist. LEXIS 69188 (N.D. Ill. Aug. 7, 2009) (supervised paralegal privilege review was reasonable, so the disclosure of one privileged email was inadvertent and a non-waiver in 40,000 page production); *Multiquip, Inc., v. Water Mgmt. Sys. LLC*, 2009 WL 4261214 (D. Idaho Nov. 23, 2009) (non-waiver for a document disclosed to a third party due to the use of an "autofill" feature which court concluded was not unreasonable and prompt steps taken to rectify this error); *Heriot v. Byrne*, 2009 U.S. Dist. LEXIS 22552 (N.D. Ill. Mar. 20, 2009) (non-waiver when disclosure was vendor error after reasonable steps taken, finding that the Rule does not require "post-production review").

Courts have also found waiver of privilege, however, when applying the Rule 502 criteria. See *CFA-NC Townridge Square, LLC v. Exxon Mobil Corp.*, 2009 WL 3763032 (S.D. Fla Nov. 10, 2009) (intentional disclosure of selected work product under FRE 502(a) was subject matter waiver as to certain related documents not disclosed); *U.S. v. Sensient Colors, Inc.*, 2009 WL 2905474 (D.N.J. Sept. 9, 2009) (waiver because plaintiff failed to reasonably "rectify the error" of disclosure per FRE 502(b)); *SEC v. Badian*, 2009 WL 222783 (S.D.N.Y. Jan. 26, 2009) (privilege was waived when producing party took no precautions at all, then took five years to request 260 privileged documents be returned.) In

960 See Report of the Advisory Committee on Evidence Rules, at http://www.uscourts.gov/rules/Reports/2007-05-Committee Report-Evidence.pdf.
961 Id.

nearly all cases in which the court found waiver occurred, had the parties agreed on a court ordered FRE 502 non-waiver order, the outcome would likely have been different.

In addition to learning from the early case decisions above, a party to litigation should establish an action plan to determine what "reasonable precautions" they will undertake to protect their privileged communications and attorney work-product. A litigant's search methodology has increasingly become an issue in privilege waiver disputes. As the Advisory Committee Notes to Amended Rule 502 state, litigants deploying culling and search strategies using "advanced analytical software applications and linguistic tools" may be found to have taken reasonable steps to protect privilege thereby potentially avoiding waiver. Guidance Software's EnCase® eDiscovery, with its search capabilities, is a perfect example of advanced analytical software that is capable of assisting organizations in taking the reasonable precautions necessary to avoid inadvertent disclosure.

Furthermore, Amended Rule 502 emphasizes the importance of securing a protective order to manage and resolve inadvertent disclosure issues between the parties. In some cases, a properly drafted protective order may eliminate the need to involve the court in disclosure disputes. In others, the protective order serves as a guide to the court in ruling on the dispute. Language may also be incorporated into a protective order that could bind whether parties can carry a state court disclosure to a federal proceeding, as well as bind state courts to a federal non-waiver decision. A protective order should be written with sufficient detail to address not only the inadvertent disclosure protocol but also consideration of a cost-effective privilege logging process. Given the potential high volume of privileged communications contained in email "strings" for example, addressing a privilege logging process in a protective order could decrease costs dramatically by defining the necessary steps up front.

If a producing party understands Rule 502 protections and seeks cooperation with opposing parties to enter a protective order governing inadvertent disclosures, litigation risks can be reduced and a more efficient—and cost effective—discovery process can result. In addition, incorporating software applications and linguistics tools into the privilege review will bolster a party's claim of inadvertent disclosure should the protective order fail to address a waiver issue during litigation.

"As the Advisory Committee Notes to Amended Rule 502 state, litigants deploying culling and search strategies using 'advanced analytical software applications and linguistic tools' may be found to have taken reasonable steps to protect privilege thereby potentially avoiding waiver."

It's Time to Bridge the Gap Between eDiscovery, Internal Investigations, Audit and Compliance

By Albert Barsocchini, Esq.
Copyright Winter 2010 by Guidance Software.

"There is a clear and present need to become 'investigation ready' and have a unified response practice and single technology platform to mitigate risk and avoid non-compliance. "

Beginning in 2009 and continuing into 2010 we are seeing corporate legal departments take a unified focus on the mission critical functions of internal investigations, eDiscovery, audit and compliance because of the global convergence of these practice areas. There is a clear and present need to become "investigation ready" and have a unified response practice and single technology platform to mitigate risk and avoid non-compliance.

With more onerous regulations and increased litigation, corporations are struggling to reduce the risks and costs associated with electronically stored information (ESI) which are potentially subject to investigations and litigation. In this regulatory environment, legal risks are extreme and therefore it is important that companies have proper governance and compliance controls in place.

The key benefits of taking a unified approach include: nurturing an ethical culture and avoiding risk through a comprehensive and effective program, diligently managing risks on an enterprise wide basis, maintaining adequate staff and resources, being proactive and adapting to regulatory and legal changes, and being able to continuously and consistently update the compliance program from lessons learned.

Traditionally these practice areas have been separate corporate functions an rarely brought under a single roof from a technology or departmental resource point of view. Corporate legal departments need to take ownership of the process because of increasing pressure from new regulations and judicial scrutiny of the process used to conduct investigations.

The risks of not having a unified defensible investigative process are similiar too.

Failure to properly identify, preserve and authenticate important relevant evidence in a timely manner can substantially affect the outcome of a case and lead to legal and regulatory sanctions.

To be sure, the failure to have a defensible and consistent process can lead to severe draconian legal and regulatory consequences including criminal prosecution, monetary sanctions, increased regulatory scrutiny, and negative publicity that can impact a company's bottom line.

The investigative technique that all types of investigations have in common is to timely identify, preserve, process and present the evidence to the appropriate forum. An effective response plan requires an organization to proactively anticipate the type of investigations and audits needed and develop an offensive response strategy.

Aligning compliance strategies and response under one roof will enhance the risk response capabilities, reduce the frequency and severity of operational surprises and losses, help to identify and manage multiple and cross enterprise risks, and improve the effectiveness of a company's capital deployment.

Technology is the linchpin to the overall implementation of any response plan. When looking for

enterprise technology to handle multiple types of digital investigations, look for technology that can search for evidence over the network from a central location, collect the evidence in a forensically sound manner and properly preserve all metadata.

Additionally, having technology that can also do a network-based forensic examination is important for IP theft, SOX investigations and HR cases.

Ultimately, the goal is to establish a legally defensible response plan that builds upon prior experience, provides a common language and establishes an effective evidence lifecycle management framework to minimize risk and increase the effectiveness of an investigation. Combining these practice areas will provide an organized business workflow that efficiently combines people, processes and technology.

For cost, efficiency, consistency and to mitigate risk, it is now good corporate governance to have a comprehensive, unified and defensible process for all types of investigations.

Judge Andrew Peck on Keywords, Cooperation, Privacy and What Sherlock Holmes Teaches About eDiscovery

Copyright Winter 2010 by Guidance Software.

U.S. Magistrate Judge Andrew Peck is one of the eDiscovery thought leaders in the federal judiciary, an author of respected teaching decisions in the eDiscovery area and a sought-after speaker to legal audiences in the U.S. and Europe. He has served as a U.S. Magistrate Judge for the Southern District of New York since 1995. Prior to that he was a litigator with Paul, Weiss, Rifkind, Wharton & Garrison. Judge Peck plays an active role in the Sedona Conference and the Georgetown Advanced eDiscovery Institute. He is also an active member of the Baker Street Irregulars, a literary society specializing in Sherlock Holmes.

Q: Last year you published your decision in William A. Gross Constr. Assocs. v. Am. Mfrs. Mut. Ins. Co., 2009 U.S. Dist. LEXIS 22903 (S.D.N.Y. Mar. 19, 2009), which has been lauded as a "wake up call" to litigants. What were you waking litigants up to?

A: First, the need to cooperate in general. Second, more specifically, to use good processes/techniques in constructing keyword searches, including transparency with opposing counsel, consultation with the knowledgeable business people at the client to learn what words, abbreviations, etc., they use, and the need to test the proposed keywords for under and over inclusiveness. As I summarized in the opinion, "where counsel are using keyword searches for retrieval of ESI, they at a minimum must carefully craft the appropriate keywords, with input from the ESI's custodians as to the words and abbreviations they use, and the proposed methodology must be quality control tested to assure accuracy in retrieval and elimination of 'false positives'."

Q: What advice would you give to in-house counsel who are seeking to upgrade their internal corporate eDiscovery processes and technology to be defensible?

A: Preservation is the most important issue: you need to keep whatever is required for regulatory and business needs, and the more organized your approach to records retention and management, the lower your cost likely will be when in litigation. That includes a record retention system that encourages the elimination of ESI that is not needed to be retained. But once litigation is reasonably anticipated, you must immediately put a litigation hold in place. A litigation hold email is the first step, but cannot be the last—the case law requires hands on communication to key employees, most likely face-to-face.

Q: You have spoken to audiences in Europe on the conflict between U.S. requirements for preservation and production of relevant ESI and EU data protection. What is the response of European courts and data protection officials to demands for ESI preservation and collection for U.S. litigation? What do you see as the way forward on reconciling conflicting priorities?

A: Privacy is considered a fundamental human right in Europe. It goes beyond material we view as confidential, such as Social Security numbers and bank account or credit card numbers, to the person's

name or other identifying characteristics. Thus, if Employee A sends a memo or email to Employee B, their names are considered private and thus the company cannot preserve and produce that email in U.S. litigation. A targeted request under the Hague Convention may be the only way to satisfy EU data protection authorities. There is a dialog going on, but only time will tell how much progress can be made in reconciling broad U.S. discovery and EU data privacy protections.

Q: You are known as an authority on Sherlock Holmes, recently quoted in the press about the new Guy Ritchie film, "Sherlock Holmes." Are there any lessons from your Sherlock Holmes scholarship that are applicable to eDiscovery?

A: Litigators today, whatever their age, must be competent in eDiscovery issues. One cannot say, "Look at my grey hair Judge; how do you expect me to understand these computer issues." So like Inspector Lestrade and the other Scotland Yard detectives who called on Holmes when they were "out of their depths" in a case, if you cannot learn how to do eDiscovery yourself, you need to associate with a Holmes-like eDiscovery expert, whether as eDiscovery counsel or perhaps employing a vendor or expert. eDiscovery is simply not "elementary."

"Litigators today, whatever their age, must be competent in eDiscovery issues. One cannot say, 'Look at my grey hair Judge; how do you expect me to understand these computer issues.'"

Best Practices for Public Sector eDiscovery Collection

by Daniel Lim, Esq.
Copyright 2008 by Guidance Software.

Daniel Lim is an Assistant General Counsel for Guidance Software, Inc. He consults with Guidance Software clients on eDiscovery and digital investigation issues in both the commercial and government sectors. He speaks regularly on legal issues related to eDiscovery, including developments following the recent changes to the Federal Rules of Civil Procedure. Prior to joining GSI, Daniel worked for the Jones Day law firm in Houston, TX. Daniel is a graduate of Columbia Law School.

I. Introduction

The risk associated with electronic discovery depends upon the effectiveness of a litigant's preservation and collection efforts. Since 2004, public sector agencies and corporations involved in high-stakes litigation have incurred sanctions and hundreds of millions in collective losses because of their failure to demonstrate defensible eDiscovery preservation and collection policies and procedures. US courts have not hesitated to apply recently enacted amendments to the Federal Rules of Civil Procedure (FRCP or Federal Rules) to respondents required to produce discovery documents to opposing counsel. Since December 2006, several US courts have invoked these new FRCP amendments in their rulings on evidence and discovery, establishing a heightened degree of scrutiny to this critical aspect of eDiscovery collection and preservation.

As courts weigh in on eDiscovery requests and challenges, issues surrounding the discovery of Electronically Stored Information (ESI) within the public sector continue to gain prominence. From deleted White House e-mails to large-scale ESI collection requests by class action suits against the government, parties, agencies and courts are now analyzing the nuts and bolts of ESI collection and preservation for the purposes of investigation and litigation. Additionally, the ever-growing burden of responding to FOIA requests is gaining increased media attention, as public sector agencies are tasked with increasing demands to demonstrate the responsiveness and accuracy of their ESI search and collection processes.

Much of the high cost and risk related to eDiscovery stems from poor collection practices, resulting in over-collection and other inefficiencies. Millions of dollars are spent per case on the collection, preservation, and processing of ESI. By utilizing best-practices polices and procedures combined with court validated technology, government agencies will be able to produce documents that flow through the entire eDiscovery cycle more effectively, at a considerable cost savings.

Public sector organizations taking a proactive approach to eDiscovery are prepared for litigation and FOIA support before discovery requests become issues requiring higher-level government involvement and/or intervention. By implementing the appropriate eDiscovery technology solution, public sector organizations can realize significant cost and resource savings.

To help government entities understand how to mitigate the potentially staggering risks and costs of eDiscovery collection and preservation, this paper will present a legal overview of current best practices for collecting and preserving ESI. This paper will cover the following topics: (1) why maintaining an established and systematic eDiscovery process is essential, particularly for public

sector entities; (2) the appropriate role of computer forensics when collecting and preserving ESI for eDiscovery purposes; (3) the importance and defensibility of targeted search strategies, and (4) considerations for determining whether the eDiscovery collection and preservation process should be outsourced or executed internally.

II. The Critical Importance of an Established eDiscovery Process and the Perils of Custodian Self-Collection

One of the most important aspects of the new FRCP amendments is their attention on the electronic discovery issues that typically arise in the early stages of litigation. For example, the newly amended rules require that relevant electronic evidence be identified, preserved and disclosed at the outset of litigation proceedings, thus necessitating, among other requirements, an effective process to meet these obligations for more stringent preservation. The Committee Advisory Comments to amended FRCP Rule 26(f) provide that: "failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes." Comments to Rule 37(f), the so called "Safe Harbor" provision, discussed the necessity of an effective litigation hold capable of preserving data at the outset of a case.

Under the new FRCP guidelines, parties must convene (per Rule 26(f)) to discuss the preservation and production of ESI. At the subsequent Rule 16 case management meeting, usually held within weeks of filing the lawsuit, counsel must be prepared to discuss ESI preservation already undertaken in the case, including details of their executed litigation hold. An influential 2007 manual written for the Federal Judiciary underscores the importance of these early meetings:

> All too often, attorneys view their obligation to 'meet and confer' under Federal Rule of Civil Procedure 26(f) as a perfunctory exercise. When ESI is involved, judges should insist that a meaningful Rule 26(f) conference take place and that a meaningful discovery plan be submitted.[962]

Under these new rules, litigants face a greater likelihood of Court sanctions for any failure to properly preserve relevant ESI at the outset of litigation. Recent cases involving the Federal Rules amendments underscore the need for a defensible eDiscovery preservation and collection process. In these important decisions, courts are carefully scrutinizing efforts undertaken by corporations and public sector agencies to execute litigation holds and discovery collection as they render decisions on motions to compel and sanctions.

A recent example of this heightened scrutiny of the federal government is United Med. Supply Co., Inc. v. United States, 77 Fed. Cl. 257 (Fed. Cl. June 27, 2007). A contractor brought suit against the United States for over $20 million in lost profits and other damages stemming from a contract to provide medical supplies to military medical treatment facilities (MTFs). The United States Court of

962 *Managing Discovery of Electronic Information: A Pocket Guide for Judges*; Federal Judicial Center, 2007 Barbara J. Rothstein, Ronald J. Hedges and Elizabeth C. Wiggins.

Federal Claims imposed sanctions against the United States based upon the "reckless disregard of its duty to preserve relevant evidence." In this case, a Justice Department attorney sent document hold notices via e-mail based on outdated and inaccurate MTF e-mail listings. As a result, relevant ESI was lost or destroyed after the litigation hold went into effect. In awarding sanctions, the Court observed:

> It is the duty of the United States, no less than any other party before this court, to ensure, through its agents, that documents relevant to a case are preserved. Indeed . . . as the enforcer of the laws, the United States should take this duty more seriously than any other litigant. . . . [T]he court concludes that it must impose spoliation sanctions against the United States.
>
> *United Medical Supply, 2007 WL 1952680 at *15 (emphasis added).*

The Court cited the new FRCP eDiscovery amendments, specifically Rule 37(f), finding that a finding of "bad faith" was not necessary to impose sanctions for failure preserve ESI.

This heightened scrutiny continues even in commercial cases. The most notable case over the past year is Qualcomm, Inc. v. Broadcom Corp., 2008 WL 66932 (S.D. Cal. 2008). In this case, over 46,000 electronic files were not produced before trial. The Court initially awarded $8.5 million in sanctions, including all of Broadcom's attorneys' fees and costs incurred in the litigation. Several attorneys were also referred to the California Bar for investigation and possible punishment for ethics violations. The Court affirmed that as to the legal standard for sanctions under FRCP 37 (sanctions for parties and attorneys for failure to comply with discovery obligations and court orders), "[t]here is no requirement under this rule that the failure be willful or reckless; **sanctions may be imposed even for negligent failures to provide discovery"** Qualcomm, slip op. at 14 (emphasis added).

Another ESI issue rapidly growing in importance is authentication, a process which often requires specific tracking of both source and metadata. In Williams v. Great-West Healthcare, 2007 WL 4564176 (N.D. Ga. June 8, 2007), the Court excluded racially-charged e-mails from summary judgment evidence. The Court noted that under F.R.E. 901(b), "appearance alone is not sufficient to authenticate a document."

> There is no question that the contested documents appear to be e-mail communications. However, the circumstances surrounding the documents do not mitigate in favor of admitting them. The requirement that there be something more than the appearance of the item is particularly important with respect to documents that can be easily altered, such as those generated by computer. Williams, 2007 WL 4564176 at *3.

The sentiment that ESI should undergo closer analysis of source and metadata is also being reflected in cases involving the government. See United States v. O'Keefe, 2008 WL 449729 at *5 (DC February 18, 2008) "A piece of paper of electronically stored information, without any indication of its creator, source, or custodian may not be authenticated under Federal Rule of Evidence 901".

The unmistakable message from these cases is that diligent and effective ESI preservation and

collection efforts are required under the FRCP amendments and are expected as a matter of course going forward. public sector entities that rely on custodian self-collection or otherwise fail to establish a defensible and systemic eDiscovery preservation and collection process do so at their own risk.

Litigants are often penalized due to the mistaken belief that ESI can be properly self-collected by the custodians themselves. This approach, which is subject to process attacks similar to the cases outlined above, has many pitfalls, including the following:

- Non-compliance: Custodian self-collection efforts are fraught with neglected litigation hold notices, missed data, cursory efforts or even intentional spoliation. Even when custodians afford proper effort, it is nearly impossible to clearly document and defend the specific search, retrieval and collection efforts of each custodian. Manual efforts, by definition, are non-systemized and do not allow for the documented, consistent application of objective criteria for ESI collection across multiple custodians.

- Metadata Alteration: File metadata, which is often relevant information itself or required for authentication, will be permanently lost or altered. For example, if a custodian forwards his/her own emails and other documents to a central location, key metadata fields, like file modification dates — will be compromised, thus calling into question the completeness and/or accuracy of the data collection. Decisions on several recent cases have shown that file metadata must be preserved and produced.[963]

- Authentication Challenges: Custodian self-collection does not generate an automated chain of custody and thus will likely (and unfortunately) require employees' personal testimonies to explain their efforts.

- Scalability: Custodian self-collection beyond a few individuals is highly disruptive and involves substantial logistical challenges, requiring extensive coordination and project management.

- Expense: The notion that custodian self-collection is less expensive is a myth. Inefficient collection efforts result in increased back-end processing and review costs; larger cases require hundreds of hours of additional project management fees by outside counsel or consultants.

To address these concerns, many government entities along with numerous global corporations are establishing a highly operational, systemized process to address ESI requirements as a part of their standard litigation practices in place of more reactive and ad hoc approaches. The traditional "wait-and-see" approach to eDiscovery — where the organization and counsel defer addressing ESI until its production is demanded by opponents — results in a disjointed approach to ESI collection typified by

963 See *Williams v. Sprint/United Management Company* 230 F.R.D. 640, 646 (D. Kan. 2005) (Court ordered production of spreadsheet files "in the manner in which they were maintained, which includes the spreadsheets' metadata."); see also, *Nova Measuring Instruments Ltd. v. Nanometrics, Inc.,* 417 F.Supp.2d 1121, 1122 (N.D. Cal. 2006); *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.,* 2006 WL 665005 at *1, (N.D. Ill. Mar. 8, 2006).

hurried outsourcing or other non-systemized custodian self-collection and preservation efforts. Such practices are no longer sustainable. Only with an integrated, systemized and efficient internal process that employs best practices technology and methodology at the outset of each case will government entities be able to routinely identify and preserve relevant ESI and establish reasonableness in the eyes of the Court.

III. The Scope of the Preservation and Collection Obligation

Once it is established that a defensible ESI preservation and collection process is needed, public sector agencies begin to ask questions about the scope of the required preservation and the methodology for a coordinated collection effort. Are full-disk images of every custodian's hard drive necessary? What is the benefit and proper role of computer forensics in the eDiscovery collection equation? What about reliance on archiving solutions? Must the entire email system be searched? Can search and collection be narrowly tailored to include documents from only specific custodians, during specified timeframes and containing certain keywords?

1) No Duty To Preserve Irrelevant Information

The duty to preserve evidence, including ESI, extends only to potentially relevant information. Kronisch v. United States, 150 F.3d 112, 126 (2d Cir.1998). Zubulake IV recognized no legal duty exists to "preserve every shred of paper, every email or electronic document and every backup tape … Such a rule would cripple large corporations." Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2004).

The FRCP amendments echo this rule, recognizing the need for a "balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party's routine computer operations could paralyze the party's activities." FED. R. CIV. P. 26(f) Advisory Committee's Note (2006 Amendment). The Advisory Committee Notes further provide that preservation efforts need only be "reasonable" and "narrowly tailored" to relevant information. Id.

Courts consistently agree that only potentially relevant materials fall within the duty to preserve ESI. Thus, preserving parties should be able to use best practices technology to identify and collect potentially relevant materials through defined search criteria. This thinking is reflected in several of the following cases.

Treppel v. Biovail Corporation, 233 F.R.D. 363 (S.D.N.Y. Feb. 6, 2006) provides that defined search strategies are appropriate in cases involving electronic data where the number of documents may be exponentially greater than paper discovery. In support of this decision, the Treppel Court cited from the Sedona Principles, which states "A responding party may properly access and identify potentially responsive electronic data and documents by using reasonable selection criteria, such as search terms or samples."[964] Similarly, in Zubulake v. UBS

964 The Sedona Principles; *Best Practices Recommendations & Principles for Addressing Electronic Document Production,* Principle 11 (2003).

Warburg LLC, 2004 WL 1620866 at *8 (S.D.N.Y. July 20, 2004) ("Zubulake V"), the Court advocates a targeted search approach where litigation holds are executed by running "a system-wide keyword search" involving a process where the responding party can "create a broad list of search terms, run a search for a limited time frame and segregate responsive documents…"

In Flexsys Americas LP v. Kumho Tire U.S.A., Inc., 2006 WL 3526794 (N.D. Ohio Dec. 6, 2006), the Court agreed on a compromise solution to a broad request for ESI, recognizing the burden of searching through years of electronic files for a large entity. Accordingly, the Court agreed to limit the defined searches to certain individuals "most likely to have information relevant to the arbitration issues."[965] See also U.S. v. Greathouse, 297 F.Supp.2d 1264 (D. Or. Oct. 20, 2003) (In this case, the Court suggests that the advent of technology "like EnCase" will require law enforcement to conduct narrowly tailored on-site keyword searches instead of seizing entire computers).

The 2006 FRCP amendments likewise support a targeted search and collection strategy. The Advisory Committee Notes to Rule 26(f) point to provisions of the sample case management order in the Manual for Complex Litigation, which provides:

> [t]he parties should attempt to reach agreement on all issues regarding the preservation of documents, data and tangible things. These issues include … the extent of the preservation obligation, identifying the types of material to be preserved, the **subject matter, time frame, authors** … and **key words** to be used in identifying responsive materials…[966]

2) Full-Disk Images Are Not A Routine Requirement For eDiscovery Preservation

Collection and preservation of ESI must incorporate a defensible process that preserves relevant data, including metadata, and establishes a proper chain of custody. With the right technology, these results can be achieved without full-disk imaging. However, full-disk imaging and deleted file recovery are emphasized by many eDiscovery vendors and consultants as routine eDiscovery practices. While deep-dive analysis is required in some circumstances, full-disk imaging is unwarranted as a standard eDiscovery practice due to the considerable costs and burdens faced by the parties involved. Large-scale full disk imaging is burdensome because the process is very disruptive, requires much more time to complete, and, as eDiscovery processing and hosting fees are usually calculated on a per-gigabyte basis, costs are increased exponentially.

---

965 *Id.* Also, the Court emphasized the importance of having a defensible e-discovery process. The plaintiff in responding to the motion to compel asserted a blanket response that it had either produced all documents at issue or that no such documents exist. In view of the fact that the defendant was able to demonstrate that other relevant documents existed, the Court found plaintiff's response to motion and explanation of electronic discovery efforts "lacking." *Flexsys Americas,* 2006 WL 3526794 at *3.

966 Manual for Complex Litigation § 40.25(2). (emphasis added).

Currently, there is no known case law requiring full-disk imaging as a routine means of collecting ESI in the context of eDiscovery. To the contrary, several recent decisions provide that forensic mirror-image copies of computer hard drives are not generally required for eDiscovery production. In Diepenhorst v. City of Battle Creek, 2006 WL 1851243 at *3, (W.D. Mich. June 30, 2006), the Court declined to require the production of full-disk images absent a strong showing of good cause, noting that the "imaging of computer hard drives is an expensive process, and adds to the burden of litigation for both parties…" The Court further noted that "imaging a hard drive results in the production of massive amounts of irrelevant, and perhaps privileged information." Ameriwood Industries, Inc. v. Liberman, 2006 WL 3825291, (E.D. Mo. Dec. 27, 2006). Id. at *4 (citing McCurdy Group v. Am. Biomedical Group, Inc., 9 Fed. Appx. 822, 831 (10th Cir. 2001)). See also, Balfour Beatty Rail, Inc. v. Vaccarello, 2007 WL 169628 (M.D. Fla, 2007) (Court rejects discovery request for production of copies of hard drives as overbroad and unwarranted).

Generally, Courts will only require that full forensic copies of hard drives be made if there is a showing of good cause supported by specific, concrete evidence of the alteration or destruction of electronic information or for other reasons. Balboa Threadworks, Inc. v.Stucky, 2006 WL 763668, at *3 (D. Kan. 2006); However, "[c]ourts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in a lawsuit are unduly vague or unsubstantiated in nature." Ameriwood Industries, 2006 WL 3825291 at *4.

3) Archiving and Enterprise Content Management Are Not Complete or Efficient Solutions For eDiscovery

Enterprise content management and archiving solutions were originally designed for records management, rather than entity-wide search and collection. They are geared for the management of business or official records and workgroup collaboration, rather than large-scale computer investigations. However, business or official records are a subset of all discoverable ESI in any government entity for purposes of litigation. Records management tools simply cannot scale to perform the distributed search, collection, storage, management and review of several terabytes of ESI for the purposes of eDiscovery --- especially under tight deadlines. When investigating which technology to implement for ESI collection, one should look towards a product with extensive court validation and proven evidentiary collection methods. Additionally, Forrester Research is skeptical of the "Archive Everything" approach to collection of ESI for eDiscovery:

> *Archiving everything means that everything is discoverable. Efficient eDiscovery finds information quickly without any system downtime. Managing large archives results in slower search queries and the need for more advanced culling tools to minimize the responsive information set. In addition, many clients report*

> *significant problems managing the indexes required with large archives. If your index breaks every six months and you need to continually re-index, you have erased the risk mitigation benefit that you thought you were achieving.*
>
> eDiscovery Best Practices, Forrester Research, Inc., Sept. 24, 2007.

The fragility of records management indexes is one of many key examples of how records management solutions are not scalable eDiscovery solutions. Indexing a relatively small subset of records for purposes of records management is a far cry from the intensity and scale associated with an eDiscovery collection requiring a systematic search of all locations where data that is potentially relevant to an investigation is stored. Further, even if all the relevant terabytes of ESI were to be successfully collected and migrated to a central repository, if the resulting index breaks, it would likely set the effort back several weeks, if not months.

Finally, indexing or storing every record within a government entity may be seen as overkill in relation to what is required for eDiscovery under the FRCP. The rules and developing case law do not require an entity to index or store every file on its network in order to respond to a discovery request for ESI. Rather, the scope of the preservation obligation is to preserve only potentially relevant ESI at the time of the litigation hold. The approach of EnCase Enterprise is to quickly search and retrieve potentially relevant ESI if and only if a litigation hold is put into place. Rather than spending months, or in some cases, years indexing every file on a network (or attempting to find all of the files to store in an archiving or ECM solution), you could search for and collect responsive ESI only when and if it is needed. If there is no pending need to search and collect the ESI, it may be left alone and allowed to follow its own lifecycle under the established records retention policy.

In sum, while all US government entities must establish a systemic and defensible process to search, preserve and collect relevant ESI, such efforts need not be overly broad and thus unduly burdensome. In fact, an effective eDiscovery collection process is one that will facilitate compliance while mitigating costs.

IV. The Benefits and Defensibility of a Targeted In-House Collection Process

A key decision for counsel is whether the organization should establish an internal eDiscovery search and collection process run by trained IT personnel equipped with the proper technology and training, or should the company rely on hired service providers. With a process that is largely outsourced, a government entity can expect to incur tens of millions of dollars in out-of-pocket costs annually, mostly in the form of outside consultant fees for data collection and processing. Additionally, using an outside vendor would automatically increase the risks of data leakage and potentially compromise the chain of custody. As much of the expense and shortcomings associated with a non-systemized eDiscovery process occur in the collection phase, an internal, systemized capability offers both cost savings and improved compliance with the amended FRCP

In addition to considerable cost savings, establishing a systemized and consistent process reduces end-user disruption and mitigates risk by enhancing compliance. As noted above, the "early attention"

requirements of the amended FCRP mandate that entities identify, preserve and collect relevant ESI at or near the outset of a litigation matter. A systemic process executed with plugged-in, scalable enterprise tools, run by a well-trained internal team that is very familiar with the IT infrastructure and works closely with legal counsel will enable a government entity to be well-suited to meet these stringent requirements.

In fact, recent case law fully supports the defensibility of large organizations handling eDiscovery internally. In addressing best practices for the searching and analysis of computer evidence, the judge in Zubulake V Court advised counsel to work closely with IT to develop a process for identifying relevant sources of computer data and to execute on preserving, collecting and searching that data.[967] In Williams v. Massachusetts Mutual Life Insurance Company, 226 F.R.D. 144 (D. Mass 2005), the Court found that the eDiscovery investigation performed by internal IT security personnel at Massachusetts Mutual was proper and competent. Notably, Mass Mutual relied upon the testimony of its CISO regarding the thoroughness and competency of the investigation to establish a defensible process and defeat the plaintiff's motion to compel further discovery.

Conversely, in Residential Funding Corp. vs. DeGeorge Financial, 306 F.3d 99 (2nd Cir. 2002), the Court found it unreasonable for Residential to continue to retain an eDiscovery service provider who was unfamiliar with the client's data storage systems. Residential's eDiscovery provider admitted to the Court that "technical problems" prevented the timely and cost-effective retrieval of sought computer data. One of the many benefits of an established and internalized process is that the key nuances and details of the organization's IT systems are accounted for, the network and key ESI storage locations are mapped and procedures to rapidly preserve and collect relevant ESI are in place in advance of the next case.

This is not to say that eDiscovery service providers are not an important part of the process. Many consultants help organizations design efficient and systemized processes that are largely executed by IT. Consultants can also effectively augment staff for larger engagements, as well as routine overflow. Outsourcing is also a good option for mid-sized organizations with a lighter litigation volume. To be sure, an untrained, ill-equipped and unprepared internal IT team could be the worst option available. However, with the right technology, people, training and well-defined procedures, an internalized process is proving to be the most effective eDiscovery collection and preservation method for large government entities and corporations.

V. Effective Enterprise Technology: The Foundation of a Defendable Process

Establishing a defensible process is a critical element of compliance, as opposing counsel are now routinely seeking to capitalize on the eDiscovery struggles of large government entities and organizations. Claimant's lawyers, in particular, seek to distract the defense by creating a "litigation within a litigation": allegations of spoliation or lack of due diligence in complying with eDiscovery requests. Plaintiffs seek to gain a significant advantage by obtaining evidentiary sanctions, petitioning the Court for an order allowing their own experts to investigate defendants' systems, or they drive up

967 *Zubulake v. UBS Warburg LLC,* 2004 WL 1620866 at *8 (S.D.N.Y. July 20, 2004).

the cost of litigation by forcing costly and over broad computer evidence investigations. Within the new framework provided by FRCP amendments, these tactics will only increase.

An established, scalable enterprise investigation capability can be a powerful shield against these tactics. For instance, EnCase® Enterprise is based on court validated EnCase technology utilized by law enforcement and is specifically designed to perform efficient and effective enterprise computer investigations for judicial purposes. (See, e.g., Sanders v. State, 191 S.W.3d 272, (Tex. App. 2006) cert. denied, 127 S. Ct. 1141, 166 L.Ed.2d 893 (U.S.), (Court takes Judicial Notice of the reliability of EnCase, finding "EnCase is a 'field standard' for forensic computer examination). The software features integrated reporting and logging capabilities to document all search and collection efforts for a proper chain of custody. Such a solid foundation of credibility and reliability provides government entities with a highly defensible and diligent process to establish compliance and confidence with the Courts in eDiscovery matters. In light of the new Federal Rules' clear and consistent emphasis on the importance of properly preserving and identifying relevant ESI, large government entities cannot afford to forgo such a scalable, systemized — and thus defensible— process in place.

The identification and preservation of ESI is a technical process that requires a technical solution, especially if a government entity has plans to establish these technical capabilities on an integrated, routine basis. An established and automated eDiscovery preservation and collection capability, based upon best practices technology such as EnCase® Enterprise, will provide a scalable, systematized and highly defensible process. Such a system will preserve and collect data while protecting metadata, establish a solid chain of custody, and document and log all search and collection parameters and results. Documentation generated by an automated and consistent technical process is presumed accurate under the Federal Rules of Evidence[968] and can qualify as an exception to the hearsay rule.[969] Using EnCase®, these tasks are achieved simultaneously in an automated fashion, without any disruption of operations.

VI. Conclusion

The authorities citied above underscore the importance of an effective and systemic eDiscovery search and collection process. Best-practices technology enables government entities to establish a defensible process that also minimizes cost. Routine full-disk imaging, over collection and high eDiscovery costs become an ad-hoc solution that lacks a systemized process. By establishing a scalable, system-wide eDiscovery procedure, large organizations can save millions annually while greatly improving compliance with the new FRCP amendments.

968 Federal Rule of Evidence 901(b)(9) provides a presumption of authenticity to evidence generated by or resulting from a largely automated process or system that is shown to produce an accurate result.
969 Fed. R. Evid. 803(6).

UK e-Disclosure Turning Point: The Corporate Focus on Cost-Effective Collection and Processing of E-Mail and Electronic Documents for Litigation and Regulatory Purposes

by Chris Dale of the e-Disclosure Information Project
Copyright September 2009 by Guidance Software.

1. INTRODUCTION

1.1 Executive Summary

This is one of a series of white papers written by Chris Dale of the UK-based **e-Disclosure Information Project**. Its purpose is to consider some of the pressures which are motivating UK companies to pay more attention than hitherto to the manner in which they collect e-mail and electronic documents for litigation, for regulatory purposes, and for other reasons, and to the costs of doing so. There is a growing awareness of the fact that it lies in a company's own hands, to a great extent, to minimise the start-up costs of instructing their lawyers and launching or defending proceedings. If litigation is to some extent a voluntary activity, there are few options when reacting to a regulator's requirement to produce documents and, in financial services in particular, heightened activity may be expected from the regulator. Recession brings other reasons why the efficient extraction of documents is a more frequent requirement just as external budgets are slashed.

1.2 The E-Disclosure Information Project

The e-Disclosure Information Project disseminates information for those with an interest in electronic disclosure in the UK courts, including judges, practitioners, suppliers and corporate clients. Its aim is the reduction of the expense of litigation. It is run by Chris Dale, a former commercial litigation solicitor and adviser on all aspects of electronic disclosure, including the court rules, the practical issues which arise and the solutions which exist to tackle them.

The main expectations of such a project are that it is knowledgeable, independent and objective. It has no client and can exist only if it is funded by sponsorship. The sponsors have in common that they are interested in and knowledgeable about aspects of e-Disclosure wider than their own commercial advantage, and that they are willing to pool resources in this indirect way to raise understanding of the issues. Guidance Software is a sponsor of the Project.

1.3 What is EnCase® eDiscovery?

EnCase® eDiscovery is a software application which can be implemented internally by a corporation to search, identify, collect, and process electronically stored information (ESI) from servers, laptops and work stations across their global network from a central location without interfering with employees' use of their computers. The software gives companies the option of automated over-the-network collection of only those e-mails or documents responsive to search criteria (keywords, time-frames,

file types, etc), of all user-created files, or of full-disk images. Companies with EnCase can also process the collected e-mail and electronic documents, culling them down and creating load file formats for loading into any lawyer review platform, thus avoiding or reducing the expense of processing by outside bureaux.

The EnCase® collection technology has substantial court validation in the United States and other jurisdictions, and is well-known worldwide as the collection and preservation technology of choice for law enforcement and regulators and various intelligence and military entities. EnCase technology has also been adopted at over 500 major companies worldwide. For these and many other major corporations, EnCase eDiscovery is a key component of an in-house, systematised, repeatable and defensible process.

It is described on the Guidance Software website at www.guidancesoftware.com/ediscovery/discovery.aspx

1.4 Disclaimer

This white paper is written by Chris Dale in conjunction with Guidance Software as an informational resource only. It is not intended to be relied upon as a source of legal or technical advice.

2 THE NEED TO FOCUS ON COST-EFFECTIVE COLLECTION AND PROCESSING

The US is generally thought of as being "ahead" of the UK in terms of its approach to electronic disclosure. There are certainly more massive volumes of documents, stricter obligations in respect of preservation and production, much more argument about them, and heavy sanctions for failing to handle them properly. The US is also "ahead" in that a considerable amount of informed thought is given to the best and most effective way of handling documents for court and related purposes. Some very sophisticated technology has been developed to handle them.

There are few, however, who believe that the US has got its approach right. A recent podcast interview by US Magistrate Judge John Facciola highlighted the need for education, both of judges and practitioners. If the former were to make proper management decisions and the latter were to fulfill adequately their duty to both their clients and the court some of the biggest problems could be reduced.

Judge Facciola did not exempt from his strictures the corporations whose documents are involved. His perception, as a Magistrate Judge involved daily in discovery disputes in the busy federal court in the US capital, is that organisations are paying little attention to how their data is accumulated, stored and managed. There is little evidence of effective document retention policies, still less of litigation readiness policies, and this in a country which imposes specific obligations on companies in relation to their records management and where the downsides of getting it wrong, in terms of costs, sanctions and duties to shareholders and the courts, are high.

On the face of it, UK companies have had less of a mountain to climb. Document volumes, generally speaking, are lower, there are few generalised obligations to preserve documents against

all eventualities, a less formalised set of duties in respect of legal holds, and no civil court sanctions beyond costs penalties as between parties.

Nevertheless, there are increasing pressures on UK companies to get and keep their data in order. These pressures come in part from an increased focus by the civil courts on the formal e-Disclosure duties, partly from heightened activity and increasing demands from regulators of companies within their purview. In addition, recession increases exposure to and discovery of internal fraud, and it encourages the search for ways to cut costs generally.

This paper looks at some of those pressures and at what companies can do to mitigate their effect.

2.1 UK e-Disclosure Coming of Age

Recent developments on the civil side include a new attention to the rules, judicial decisions and the implications of the pending report by Lord Justice Jackson on civil litigation costs. This section takes each of these in turn.

2.1.1 Practice Direction and e-Disclosure Questionnaire

The primary source of the UK e-Disclosure obligations is the Practice Direction to Part 31 of the Civil Procedure Rules (CPR). Until the 2008 *Digicel* judgment[970] shone a fierce spotlight on it, the Practice Direction was not merely ignored but was largely unknown to both practitioners and judges.

In an attempt both to remedy the perceived defects in the Practice Direction, and to gain greater visibility for it, a drafting group (of which I am a member) led by Senior Master Whitaker has prepared a draft replacement Practice Direction. This will relate exclusively to electronic disclosure and its key new element is to be an e-Disclosure Questionnaire.

The proposed Questionnaire tightens up considerably the parties' obligations in respect of their sources. The existing bland obligation to "discuss" electronic sources is replaced by a document in which parties will set out in some detail what systems (servers, PCs, PDAs, backup systems, etc), applications (Word files, spreadsheets, etc), and databases such as HR systems which the clients have. The result will be a formal court document, signed by a party or a solicitor, and exchanged with opponents before the first case management conference. There is an obligation to update the answers to the Questionnaire as more information becomes available - it is recognised that things will change as the case progresses. The obligation extends to metadata - parties will be obliged to say if they think that metadata beyond the basic metadata is to be extracted and exchanged, with the implication that good reason must be given for its inclusion.

Objection will doubtless be raised to the alleged burden which this will impose on parties and their lawyers at the early stages of a case. This is easily rebutted: the Questionnaire merely gives formal shape to an obligation which exists already, since the present duty to discuss sources clearly implies that parties should know what their sources are. It does not seem unreasonable that a party seeking justice, and proportionate justice at that, should at least be able to point to the resources on its side

970 http://www.bailii.org/ew/cases/EWHC/Ch/2008/2522.html

which contain the potential evidence. The US experience, touched on by Judge Facciola in his podcast, is that lack of control, or even awareness as to the extent, of data sources is a major contributor to the expense of e-Disclosure and the expense of litigation as a whole.

2.1.2 Increased Focus from the UK Judiciary

Unlike in the US, there are few reports of the outcome of case management hearings. One of the reasons for this, perhaps, is that the CPR expressly gives a very wide discretion to judges to manage cases. They cannot ignore specific rules, but they have considerable latitude within those rules to do what is right to promote the overriding objective set out in Part 1 of the CPR. Case management decisions should therefore closely reflect the facts of the case and are correspondingly of less wide application than was the case before 1999.

The disclosure rules are no exception. Although the definition of a disclosable document in Rule 31.6 CPR and the definition of the scope of a reasonable search in Rule 31.7 CPR are expressed as obligations, they allow considerable discretion to both the parties and the court. They are also rarely complied with properly, or enforced. The Rule 31.6 definition of a disclosable document is a narrow one compared with the US obligation - not "relevant" documents but only those which support or are adverse to the giving party's case or the case of any other party. The Rule 31.7 definition of the scope of a disclosable document (amplified on in the Practice Direction to Part 31 CPR) lists factors relevant to the scope of the search (e.g. the "ease and expense of retrieval" and the "significance of any document which is likely to be located") and is subject to an overriding duty of proportionality. One of the few unequivocal obligations, with little or no room for discretion, is the duty under Paragraph 2A.2 of the Practice Direction to discuss with opponents any difficulties which arise in relation to electronic documents.

The judge is the final arbiter if there are difficulties or disagreements between the parties and the proper course is to make the investigations required under Rule 31.7 for documents which meet the Rule 31.6 definition of "disclosable" and to negotiate with opponents to decide on the appropriate balance between the significance of sources and the documents in them (on the one hand) and the expense of retrieval and extraction (on the other). Both parties ought to gain by a proper attention to these obligations since the upshot ought to be a much narrower range of documents being held in common and being put before the court.

Completing the Questionnaire will necessarily require a closer attention to the electronic sources, and at a much earlier stage in the case. It should result in a roadmap for subsequent collection, review and exchange of a proportionate volume of the electronic evidence required for that case.

2.1.3 Court Decisions – Consequences of Failure to Address e-Disclosure

Digital (St Lucia) v Cable & Wireless[971] was the first big case where all these factors were considered. Put briefly, the defendants' disclosure was challenged on two grounds: the keywords which they

971 http://www.bailii.org/ew/cases/EWHC/Ch/2008/2522.html

had used to search their sources were alleged by the claimants to be inadequate to find potentially disclosable documents, and 800 or so backup tapes were disclosed as existing but were, the defendants said, disproportionately expensive to access and review.

Mr Justice Morgan made a careful analysis of the obligations, and particularly those under the Practice Direction to Part 31. He ordered that the defendants' existing disclosure be largely redone using a different set of keywords, and that the parties should meet immediately to discuss and plan the extraction of information from the backup tapes.

It is hard to under-estimate the potential implications of this well-publicised case for large companies engaging in litigation and for their lawyers. Whereas the ruling as to keywords really concerned only the methodology of giving disclosure (that is, the implications would be much the same whatever the state of the company's data) the ruling as to the backup tapes is rather different. A collection of 800 tapes represents a significant volume of data. There seemed to be no clear record as to what the tapes contained, nor much planning as to the eventualities in which they were likely to be used. The defendants were not penalised in sanctions (as might have happened in an American court) but the clear indication that such sources may be the subject of an order for specific disclosure is a warning to companies to be much more focused on what information they are keeping and why they are keeping it.

Abela v Hammond Suddards[972] involved a significant claim against a firm of solicitors. Amongst the points which arose was one involving the loss or destruction of a PC (the defendants were ordered to produce evidence as to what had happened to it) and as to whether printed files of e-mails were an adequate way of giving disclosure. The defendants were ordered to make electronic searches of the mail files, not least because the paper files revealed some obvious gaps. The defendants' arguments in opposition to the latter application strongly suggested that the system for archiving mail left something to be desired — it was unclear for example, what if any overlap there was between archived material and material still on live servers, and questions arose as to whether the tapes might have deteriorated or otherwise become inaccessible. The defendants obtained a quotation for £150,000 for dealing with the tapes alone. The judge thought it probable that the exercise could be done far more cheaply and said that, in the circumstances of the case, "the apparent size of the claim and the seriousness of the allegations being made, seem to me to justify more than a nominal amount of time, effort and costs being devoted to an electronic search."

The point of importance from both these cases is not the particular facts in either of them, that is, whether the record keeping of those particular parties was in fact deficient. The point is that the court concerned itself very closely in what records, including archived records, existed, and made orders for disclosure which imposed significant and unanticipated costs on those who owned the documents.

2.1.4 Lord Justice Jackson's Litigation Costs Preliminary Report

That the senior judiciary is concerned about litigation costs, and their implications for justice, is evidenced by the appointment of Lord Justice Jackson, a Court of Appeal Judge, to spend a year

972 http://www.chrisdalelawyersupport.co.uk/documents/Abela%20and%20Ors%20v%20Hammonds%20Suddards.pdf

reviewing costs and making recommendations about them. Lord Justice Jackson's Preliminary Report in May 2009[973] reports on the information acquired in the first stage of the review. That information came from lawyers, from companies and from representative bodies involved in a wide range of litigation, and from other jurisdictions as well as the UK. Specifically, he had a meeting with Judge Facciola, and heard directly from him of the problems faced in US courts.

Lord Justice Jackson paid attention to disclosure and to electronic disclosure, which is covered in Chapter 40[974] of his Preliminary Report. He covered, amongst other things, the adverse comments made about the lack of active management by judges and the absence of any training for them aimed at increasing their understanding of e-Disclosure Whatever the final recommendations made in this regard, it is unlikely that the subject will be ignored, and lawyers and their clients can expect much more attention to be paid to this aspect of case management.

2.1.5 Costs Management in Birmingham

Lord Justice Jackson has paid particular attention to ways in which costs can be predicted and managed throughout the life of a case. He has instituted in Birmingham, where His Honour Judge Simon Brown QC — one of the UK's most e-Disclosure-aware judges sits — a costs management trial under which judges responsible for case management will seek to manage the proposed costs as well. The trial is voluntary because the rules do not presently require costs management to the extent which Lord Justice Jackson envisages.

It is, however, implicit in the present rules that parties must be in a position to explain to their opponents and to the court what course they propose to adopt in relation to disclosure and what the likely costs are. That places a premium on being able to identify potential sources and thence the costs of handling them, as quickly and cheaply as possible.

2.1.6 US-UK Judicial Panel at May IQPC Conference

It is commonly said that the UK is between two and four years behind the US in its attitudes to and handling of electronic disclosure. I do not entirely agree with this, believing that the differences between the two jurisdictions, and the cultural differences, create a more complex relationship. There are, nevertheless, certainly lessons to be learned from the American experience. Albert Barsocchini, an Assistant General Counsel at Guidance Software, said in a recent speech in Australia that he had come "back from the future" to warn other jurisdictions of the dangers of following the American experience uncritically.

Nevertheless, it is important that those in a position to influence developments on both sides should know what the problems are and what steps are being taken to reduce them in the interests of cost-effective justice. This is by no means a one-way process since there are aspects of the UK rules and practice which have lessons for American courts. Proportionality is an element in both, but the

973 http://www.judiciary.gov.uk/about_judiciary/cost-review/preliminary-report.htm
974 http://www.judiciary.gov.uk/about_judiciary/cost-review/docs-prelim-report/part8.pdf

manner in which it is applied in the UK (and, in particular, a reference in *Digicel* to the folly of looking under every stone for evidence which may be material) has something to offer to the US system.

The common elements from the two approaches were covered at a judicial panel held at IQPC's E-Disclosure and Information Management Conference in London in May 2009. Moderated by Guidance Software's Patrick Burke, the panel comprised chief US Magistrate Judge Paul Grimm and US Magistrate Judge John Facciola and, on the UK side, Senior Master Whitaker, His Honour Judge Simon Brown QC and me. The subjects discussed included competence, co-operation and cost control.

As I have suggested above, English lawyers and judges tend to discount the US experience as having little relevance to the development of case management in the courts of England and Wales. It is easy to see the US as being at one of two opposite extremes, neither relevant to us — on the one hand, American lawyers are seen as technologically able and predisposed to look to technology as a solver of all problems; the opposite view is that American courts are a Wild West of uncontrolled expenditure. What was said by these two leading US judges made it clear that neither of these caricatures suffices to let us ignore the US model. I say more about the US below, but the main lessons taken away from the US contribution to the judicial panel were firstly that, outside the very big firms, American lawyers are no more technologically able than anyone else, secondly that the competence issues are primarily to do with not following the rules and ignoring case law rather than pure technology defects, and thirdly that serious attention is being paid by many judges to imposing directions and sanctions aimed at reining in costs and imposing efficiency. That is achieved in part by education of judges as well as of practitioners.

There is a long way to go on this and, as I have said, the traffic in ideas went both ways on our panel. Nevertheless, there are implications here for English lawyers, as those who direct policy in the UK realise that the US experience has positive lessons, as well as awful warnings, for those responsible for case management. We can expect these lessons, when coupled with the anticipated effect of the Jackson Report and the proposed new Practice Direction and e-Disclosure Questionnaire, to have a forceful effect on case management in the UK courts.

2.2 Increased Regulatory Demands for Production of E-Mail and Electronic Documents

It is not only in the civil courts that there has been increasing pressure on companies to be able to produce documents. Regulators have turned up the temperature, and the deadlines and costs implications of civil proceedings can appear relatively benign by comparison with a regulator's demand. Companies are being compelled to produce larger and larger volumes of digital data of many different kinds.

2.2.1 Increased FSA Demands for Documents

The post-recession fall-out must inevitably include increased activity from the Financial Services Authority (FSA). This is not simply a matter of a belated closing of the stable doors. The FSA has let it be known that it had been told by the government to regulate with a light hand in the years prior

to the recession, with the implication that it would have exercised more control if left to itself. The FSA's Chief Executive said this in March: "there is a view that people are not frightened of the FSA. I can assure you that this is a view I am determined to correct. People should be very frightened of the FSA ... we will use all our powers, including criminal prosecutions, to deliver our mandate." At the same time, the FSA announced the recruitment of 280 specialist staff, a headcount increase of 30%. It is reasonable to assume that many of those were on the enforcement side.

It is not easy to measure the increase in FSA investigations and enforcement activity. Companies who have been visited tend not to shout about it. The FSA itself will probably wait until it has an outcome to talk about before it says anything. Professionals — lawyers and disclosure experts — engaged on either side have duties of confidentiality. Anecdotally, at least, FSA activity is increasing as one would expect.

Although they may not talk about particular cases, the FSA does seem willing to talk publicly about enforcement in general. On May 21, 2009, Owen Brady of the FSA's Enforcement Digital Evidence Unit told the attendees at the IQPC Information Retention Conference in London that digital evidence was "a pretty key component of every single case." He said he usually asks companies to produce e-mails "between certain parties and between certain dates" and if you have a tool that does that "you're on a winner and life is considerably easier." If a company which has been issued a "compelled request" does not provide all that the FSA believes it deserves, it can get a search warrant, and come for the data itself, often using EnCase technology for the collection. Brady said search warrants are "a tactic that we have to use quite frequently."

There is more to FSA compliance than merely being prepared for an early-morning knock on the door. Since 2001, the FSA has increasingly required companies to provide special reports from so-called "skilled persons". This approach, described by the FSA as "risk-based", is common to all sectors — banks, insurers and investment firms — and applies in the same way across the FSA's supervisory and enforcement functions. The requirements of such a report include information, analysis of information, assessment of a situation, expert advice or recommendations, risk assessment and response to risks. According to an article in *The Times* on 19 August 2009, the use of skilled persons' reports is increasing: in 2006 to 2007, the FSA ordered 18 such investigations; in 2008 to 2009, the number rose to 56. That figure is expected to increase substantially this year. The most expensive investigation apparently cost £2.4 million and the total paid to accountants, lawyers and other outside experts was £12.8 million.

It is also increasingly common for companies to commission private reports, proactively anticipating what will be expected of them if there is an investigation. The FSA encourages such reports, particularly if they are consulted as to the scope and purpose of the report. These reports can be made relatively at leisure, and the outcome may reveal difficulties encountered in obtaining information.

Such a "dry run" is potentially useful against the day when the regulator does launch an unexpected investigation, revealing as it does not merely defects in practice but scope for improving the delivery of required information promptly and efficiently when demand is made for it. Companies with appropriate in-house technology can collect and process the electronic evidence to support a private

report which will be found credible by FSA lawyers considering whether additional investigation is called for.

2.2.2 EU Competition Authority Demands and "Dawn Raids"

One of the hardest aspects of dealing with a so-called "dawn raid" arises in relation to documents. Assuming that the officials are suitably authorised, they are entitled to seal up data sources and to look at, copy or see documents. They are not, however, entitled to see or take privileged documents. The principle may sound simple, but the practice is usually very much harder, particularly if no attempt has been made to identify in advance which documents or classes of documents can properly be considered privileged in these circumstances.

You can picture the problem clearly if you envisage the nearest you might get to the ideal scenario. All the executives are in the office, general counsel or in-house lawyer is present, and the company's senior external lawyer just happens to be on the premises. Furthermore, the senior IT and information management staff are all in that day. Suitably authorised competition authority officials arrive and ask to see a wide range of documents. That range includes many documents for which privilege can and should be claimed, but there is no classification system nor any document retention policy which allows the privileged and non-privileged documents to be easily segregated from those which the officials are entitled to see.

There is a big enough problem even if all these senior people are present. In real life, the office is unlikely to be so well manned and junior staff find themselves at risk either of putting the company in breach of its obligations or of handing over material for which privilege should be claimed. In practice, the staff has little choice — they will be ordered to give access to the demanded data, so that the FSA representatives can collect it and take it with them.

It is easy enough to say that the company ought to have a document retention policy. That achieves multiple objectives, all of them beneficial, including readiness for the litigation regime described in the first part of this paper and the ability to react promptly in compliance with a regulator's demands. From the shareholders' perspective, the proper implementation of such a policy has a pre-emptive element to it — internal fraud and misfeasance, as well as outward-facing issues such as anti-competitive behaviour, price fixing, etc. are harder to conceal if the company's data is subject to a rigourous retention policy. There are also obvious savings and efficiencies in the day-to-day running of the company's business.

All this, however, is non-trivial and comes at a price. The software applications required to manage such a policy are not cheap and the implementation of a document retention policy requires considerable internal resources as well as outside help. Whatever the pressures, the investment is hard to find in the current economic climate.

There is another factor to consider. The procurement, planning and execution of a policy takes time as well as money. For many companies — those with a high risk profile whether for litigation or in relation to a regulator— a long implementation is inconsistent with the imminence of the risks.

Less expensive and easier to implement is technology to search and collect the wide array of

existing data locations — such as EnCase eDiscovery software. By making that relatively modest investment, organisations can meet their obligations to regulators and litigation adversaries.

2.2.3 Subject Access Requests

At first sight, the right of an individual to ask for any personal data processed about him or her by the company looks out of place beside the obligations to give disclosure in litigation or the duty owed to a regulator. In fact, subject access requests can place demands on a company which are just as significant as those apparently bigger things. Briefly, an individual is entitled under the Data Protection Act 1998 to ask a company's data controller for a description of any personal data which is being processed about that individual, the purposes for which the data is being processed, and for other information about the sources of the data and the potential disclosure of it to third parties.

The data controller is entitled to satisfy himself as to the identity of the alleged data subject and can ask him or her for information which will help find the data which is sought. Once that stage is complete, the company has 40 days to comply with the request. In most cases, the fee payable by the data subject is only £10.

Although the potential range of documents relating to any one individual is likely to be very much smaller than would be needed for litigation or for a regulator, the potential burden of the exercise is considerable. Amongst the factors which the data controller must consider is whether disclosure of any document to the requesting individual will put the company in breach of its data protection duties owed to other individuals named in, or identifiable from, those documents. The data controller must either obscure such references or seek the consent of the named third parties. A company may face numerous such requests simultaneously.

Again, a properly specified and implemented data retention policy ought to ease the burden of compliance. The need to comply with subject access requests (and some companies are more at risk than others) is part of the investment case. That does not make it any easier to fund the investment nor does it help with subject access requests which arrive next week.

2.3 Summary

Any company is at risk from litigation or subject access requests, and regulated companies have the additional potential burden of regulatory compliance. The advice to invest immediately in the software and processes necessary to provide an adequate document retention policy is easily given, and less easily complied with. What every company must do, however, is undertake the risk assessment which weighs the potential costs and disruption of complying with the company's obligations against the costs of pre-empting them. Thus there is another argument for implementation of an effective data search and collection technology, at a minimum, as a stop-gap.

3. PARALLELS WITH THE US EXPERIENCE

This increase in activity from both courts and regulators parallels the American experience over the last five years or so. That period has seen not merely the 2006 amendments to the Federal Rules of Civil Procedure (FRCP), but substantially heightened expectations on the part of the SEC and other US regulators.

This paper is about the UK and not about the US. In general, I resist the lazy assumption that the UK is merely following in America's footsteps which, certainly in relation to civil litigation, ignores the differences in the rules, quite apart from the culture. It is helpful, however, to look back over the US experience of recession because it is undeniably true that the UK came to each stage of it at an interval after the US. It is necessary, on the way, to touch briefly on the components of the US experience so far as it relates to discovery. That involves a look at the procedural setting of litigation and regulation and at the development of working practices which grew up around them.

3.1 The FRCP Amendments

Disquiet at the growing costs of handling documents led, in 2006, to the Amendments to the FRCP specifically on discovery. Their intention was to clarify the obligations and control the burden and the costs of doing so. That intention was thwarted by a combination of rapidly increasing volumes and (to UK eyes) an emphasis on strict compliance with the rules, backed by sanctions, which drove up both the burden and the costs. Whilst the technology has developed to meet the challenge, the skills of lawyers and judges have not kept pace. The UK perception is that both lawyer skills and judicial training in the US are far ahead of those in the UK. That is probably true, but the scale of the problem outstrips the ability of many involved to handle it. Recession is now forcing attention on different and better ways of controlling the problem and, whilst the UK may avoid the worst of the US procedural experience, it cannot ignore the lessons of recession.

3.1.1 Requirements to Keep Documents

The 2006 FRCP Amendments placed a duty on companies to preserve all documents which may be required. Rule 26(b)(2) requires the production of reasonably accessible responsive data. Rule 37(f) gives a narrow exception in relation to discoverable electronic data which is no longer available as a result of routine operations. The intention is a positive and virtuous one in terms of the availability of evidence. The effect, however, is to increase vastly the volume of documents retained by businesses in disparate locations, the obligation to find and produce that electronic data, and the obligations to say what has happened to it if it is not available.

3.1.2 Increased Role of E-Mail as Evidence

There was, in parallel, a growing recognition of the undeniable fact that most companies conduct the majority of their communication by e-mail. E-mails carry everything from the making, varying

and breaking of major contracts to trivial communications about drinks after work. Classifying and grading them for importance, by reference to the subject matter, and with regard to characteristics such as privilege, becomes a major issue. This growth was accompanied by significant reductions in the cost of storage space. The combination of statutory requirements to keep documents, the low cost of doing so, and the significant cost of classifying them was not a good combination.

Courts inevitably came to expect to see the e-mails, Word, Excel, PowerPoint and other electronic documents which were indeed the source of the evidence on which cases were won or lost.

3.1.3 US Preservation Sanctions Cases

No survey of the US eDiscovery scene is complete without a summary of US cases about preservations sanctions. US case law develops at an alarming speed. I asked Patrick Burke, Assistant General Counsel at Guidance Software, to give me some examples of cases which illustrate the attitudes being taken by American courts when spoliation questions come before them and what appears below came from him.

We do not have sanctions, that is, financial penalties for conduct not directly related to another party's wasted costs, in the UK civil courts. Judges do, however, have power to make adverse costs orders, to draw adverse inferences and (as Digicel showed) to order that an exercise already done must be redone if justice requires it. US cases do not provide formal precedent in UK courts; they may, however, provide examples which English courts may find helpful, and UK lawyers and their clients cannot ignore them.

The American courts, having given the bar some time to become familiar with the 2006 eDiscovery provisions of the FRCP, have recently been issuing a steady stream of sanctions, in particular for the failure to preserve potentially relevant electronic evidence. See *Phillip M. Adams & Assocs. V. Dell, et al.*, 521 F.Supp.2d 1173 (D. Utah 2009) (sanctions against defendant ASUS for failure to preserve ESI relating to development of microchip technology); *Micron Tech v. Rambus*, 225 F.R.D. 135 (D. Del 2009) (Rambus DRAM patents held unenforceable because of destruction of ESI prior to litigation); *Innis Arden Golf Club v. Pitney Bowes, Inc.*, 257 F.R.D. 334 (D. Conn. 2009) (plaintiff's evidence excluded because of failure to preserve electronic records relating to investigation of potential lawsuit); *Beard Research, Inc. v. Kates*, Civ. A No. 1316-vcp, 2009 WL 1515625 (Del Ch. May 29, 2009) (adverse inference instruction, attorneys fees and expenses against defendants for failure to preserve PowerPoint on employee's hard drive after the start of litigation).

Of these recent sanctions decisions, I would recommend Judge Grimm's recent decision in *Goodman v. Praxair Services, Inc.*, 2009 WL 1955805 2009, U.S. Dist. LEXIS 58263 (D.Md. 2009) (defendant sanctioned for loss of data on the laptop of a "key player" and that key player's deletion of e-mail after preservation obligation arose) which, like so many other eDiscovery decisions by Judge Grimm, is probably destined to be deemed a landmark if only for the opinion's pedagogical approach to explaining the American concept of spoliation and the justification for imposing sanctions including adverse inference instructions. Judge Grimm looks back to 18th Century English common law for the roots of US spoliation jurisprudence.

Indeed, the origin of the doctrine of spoliation is often traced back to the 288-year-old case of *Armory v. Delamirie*, 93 Eng. Rep. 664 (K.B.1722). See, e.g., *Sullivan v. Gen. Motors Corp.*, 772 F.Supp. 358, 360 n. 3 (N.D.Ohio 1991) ("At least two federal courts have traced the origins of [the spoliation doctrine] *to Armory v. Delamirie*....") (citing *Welsh v. United States*, 844 F.2d 1239, 1246 (6th Cir.1988); *Nation-Wide Check Corp., Inc. v. Forest Hills Distribs., Inc.*, 692 F.2d 214, 218 (1st Cir.1982)); Stefan Rubin, *Tort Reform: A Call for Florida to Scale Back its Independent Tort for the Spoliation of Evidence*, 51 Fla. L.Rev. 345, 346 (1999) ("Perhaps the earliest recorded decision to recognize and reprimand the spoliation of evidence was the eighteenth century decision in *Armory v. Delamirie*."); Lawrence B. Solum & Stephen J. Marzen, *Truth and Uncertainty: Legal Control of the Destruction of Evidence*, 36 Emory L.J. 1085, 1087 & n.4 (1987) (noting that an unfavorable inference for spoliation of evidence is of "ancient lineage") (citing *Armory*, 93 Eng. Rep. 664) (citations omitted)). The Armory case involved the removal of a ring's stones by a goldsmith's apprentice and the court's conclusion that the value of the (now missing) stones should be assessed at the highest cost of jewels which would fit the empty sockets because it was the defendant's fault that the evidence which would have proved the true value was not available. This could not be a clearer example of an adverse jury instruction for the spoliation of evidence. Following *Armory* and preceding *Zubulake IV*, courts continually applied the spoliation doctrine to address possible injustices after relevant evidence had been destroyed.

The point so far as the UK courts are concerned is that the absence of US-style sanctions may result in less extravagant penalties for missing or destroyed evidence but a party who cannot produce evidence which he ought to be able to produce runs risks in inferences which may lose him the case and in costs.

3.2 Increased Regulatory Demands

Companies, and particularly those in the financial sector, were coming under increasing scrutiny before the recession. That has intensified since the fall of Lehman Brothers. Both the SEC and the US Department of Justice are ramping up the numbers of formal and informal investigations which they undertake. Section 10A of the Securities Exchange Act imposes duties on auditors to report apparently illegal acts, triggering a requirement to investigate the allegations. Compliance with the Sarbanes-Oxley Act and other regulatory obligations imposes duties of investigation and reporting. Companies face shareholder class-action litigation, whistle-blowing allegations and charges of anticompetitive behaviour.

These increasing burdens impose obligations which are either anticipatory or reactive. All of them require that companies can produce electronic documents quickly, efficiently, and cost-effectively.

3.3 How the Lawyers Faced the Challenge

The pre-electronic phase of US litigation spawned a vast industry in photocopying as corporations and lawyers sent out millions of pages for duplication. As document imaging took over, the copy shops converted to scanning shops. Finally, as Socha and Gelbmann note in their commentary on their 2009

report, every copy shop started offering EDD services. Volumes grew over the same period as the FRCP Amendments brought fear of sanctions and promoted a culture in which excessive discovery was demanded and given.

Few of the law firms or their clients had the skills or the technology in house to handle the growing volumes. The activity levels outstripped the development of best practices. It was a time of growing prosperity and the companies who were ultimately paying for the work - which was being outsourced - had neither the incentive nor the knowledge to challenge the costs being incurred on their behalf by lawyers and their outsource providers. The division between legal work and ancillary EDD services, and the relationship between them, became blurred.

If one were cynical, one might suggest that this suited the lawyers well. There was little incentive to control either the collection or the culling down of data when large fees were payable for the review stage. The threat of sanctions for non-compliance appeared to justify the legal resources applied to the review.

3.4 Client Revolt and the Move to the Left

Even before the recession forced a close focus on all elements of expense, corporate clients were beginning to rebel at the cost of litigation and of complying with regulatory demands. The recession sharpened that focus.

There was a growing realisation that the root of the problem lay in the original volumes and in the manner in which they were kept at source. This led to the so-called "move to the left", that is, to the information management end of the Electronic Discovery Reference Model (EDRM). Both software and services suppliers reported that the bulk of their work had shifted away from reactive work (that is, dealing with problems as they arose) and towards proactive investment. Companies started to buy applications and services aimed at anticipating the various demands for documents by paying more attention to document retention and litigation readiness and legal hold mechanisms.

Recessionary curbs on investment cash put a brake on this. The demands of the FRCP, the threat of sanctions and, not least, the tightening requirements of regulators continued at full force, however. In addition, the recession, as recession always does, flushed out internal fraud and other examples of conduct which tends to go unnoticed when times are good. The emphasis shifted back to reactive work. This was not merely a US phenomenon: at the beginning of 2009, the head of one of London's big forensic and investigations firms was still reporting that the bulk of his department's instructions were about proactive and anticipatory work. By May, he was heard to say that the emphasis had changed back to reactive work.

Faced with these conflicting pressures, companies have limited options. They can perhaps reduce litigation by deciding not to bring claims and by settling those brought against them. They can, to some extent, squeeze their lawyers to reduce their costs, both by reducing their charging rates and by seeking new efficiencies. Some litigation has to be fought, however, and it is not optional to deal with regulatory investigations; there are limits on the cost-cutting which can be forced on the lawyers. The alternative is to take as much of the work in house as possible.

4. THE MOVE IN-HOUSE

4.1 Looking Behind the Buzzwords

There are terminological conventions which have been devised in the US to describe the benefits of the processes and applications used to collect ESI. The applications must *identify, collect, preserve* and *process* ESI, and must do so in a *systemised, defensible*, and *repeatable* way. They must allow companies to comply with the requirements of the FRCP and the case law derived from it and they must allow an organisation to make an early assessment all its ESI and the strength or weakness of the case revealed by it. This should not rely on employee self-collection because that is neither systemised nor repeatable.

All this terminology is useful up to a point in that it defines the standards which must be reached, standards honed in a jurisdiction which lays strong emphasis on all these things and on court validation of both the processes and the results. The UK lays less stress on some of these things as a formal matter. As I have described above, there is no UK equivalent of the FRCP obligation to keep all documents against the possibility of litigation, there is no string of case law requiring or validating any particular process, and no court-imposed sanctions for technical breaches of the rules. There are, however, multiple reasons why companies need to adopt tools and processes which meet the more stringent requirements of the US jurisdiction.

Having described in the earlier sections of this paper what the UK context is, it is helpful to look behind the buzzwords to see how tools like EnCase eDiscovery help companies handle ESI quickly, efficiently, and at the lowest cost.

4.2 The Benefits of a Repeatable Process

For the most part, it is obvious. Let us go back over the main triggers for data collection in descending order of urgency.

4.2.1 Regulators

If you are subject to the powers of a regulator, his emissaries may turn up at any time demanding to see a wide range of e-mail and electronic documents at short notice. Although the sharpest focus is on the proper withholding of documents which are privileged, there are considerable merits in being able to produce all the right documents, and only the right documents, as quickly as possible. The relative economy of being able to do so from a repeatable system is only half the story; the regulator's perception that you are in control has merits of its own. In this context, the increasing number of "skilled persons" reports for the FSA has two results: it increases the chance of being forced to go through the production process and it gives an opportunity for a "dry run" at producing the documents, and only the documents, which matter. Put like that, the words "repeatable" and "systemised" have more immediate and practical meaning than may appear from their reiterated recital in software marketing materials. They are not just words.

4.2.2 Subject Access Requests

If relatively few UK companies are regulated, all are at risk of a subject access request. If a company cannot readily search and collect its own electronic data, then each subject access request can be a burden. Even for companies with effective search and collection, the pressure here becomes not so much the need to produce everything relating to the subject, but the need to identify and eliminate (or get consent in relation to) references to other people. Forty days is not a long time when the data controller may face concurrent applications. Every such request will be different in that they will necessarily relate to individual data subjects. What is needed here is a set of processes which run on rails and do not require fresh instructions to an external collection agent every time.

4.2.3 Litigation

As to litigation, it would be easy to conclude that the UK regime is lax relative to the US one. As I have made clear above, changes are in hand which will formalise and give more urgency to what is already the strict obligation of parties to litigation — to make their lawyers aware as quickly as possible of the range of data sources which must be preserved and may have to be disclosed. It is not enough merely to identify custodians, date ranges and the servers and PCs, etc on which the data may reside. If the information is to be at all meaningful, it must also is be culled down to a relatively narrow range of potentially disclosable material. The pressure here is not merely the formal obligations of the rules. Lawyer time is expensive, and it is very much in the interests of a company to limit the amount which the lawyers have to deal with, while simultaneously being able to satisfy them that nothing has been overlooked or wrongly culled.

4.2.4 Other Collateral Benefits

With any investment, one looks to collateral benefits beyond the primary reasons for the acquisition. If the points listed above are motives in themselves for acquiring a product like EnCase eDiscovery, there are several other things you would use it for once you had acquired it and developed the internal processes to use it effectively and efficiently. These include records management, enforcement of internal procedures, detection of data leakage, financial auditing, fraud detection and internal investigations. A company may face any of these in a given year.

5. SUMMARY

If it is right that the ideal is a fully fledged document retention system, consisting of applications, processes and user input from the moment of document creation, that is an ideal which, in the current economic climate, relatively few companies can contemplate. At the other extreme, companies which are unregulated, see the risk of litigation as minimal, and do not anticipate subject access requests or the need for internal investigations, may reasonably take the view that they can face anything which turns up on a reactive, case-by-case basis.

Between these two extremes lie companies of all sizes facing one or more of these factors on a continuing or repeating basis. The cost of facing each one as if it were a new problem very quickly becomes prohibitive as external costs mount. Those external costs are not merely the costs of individual data collections but the accumulated hourly costs of the lawyers who are instructed to advise on the data. For those companies, and there are many of them, Guidance Software's EnCase eDiscovery provides what is needed to reduce both duplicative work and multiple instructions to third parties.

Like everything else, EnCase eDiscovery requires an investment to yield results. For those who are not in a position to compute accurately their annual expense on outside costs, or who are not in a position to make an outright purchase, Guidance Software offers a pay-per-use model which, as its name implies, allows you to pace the expense to the usage. That represents a half-way house between a major up-front investment and an unquantifiable accumulation of external costs.

There is no answer which is the right one for all companies and all circumstances. The biggest risk lies in not assessing the risk and in failing to estimate the costs which will be incurred either as an investment or on a transactional basis. The challenges discussed in this paper are not diminishing.

What's New in EnCase eDiscovery Version 5

Overview

Version 5 is the latest release of EnCase® eDiscovery, the leading enterprise e-discovery solution that provides everything from legal-hold and collection to review and production, delivering potentially relevant electronically stored evidence (ESI) located on premise or in the cloud, producing results that are accurate, defensible, and repeatable. EnCase eDiscovery V5 includes several new features and enhancements to help you and your e-discovery team significantly lower costs, reduce risk, and swiftly gather more types of information in more languages and from more locations than before.

One Click EnCase® eDiscovery Integration with EnCase eDiscovery Review

Even non-legal and non-technical members of your team will work faster with the integration of EnCase eDiscovery and EnCase eDiscovery Review. With just one simple click, you can directly and securely upload an entire corpus of documents for attorney review.

Enhanced Legal-hold Module

You and other team members will enjoy a more powerful and simplified workflow with all-in-one legal-hold creation and a personalized custodian dashboard. Enhancements to the Legal-hold module enable centralized legal-hold management with escalation capabilities, customizing legal-hold messages, global legal-hold reminders, updated reporting, and greater automation throughout.

New and Updated Connectors

Collect from more sources more easily with new and updated connectors for Box.net, Google Drive, Amazon S3, Office 365, Exchange 2013, and SharePoint 2013.

New Reporting Interface and Robust Reporting Functionality

A greatly improved reporting experience delivers robust reporting around all phases of electronic discovery, including legal-hold, collection, processing, and delivering of data.

Improved Desktop Interface

The enhancements to the desktop interface streamline the workflow for collecting, processing, and producing ESI, providing higher productivity for all team members.

Expanded Foreign-Language Support

Improved Unicode support in EnCase eDiscovery means you can now index, search, and display data in all known foreign languages supported by Windows for more complete results. This Expanded Unicode support is also included in EnCase eDiscovery Review and includes searching, processing and production.

Ability to Read and Work with Encrypted Data

E01 and L01 evidence formats are now available in encrypted versions as Ex01 and Lx01.

Centralized Examiner Management

Centralized management of examiner machines is easier with a streamlined, web-based workflow with greater configuration and deployment flexibility. The Examiner Service now runs as a true Windows service offering superior load balancing and parallel processing and the ability to globally view and manage all server-based processes.

* This document includes all Version 5 features available, including those in Version 5.4.

Key Features for Legal

Key Feature	Function / Description	Advantages
ENHANCED: Legal-hold Module	• Enhanced and simplified workflow • Centralized hold management and escalation • All-in-one legal-hold creation • Global legal-hold reminders • Personalized custodian dashboard • More flexible reporting • Customization of legal-hold messages	• Lower risk • Easier custodian process management • Greater efficiency • More reports in more formats
NEW: EnCase eDiscovery Review Integration	• One-click upload of data collected in EnCase eDiscovery to EnCase eDiscovery Review • Automated uploads to the secure hosted review platform • Move subsets to review as needed • Includes metadata and other subjective fields (tags) for each item	• Faster collaborative review • Reduced time to ECA • Greater contributions by non-technical and non-legal team members • More complete collection of more types of data
ENHANCED: Foreign Language Index Support	• Improved Unicode support enables the following for data in all foreign languages supported by your version of Windows: o Indexing o Searching o Displaying	• Able to handle global data sets with one solution

Key Features for IT

Key Feature	Function / Description	Benefits
ENHANCED: Centralized Examiner Management	• Centralized examiner management is implemented as a true Windows service	• Enables examiners to more quickly resume work from the point of interruption in case of system issues
ENHANCED: Foreign Language Index Support	• Improved Unicode support enables the following for data in all known foreign languages: o Indexing o Searching o Displaying	• Able to handle global data sets with one solution
NEW: Additional Con- nectors	o Amazon S3 o Box o Office 365 with SkyDrive Pro o Google Drive	• Collect from more sources more easily
ENHANCED: Web API Methods	• More methods associated with custodians and cyber security investigations are exposed in the web API	• Gives you greater flexibility to create custom workflows
NEW: Support for MS-Office Metadata Field	• Data is now indexed by individual field, including Microsoft Office 2007 and 2013 metadata fields	• Search for a data value within a specific metadata field in Microsoft Office 2007 and 2013
NEW: Encrypted Evi- dence Formats	• E01 and L01 evidence formats are now available in encrypted versions as Ex01 and Lx01	• Read and work with encrypted evidence
ENHANCED: Desktop Application Workflows	• Streamlined workflow for collecting, processing, and delivering data	• Greater efficiency and lower costs of legal- hold processes • Higher productivity for even non-technical and non-legal team members

More Information

We invite you to visit www.encase.com/ediscovery or contact your Guidance Software Account Executive.

The Place for EnCase® eDiscovery in Electronic Disclosure for Major Corporations in UK Courts

by Chris Dale of the e-Disclosure Information Project
Copyright 2009 by Guidance Software.

1. INTRODUCTION

1.1 Executive Summary

This is one of a series of whitepapers written by Chris Dale of the UK-based **e-Disclosure Information Project**. Its purpose is to gain further understanding of the issues arising from electronic disclosure in the UK and the part which EnCase® eDiscovery from Guidance Software and similar data image collections applications can play in addressing those issues for large corporations. This is the second edition of the paper, which has been updated to reflect developments since its publication in May 2008.

1.2 The E-Disclosure Information Project

The e-Disclosure Information Project brings together those with an interest in electronic disclosure in the UK courts, including judges, practitioners, suppliers and corporate clients, with a view to reducing the expense of litigation, and ensuring compliance with court rules and regulatory requirements. It is run by Chris Dale, a former commercial litigation solicitor and a consultant in all aspects of electronic disclosure, including the court rules, the practical issues which arise and the solutions which exist to tackle them.

The primary function of the Project is to collect and disseminate information. The information passes in all directions between the interest groups involved – client needs, lawyer requirements, judicial expectations and supplier solutions all depend on an understanding of what the other parties want or can offer.

1.3 Sponsorship

The main expectations of such a project are that it is knowledgeable, independent and objective. It has no client and, in practice, can exist only if it is funded by sponsorship. The growing number of sponsors have a common interest in the project, each are knowledgeable about aspects of e-Disclosure beyond their own commercial advantage, and they are willing to pool resources in this indirect way to raise understanding of the issues. Guidance Software is a sponsor of the Project.

1.4 What is EnCase® eDiscovery?

EnCase® eDiscovery is a software application that can be implemented internally by a corporation to search, identify, collect, and process electronically stored information ("ESI") from servers, laptops and work stations across their global network from a central location without interfering with employees'

use of their computers. The software gives companies the option of automated over-thenetwork collection of: (1) only those e-mails or documents responsive to search criteria (keywords, time-frames, file types, etc.), (2) all user-created files, or (3) full-disk images. Companies with EnCase can also process the collected e-mail and electronic documents, culling them down and creating load file formats for loading into any lawyer review platform, thus avoiding or reducing the expense of processing by outside bureaux.

The EnCase® collection technology has substantial court validation in the United States and other jurisdictions, and is well-known world-wide as the collection and preservation technology of choice for law enforcement and regulators and various intelligence and military entities. EnCase technology has also been adopted at over 500 major companies worldwide. For these and many other major corporations, EnCase eDiscovery is a key component of an in-house, systematised, repeatable, and defensible process.

Companies can obtain EnCase eDiscovery in one of two ways. They can buy a perpetual license to the software or, alternatively, can avoid making a capital expenditure by obtaining it on a pay-per-use plan, installing the software on their system but paying only when it is used.

It is described on the Guidance Software website at www.guidancesoftware.com/ediscovery/discovery.aspx

1.5 The Purpose of the Whitepaper

This whitepaper sets EnCase eDiscovery in the context of the requirements of UK litigation. Corporate awareness on this subject is less advanced in the UK, although (as I will show) the requirements of the UK courts are no less onerous than those of the US. They are focused more on the narrow, more "surgical", selection of documents which matter, and less on purely technical compliance with the rules.

This is not a review nor does it give a technical description beyond what is needed to show lawyers and their clients what part EnCase eDiscovery can play in helping them to be prepared, in a timely and cost-effective way, for giving electronic disclosure in the courts of England & Wales. The same principles and technology apply to preparation for a regulatory investigation and (of increasing importance in a recession) for internal investigations into possible fraud.

My starting point is therefore the Rules, the trends in judicial practice and a summary of best practice for those who must comply with them. An understanding of this context is needed to see the role which EnCase eDiscovery can play in helping with this.

1.6 Disclaimer

This whitepaper is written by Chris Dale in conjunction with Guidance Software as an informational resource only. It is not intended to be relied upon as a source of legal or technical advice.

2. E-DISCLOSURE IN ENGLAND & WALES

2.1 The impact of the Rules - Summary

The rules require narrow selection of documents at an early stage in the litigation process, disclosure which is proportionate to the case, a high level of co-operation and information exchange between parties and the court, and a close degree of management by the court. There are judicial moves towards much tighter regulation of disclosure in a manner described as "surgical". The effect of this is to increase the need to control and capture documents efficiently, at the latest when litigation first becomes a possibility, for reasons of compliance, costs and tactical advantage. This applies, where proportionate to the case, to all parties in all courts, but is particularly significant for large organisations which have a continuous flow of litigation requiring continual collection and processing of e-mail and electronic documents.

2.2 The 1999 CPR – the drafting intent

Part 31 of the Civil Procedure Rules[975], radically altered the scope of what had hitherto been called discovery but was henceforth called disclosure. Previously, discovery was required of any "relevant" document. The new rules expressly limit disclosure only to those documents which support or adversely affect the case of the giver or any other party. The duty of search is limited to sources whose likely evidential value warrants the cost of extraction.

The whole process is subject to the "overriding objective of enabling the court to deal with cases justly"[976] whose key component is proportionality. Proportionality covers not only factors relating to the parties and their claim, but the use of the court's resources. The rules give very wide powers of management and a high level of discretion in achieving the overriding objective.

The intent behind the changes was to make parties focus on the issues on which justice would hinge. The rules made no express provision for electronic documents, and so proved inadequate, at any rate as used in practice, for the electronic deluge which followed. A more significant defect lay in the fact that the powers and definitions given by the rules were largely neglected by courts and practitioners alike.

2.3 The 2005 Practice Direction

An attempt was made to remedy the formal defects in disclosure by the Practice Direction to Part 31[977]. It expressly extended the definition of a document to include electronic documents and their metadata, and elaborated on existing rules with regard to specific disclosure, the scope of the search and other matters.

Its most important provisions, however, imposed new obligations on parties to discuss issues

975 www.justice.gov.uk/civil/procrules_fin/contents/parts/part31.htm
976 www.justice.gov.uk/civil/procrules_fin/contents/parts/part01.htm
977 www.justice.gov.uk/civil/procrules_fin/contents/practice_directions/pd_part31.htm

which arise in respect of electronic sources of documents and to co-operate with regard to the format for exchange. Both of these obligations expressly made the judge the arbiter in case of difficulty or dispute, and both were required to be dealt with "at the earliest practical date, if possible at the first Case Management Conference" - paragraphs 2A.2 and 2A.3 of the PD to Part 31 CPR[978].

The theoretical effect was twofold – one, the whole business of discovering what a client's sources were became an urgent priority in case management terms even if the parties and their lawyers would rather defer it, and two, it gave the court an express set of management tasks.

2.4 New Attention to Management

The theoretical effect of the Practice Direction is gaining new attention since the end of 2007. Five factors are at work: since the beginning of 2008, a new rigour is being imposed in the management of cases in the Commercial Court; in parallel with that, an initiative has emerged from the Birmingham Civil Justice Centre aimed at introducing the same rigour in lower courts and at helping judges understand the problems and the technology; Senior Master Whitaker is charged with producing a wholly new Technology Questionnaire and a Practice Direction; after a long period with no disclosure case-law, 2008 saw three new cases which are relevant to lawyers' obligations; Lord Justice Jackson is undertaking a review of civil litigation costs; and new developments in other common law jurisdictions are informing UK thinking.

2.4.1 The Commercial Court Recommendations

The Commercial Court Recommendations[979] of December 2007 included four elements relevant to disclosure:

- tight focus on the issues which matter and on the documents which matter in relation to those issues
- express use of the term "surgical" to describe the manner in which disclosure is to be approached
- a duty placed on the lawyers to take part in the discussions about the management of disclosure
- an emphasis on the responsibility and involvement of a party's boardroom level management in costs and settlement aspects.

None of this involved new rules, merely proper compliance with the existing rules and more rigorous exercise of the court's powers and discretion. The success or otherwise of the Recommendations can only really be measured over the whole life of a representative number of cases and there is as yet no consensus on the effect of the trial. There seems little argument about the value of the four points identified above.

978 www.justice.gov.uk/civil/procrules_fin/contents/practice_directions/pd_part31.htm#IDAYERW
979 http://www.judiciary.gov.uk/docs/rep_comm_wrkg_party_long_trials.pdf

2.4.2 The Birmingham Initiative and Judicial Awareness

The initiative at the Birmingham Civil Justice Centre affects a wide range of cases and not just the very heavy commercial cases. His Honour Judge Simon Brown QC, a Designated Mercantile Judge in the Birmingham Mercantile Court, has joined Senior Master Whitaker as judicial advocates of both tighter use of the rules and more informed use of the technology.

These two judges actively practice an approach to case management which emphasises that the judge is the end-user of the disclosure / discovery exercise, that it is to be tightly managed by the court, and that its end is a close focus on the issues and on the documents which support or undermine the facts which must be proved in relation to those issues. The case management regime will include a technology questionnaire and a draft order for directions which will leave no room for parties to duck their obligations.

As well as imposing this management regime in their own courts, Master Whitaker and Judge Brown actively seek out public platforms at which they carry the message to corporations and practitioners as well as to fellow judges.

2.4.3 Technology Questionnaire and Practice Direction

The obscurity of the Practice Direction is the driver for the proposed Technology Questionnaire and new proposed Practice Direction. The purpose of the Technology Questionnaire will be to force parties to exchange information about their sources of electronic data at an early stage and thus give teeth to the present loose obligation to "discuss" sources. Decisions about identification and collection will assume their proper place as the key starting point. The Practice Direction will be dedicated to electronic disclosure, isolating the e-disclosure elements of the present Practice Direction. Both are being supervised by Master Whitaker, of whose drafting group I am a member.

2.4.4 Case Law Relevant to Identification, Collection and Identification

Few case management decisions are reported in the UK and there has hardly been any case law on electronic disclosure before or since the 2005 Practice Direction. 2008, however, brought the Digicel[980] and Abela[981] cases, both of which concerned the scope of disclosure and the balance between expense and likely value – the components of proportionality. Both emphasised the need for an informed and co-operative approach to the identification of electronic sources of information and the role of the court in managing the time and expense of disclosure.

A third case, Hedrich[982], drew attention to the downside risks of getting it wrong. Solicitors in a relatively small case were pursued for a wasted costs order by their clients' opponents who alleged

980 Digicel (St Lucia) v Cable & Wireless [2008] EWHC 2522 (Ch), [2008] All ER (D) 226 (Oct), Chancery Division, Morgan J., 23 October 2008

981 Lawtel, 2 December 2008, Deputy Judge Paul Girolami QC

982 Hedrich v Standard Bank [2008] EWCA Civ 905 (30 July 2008)

that their e-disclosure failures had led them to waste money. The solicitor beat off the claim, but the case has focussed attention on the risks of ignorance.

2.4.5 Jackson Review of Litigation Costs and other Influences

Lord Justice Jackson is conducting a year-long review into the costs of civil litigation. Part of his remit is to consider what is happening in other jurisdictions with regard to costs generally. He is not due to report until the end of 2009, but the mere fact of his appointment with such a brief is both a reflection of the importance of the subject and a likely catalyst for change. A section of his report will be devoted to disclosure, with help from me amongst others. Much of the input he has received relates to the management of the early stages of a case and to the significance of what is happening in other countries.

2.5 Implications for Court Users

The obvious results of this new attention to case management include these:

- The clients must get their data ready for litigation as soon as it becomes a possibility and must, at the least, freeze the document population for future culling and filtering.
- A premium attaches to software tools which can hack through the volumes in a way which is transparent – that is, which give the disclosing party the comfort that he has not missed anything vital and, crucially, allow him to demonstrate that fact to opponents and the court. Guidance Software's EnCase eDiscovery is such a tool, as it provides full documentation of its search and collection from laptops, workstations and servers.
- Software which allows easy tagging by issues is going to be increasingly valuable to comply with the court's expectations.

In addition, there will be a new focus on issues of responsibility in four different ways:

- Making a "surgical" selection may result in lower volumes and thence costs, but involves a more onerous task for clients and senior lawyers.
- The person who signs the Disclosure Statement faces more than a mere formal duty; the Technology Questionnaire will bring forward the time when parties must focus on, and exchange information about, electronic sources.
- The senior management of a litigant will be held more to account by the court for the costs and for inadequate attempts to settle.
- The judge assumes a higher share of responsibility if he is to order or sanction a selective approach to the documents.

This is the context in which I now focus on the collections stage of disclosure.

3. BEST PRACTICES AND TECHNOLOGY FOR UK E-DISCLOSURE COLLECTION AND PROCESSING

3.1 The Importance of Having an e-Disclosure Process

Software vendors necessarily want to send out the message that their application is the key component in capturing the data which must be preserved for pending litigation or for a regulatory investigation. The lawyers will often have a different view, and that view may be different as between the in-house lawyers (if any) and the external lawyers.

The most important thing, in fact, is *process*, the methodology used to extract just the right data, at just the right time, cost-effectively, and in a manner which cannot be challenged. I will come on to look at each of these components – scale, time, cost and manner – below, but it is first worth considering the issue of scale, which is of particular importance to large organisations. I will then look to the alternative broad approaches toward collection of data.

After considering scale, the factors which dictate your approach can be collectively described as "proportionate". What is "over the top" for one case may be grossly negligent for another. The smallest, least contentious, case requires a well thought-through process in much the same way as a large one does, whatever the mode of collection.

3.2 The Challenge of Scalability of Collecting E-mail and Electronic Documents Across Large Organisations

For large companies and organisations, scale is often the largest e-Disclosure collection challenge. Even a modest collection from just four or five employees can involve computers in four or five separate offices hundreds or thousands of miles apart. Sometimes all the target computers are in one office – although that office is a plane flight away from the IT collection team.

Consider what must happen when a company's lawyers determine that it must collect data from scores, or hundreds, of employees who might have custody of potentially disclosable e-mails and electronic documents (for example, in response to a request from the EU Competition Commission for e-mail and other electronic documents relating to a pending merger). After the company's legal team has identified the appropriate custodians, they must quickly:

1. Identify, in collaboration with IT, all the locations where those custodians' e-mail and electronic documents are kept, probably including servers as well as the employees' personal laptops/workstations;
2. Collect the disclosable e-mails and documents (which may mean collecting all those employees' e-mails and whatever electronic documents are in their possession);
3. Filter out the potentially disclosable e-mails and documents from the larger bulk that was collected; and
4. Process the resulting filtered set of e-mails and documents so that they can be loaded into a lawyer review platform.

To accomplish these tasks for scores of custodians is a daunting task for even the largest corporations, which is why they frequently outsource the process. The collections service provider will then send teams of data collectors to each office where the computers are located, charging for time and expenses. Some eDiscovery collection agents typically collect full-disk images of each employee's computer, often tens of gigabytes per machine. They then charge hundreds of pounds per gigabyte to filter – or "process" – the collected data and load it into a review application.

Thus, companies with a regular need to collect potentially-disclosable data can save substantial amounts of money by collecting data themselves, collecting less than full-disk images, and doing their own processing in house without paying outside experts. This also allows them to bring in house a process that is consistent and repeatable whilst accumulating additional knowledge about where important data resides.

This is what EnCase® eDiscovery offers large organisations – the ability to collect data from any laptop, workstation or server on the organisation's network(s), and then process that data in house so that it can be loaded directly into a lawyer review platform without paying processing fees to outside experts.

Scale – and reach – can play a role in small collections as well. Take the challenge of collecting from five employees' computers in the company's remote offices. The traditional approach would call for a technician to travel to each office and image the five machines (asking each employee to halt use of their computer for several hours while the imaging takes place). All that travel, expense and disruption take place before it is even determined that there is any usable information on any of those computers. The ability to preview machines remotely over the network would avoid this. EnCase eDiscovery offers this capability.

3.3 Different Approaches to Data Collection

It follows from what I say above that there is no single answer to what is the best way of going about data collections. The broad approaches are

a) Custodian self-collection with corporate "Windows Explorer collection", where users make their own selections and have their IT department collect the results together non-forensically for the lawyers;

b) Collection by a third party expert, hired for a single job or for several jobs performing either forensic or non-forensic collections with secondary culling and load file creation performed by the vendor at per-gigabyte charges; or

c) Automated enterprise-wide forensic collection using a software application – such as EnCase® eDiscovery – which can reach all laptops, workstations and servers from a central location according to search criteria determined by the lawyers, and can perform free inhouse secondary culling and processing into load files for lawyer review platforms.

I group them like this because the difference lies not in who actually does the job, but how it is done. The distinctions lie in whether the task is repeatable, forensically sound and independent of the variations implicit in user subjectivity, skills and concentration.

Strictly, the terms self-collection and forensic collection are not opposites. A company can do its own forensic collections if it is equipped with the tools and the skills to do so. An external provider may do a non-forensic collection, either because it was so instructed or because it fouled up an attempt to do a forensic one.

3.4 Forensic and Non-Forensic Collections

I have said above that the question whether a collection is forensically sound is independent of the identity of the collector. I put it in this way because the term "forensic collection" implies more than merely a method.

A "forensic copy" is conventionally described as *"An exact bit-by-bit copy of the entire physical hard drive of a computer system, including slack and unallocated space"* and the term "forensically sound procedures" may be defined as *"Procedures used for acquiring electronic information in a manner that ensures it is "as originally discovered" and is reliable enough to be admitted into evidence"*[983].

I do not propose here to examine the technical elements which make up a forensic collection. It is enough to appreciate that the more forensically sound the collection, the greater the amount which can be proved by it, but that increased time and expense may outweigh that benefit. The UK courts are more concerned with time and expense and less (in most cases) with whether the collection method was perfect.

3.5 Factors Influencing Collection Methods

Six broad factors apply in choosing a collection method for a large organisation. They might be loosely described as *scale, cost, responsibility, context, irretrievability* (that is, loss of the ability to recapture the original state of the data) and *admissibility*. Each of these has its corollary under the other headings (that is, lower cost may bring diluted responsibility and more significant irretrievability).

3.5.1 Scale

For large companies, scale becomes the most important factor for reasons of risk, cost and efficiency. Scale refers to the ability to reach all employees' data – whether on laptops, workstations or servers – from one centralised location. For global organisations, the task of collecting employee data is exponentially more difficult when the need is continual or frequent and the employees are spread across multiple offices. In those circumstances, the contrast between options becomes starker - either pay large sums of money to outsource the task or bring the process in house by taking advantage of

983 Both definitions from the glossary to the EDRM (Electronic Discovery Reference Model) at www.edrm.net

technology that allows for global collection from a central location and in-house processing at no marginal cost. That's the advantage of implementing EnCase® eDiscovery.

Scalability is also important when lawyers can foresee the need for supplemental collections from the same custodians to obtain subsequently created or modified e-mails or documents (for example, if the controversy or transaction at issue is ongoing). Companies doing manual machine-by-machine collections must redeploy the collection teams and re-collect all the data from the custodians (including what was previously collected), then pay to have that recollected data re-processed and the new data culled out. Companies with EnCase eDiscovery, on the other hand, can simply re-run the over-the-network search with instructions to only collect new or modified files not previously collected, and that's all they'll get. They can simply top off their prior collections, and can do so on whatever periodic basis the lawyers deem advisable.

Of course, if your organisation has infrequent collections that are generally confined to a small number of close-by locations, then the contrast is less stark. In those cases, traditional alternatives become more viable, including outsourcing. In such situations, companies can also consider obtaining the EnCase eDiscovery software on a pay-per-use basis, so that the company can handle its collections on an enterprise-wide basis, and save money as compared to outsourcing. Both of these approaches appeal to companies that have sporadic needs, or those companies with more consistent needs that have not yet focused on the issue – this being a goodly percentage of UK companies. There are signs that a growing number of UK corporations are beginning to pay attention to this, as much as a side-effect of recession as a consequence of judicial or other pressure.

3.5.2 Cost

After scale, cost is the major consideration of large organisations. Big collections are expensive to accomplish manually with internal IT staff, and far more expensive when outsourced. And once collected, the data has to be processed which can be more expensive (even if it is a push-button process).

Cost comes from the very start of the process. If you don't have a tool like EnCase®, you can't perform an "early case assessment" – or data sampling -- over the network. By conducting an early case assessment, a company can test out its search criteria (custodians, keywords, timeframes, etc.) and better target their searches so that a smaller, more targeted set of data is collected. Their only option is to deploy the vendor's collection teams to go out and acquire the data and then analyse it.

The cost-reduction opportunities come when an organisation can collect over a network, and then process the data in house without paying outside collection fees. That is what EnCase eDiscovery does. The added benefit lies in not disrupting executives and employees when they're using their computers. Traditional collections usually require that executives and employees turn over their machines to the collection experts for a few hours – taking an involuntary break from productive work. EnCase, of course, enables a company to collect data from a machine without disrupting the user.

Of course, if the volumes are very small and can be readily pared down by reference to a few custodians, a date range and a well-organised folder structure, then the cheapest manner of collection

may be to set the users, or the IT department on their behalf, to pull out the key message folders and document directories. This is sometimes known as *Windows Explorer collection*, because the identified files are simply dragged onto a DVD using Explorer. Compared to scalable collections, "Windows Explorer collection" is a process which makes sense only in the smallest scales. For large organisations, even the small collections add up quickly, so "Windows Explorer collection" usually makes no sense.

Cost-conscious companies also may be attracted to the pay-per-use option offered by EnCase eDiscovery, whose usage rates are well below the usual cost of outsourcing collection. Because the monthly pay-per-use bill for EnCase eDiscovery is broken down on a case-by-case basis, chargebacks to business units and/or submission of these litigation costs to insurers are facilitated.

3.5.3 Responsibility

The courts are increasingly emphasising the duty of the lawyers to the court. That is most marked in the US, particularly following the Qualcomm case in early 2008 and in a range of opinions delivered in that year, notably by US Magistrate Judges Grimm and Facciola. The UK courts may not have the weapon of sanctions as used in Qualcomm, but they can make costs orders where they consider that costs have been wasted. Such orders may be made personally against the lawyers – the Hedrich case, referred to above, is a reminder that US-style sanctions are not the only form of threat to those who are not clear as to their duties. At the least there is the potential for disputes between lawyers and their clients as to who should pay these costs. This argues for a close liaison, and definition of responsibility, between clients and lawyers.

3.5.4 Context

By this I mean the type of case. A commercial dispute over some contract terms may give rise to no potential arguments about authenticity or the manner of collection. A fraud case, or one involving allegations of conspiracy, raises very different considerations. The existence of hidden, "deleted" or over-written files may matter very much. Harsh economic times, such as are seeing now, both make fraud more likely and the incentives to uncover it rather greater. The metadata, particularly relating to dates or authorship may be critical. In those cases, a non-forensic collection by the clients may be unsafe (but note what is said below as to the fact that "non-forensic" and "by the clients" are not necessarily opposites).

3.5.5 Irretrievability

By this I mean the inability to go back to the source data for a second and different selection of documents or for a more acceptable manner of collecting them. The pressures – the client's own wish to limit the start-up costs and that from the courts – to limit the sources, should not obscure the possibility that events will require a wider or more detailed trawl at a later stage. It may not be possible to repeat and extend the Windows Explorer approach, not least because the first pass may have altered some of the metadata. This is an area where the ability of EnCase® eDiscovery quickly and easily to

re-run its search and find only new or modified e-mail and documents (and leave behind what it has already collected) has particular value.

3.5.6 Admissibility

Unlike the US courts, which claim jurisdiction over how a company organised its documents prior to the litigation, the English courts take a litigant's documents as it finds them. It will, of course, inquire into allegations that documents or data have been destroyed in contemplation of litigation. A conclusion or a suspicion that this happened is a factor which is generally considered at trial as part of the overall facts considered in deciding what is just. Striking out on this ground alone is possible but is a rarely used power.

The courts will certainly hear arguments as to whether a document is all it purports to be, and will attach what weight seems appropriate to it accordingly, in much the same way as it will judge a witness as much by his demeanour as by what he says. If there are arguments about documents alleged to have been omitted, or tampered with, or collected or culled in a way which challenges a party's compliance with the rules, then the court may make an order for specific disclosure or for payment of costs thrown away, but it will only debar a party from trial if justice cannot be done with the evidence as it stands. In the United States, prominent judges including Chief Magistrate Judge Paul Grimm have focused a spotlight on the applicability of US authentication requirements to ESI.

3.6 Choosing Between Collection by Third-party Agents or by In-house Applications such as EnCase® eDiscovery

The decision as between using a third party bureau and buying an in-house enterprise-wide collection and processing application such as EnCase® eDiscovery will turn on five elements:

- the scale issue – is it simply too expensive and time-consuming to outsource the collection and processing functions to a third party?
- the amount of repeat business which is expected
- a choice between capital spend and transactional costs
- the availability of in-house skills and other resources
- issues of responsibility and liability for a critical business process

These elements are not conclusive or, rather, different factors will weigh more heavily with some companies than with others. Most companies of size will find that their needs are frequent, if not continuous, and that outsourcing the collection and processing function is cost-prohibitive.

Outsourcing of data collection necessarily means that companies are outsourcing knowledge about their network, and where its data resides. This knowledge is lost as companies change their collection service-providers. There is increasing value in institutionalising knowledge about where particular data is located. This knowledge is valuable not only for litigation, but for overall document management concerns.

A company which does not anticipate repeat collection needs might nevertheless want to keep as much as possible of the process in house, whilst one with a near-continuous flow of collections might reasonably choose to delegate it to external consultants where in-house skills and the responsibility issues (to which I revert below) are dominant factors.

I am neutral as to the principles, not least because in most cases the application of the five elements above will point to one approach or the other. However, there is no arguing with the scale (and its related cost) issues. My purpose here is not to push you towards the type of in-house solution which Guidance Software and others offer, but to show how they fit into the requirements of UK litigation.

3.7 Processing Considerations for UK litigation

Processing is a universal requirement of e-Disclosure – whatever is collected must be processed so that it can be effectively loaded into a lawyer review platform.

4. APPLYING THE TECHNOLOGY TO UK PRACTICE

4.1 Introduction

I have summarised the key elements of the UK civil procedure relevant to disclosure as involving:

- a wide range of document types and sources….
- subject to a surgical narrowing to a tight list of issues….
- by a rigorous application of the rules and management powers of the court…
- which imposes a strict responsibility on lawyers and their clients…
- to be at once comprehensive and economical in fulfilling their obligations…
- in a proportionate manner

The fact that the UK has neither the remedy of sanctions (as the FRCP imposes them) nor US-style pre-trial battles over the mode of collection and resulting admissibility issues, does not make it any less rigorous as a process. Costs may be awarded for defaults; disclosure is a continuing obligation and sources which have hitherto been ignored may be examined later in the proceedings; the fact that admissibility might be challenged only at trial does nothing to diminish the need to be able to prove something at that stage about the original document or the manner of its collection.

How should one be ready for such a regime and what technical and logistical steps best tie in with the requirements of the court rules and practice?

4.2 Who are the Players?

A number of factors point towards increased responsibility of people at various levels:

- The US Qualcomm case and the CREDO (Case Review and Enforcement of Discovery Obligations) programme which the judge ordered as a result has thrown a spotlight on the

respective roles of in-house and external lawyers, as well as of the IT personnel, and the implications of responsibility (both in the sense of doing the job and being held to account for it) which arise.

- There is a new focus on the identity and skills of the person who makes the disclosure statement required as part of the list of documents and who will, in due course, have to sign the Technology Questionnaire. This requires two distinct skill sets – an understanding of the issues and a knowledge of the party's systems and procedures. The giver may be examined (and cross-examined) in court on what is said in the disclosure statement and held to account for it.
- The judge assumes a greater degree of responsibility than has hitherto been observed. If surgical decisions are being made at an early stage, then that can only be on the strength of what the parties say at an early stage, and the burden on the parties to be prepared – and comprehensive and accurate in what they say – is increased, not diminished by this assumption of responsibility by the judge.
- The party's senior management is likely to be fixed with a greater degree of responsibility for the costs, following the Commercial Court Recommendations emphasis on this.

Someone has to take the lead on the clients' part as soon as litigation is threatened. A team from all sides – lawyers and clients – and from both legal and IT, must be assembled quickly. There may be only a one-off opportunity to collect the data properly. It may be advisable for companies to have a dedicated team in place for the sake of efficiency and consistency.

4.3 What are the steps when litigation threatens?

4.3.1 The Parameters of this Discussion

It is beyond the scope of this paper to consider the identification of the moment when litigation threatens, what the mechanism should be for spotting that moment, what standing procedures should be in place for a litigation hold, and going even further back, what document retention policies should exist. Nor is this paper concerned with what the backup regime ought to be. As noted above, the court will give such weight as it thinks fit to the apparent absence of documents which ought to exist in deciding what is just. The release, in late 2008, of BS 10008 "Evidential Weight and Legal Admissibility of Electronic Information" provides a new set of standards by which these things will be weighed as technical and management matter.

The primary concern is to preserve the documents which exist (and such records as exist of those which once existed) at the earliest time when litigation becomes likely. I have outlined above the various factors which must be weighed to decide whether self-collection of the Windows Explorer kind is appropriate and whether this is a case which warrants a forensic collection. The rest of this whitepaper assumes that a forensic collection has been decided upon, if only as a matter of prudence. How much to collect?

It will not be known by anybody at this stage what is the scope of the threatened litigation, still

less what issues within the wider dispute will be identified as being worth fighting over. It follows that those charged with the collection will not necessarily know what documents or classes of document will fall within the scope of standard disclosure or might have to be produced by way of specific disclosure.

It is also worth pointing out that the formal requirements of the court are not the only reason why one might want to capture documents which might have any bearing on the matters in issue. The clients want some advice, for example, and as early as possible, as to what their prospects are in the proposed litigation.

That much argues for collection on the widest basis, of everything which might possibly be required. That need can be met by making a full disk image of every PC, every laptop, and every other device used by any person connected with the likely issues, as well as every server to which they had access or on which documents created by them might be found. This is, indeed, often done, and often necessarily so. It can, however, be extremely expensive, time-consuming and disruptive to do this, particularly if empty space and slack space are included. The first exercise of the team referred to above is to assess the costs (including the downtime for users whilst their computers are unavailable) and to weigh that against the benefits for the case in question.

This is an exercise in proportionality, that concept which governs the whole management of cases in the UK courts. Anecdotal evidence suggests, however, that it is not uncommon for full forensic disk images to be commissioned. Apart from the obvious cases where fraud or similar is suspected, reasons for taking this course include those where there is fear of future destruction of data, or where it might be necessary to rebuild an entire disk drive on a new computer, or where there is simply no time or available instructions to be selective. It might just be an excess of caution.

4.3.2 Collecting Less than the Whole

If it is safe to collect less than all the data, how much less should one aim for? There are various obvious ways of cutting down the primary volumes:

- By a date range, with a margin allowed at each end of the scale.
- By custodian, that is the author, recipient, copyee etc. of documents, where it is possible (as it usually is) to define the staff or classes of people likely (on the widest basis) to have documents.
- By file type – the obvious ones are operating system files, executables and other non-user files and (possibly) temporary files; it may also be possible to eliminate some user files whose nature makes them irrelevant on any basis.

This much can often be eliminated without much deliberation. One might, however, go further and pre-empt decisions more usually taken at the processing or review stage. Some collection methods allow culling or filtering (that is, decisions to exclude or to include files) by reference to keywords, file names or other characteristics of the files.

Organisations with EnCase eDiscovery can use such criteria to adjust their collection approaches based on the needs in a particular case, or based on the lawyers' confidence in their search criteria:

Full Disk Image

All User-Created Data

Date restrictions and exclude known irrelevant file types (e.g. Microsoft applications)

Keywords & Date Restrictions & Include Only Known Relevant File Types (e.g. Word, Excel, PowerPoint)

This approach has easily quantifiable benefits, and some drawbacks. The most obvious benefit is that the quantity of data which is retrieved, and which then has to be processed and stored, might be substantially reduced. Someone, however, has to make the decision as to the choice of keywords, etc., and that decision may be challenged later by opponents or by the court, as happened in Digicel, referred to above. By collecting all user-created data, a company can exclude all known irrelevant file types without leaving behind any potentially relevant e-mails or files.

4.3.3 Documenting Culling Decisions

There is no general rule to apply here, save for this: it is implicit in the concept of proportionality which governs UK civil proceedings that decisions are made which involve balancing the likely importance of any classes of documents against the difficulty or expense of extracting them – indeed, that is expressed in Rule 31.7 CPR[984] and in the Practice Direction to Part 31 CPR[985].

Whilst that is primarily aimed at sources which are physically inaccessible (e.g. in a large collection of unsorted backups tapes, or requiring redundant systems which cannot be rebuilt cost-effectively), the principle can be applied to other material which is not inaccessible but which is nevertheless disproportionately expensive to collect.

Once the proceedings are under way, such questions may be brought before the court, which can apply the Rule 31.7 factors to the circumstances. Where the collection is being done in anticipation of possible proceedings, a party must make its own decisions. Relevant factors may include the probability (if such be the case) that the culled data will remain available and undamaged and could be retrieved in a later exercise, albeit at extra expense.

The critical thing is to record such decisions – what the considerations were, what advice was sought and given and what was done or not done. This is partly an audit measure – if you know what

984 www.justice.gov.uk/civil/procrules_fin/contents/parts/part31.htm#rule31_7

985 www.justice.gov.uk/civil/procrules_fin/contents/practice_directions/pd_part31.htm#IDAYERW

you left out, you know what to go back for – but is also a means of showing your bona fides. Ideally, the system used to do the collections should have a means of logging both the decisions and their effect.

4.3.4 Supplementing Preserved sets of Potentially Disclosable Data

It may prove that the timing decision was wrong – the anticipated litigation did not arise after all, but may yet do so in relation to a data set which is changing. It may be necessary to repeat the exercise, and to top up the original collection with later files or with different parameters. Unless the whole exercise is to be done again (in which case there will be a potentially large de-duplication exercise to do as well as a double charge for collections) this requires a methodology which can both repeat the original criteria (perhaps with variations) and identify files which are unchanged.

4.3.5 Analysing Preserved sets of Documents and E-mail

The steps set out above should leave a party with a data set which has been refined to some extent, which preserves the collected documents exactly as they were found, and which is documented. The chain of custody and control can be verified by one or more of the people involved – the relevant people at the clients, the lawyers involved in the decision-making, and the expert who actually made the collection.

If the case proceeds, the data will usually go through two further stages – processing and review. These steps may take place in a single end-repository or may pass through an intermediate one whose function is to apply rules and processes to reduce or refine the document population still further. It is beyond the scope of this paper to describe these functions.

Each such stage may involve some degree of conversion, and will certainly involve a data transfer exercise. Most end-repositories make a charge for both processing and storage which take account of the volume. A collection system ought to have a means of further refining the data set before any transfer to another system. This will usually allow a mixture of user review and block coding.

Again, this must be documented, auditable and defensible in the sense that the decisions taken, the reasons for them, and their effect should be recorded and be repeatable. A back-up of the original collection should obviously be retained.

4.3.6 Applying Metrics

The various components of this exercise – of time, cost, volume and value – are important not just to assess the scale of the burden, but to assess proportionality and to compare different approaches.

For example, the decision to refine the data set before transfer to another processing engine or review tool can only properly be made by weighing the relative costs of the larger transfer against the costs of an intermediate review. If the next stage process will refine data more efficiently than the present tool allows, it may be worth making the transfer without further refinement despite the additional transfer, processing and storage costs. Speed too may be a factor.

The system and method used to handle this stage ought to allow such calculations to be made, perhaps by reference to parallel experiences with similar collections.

5. EnCase® EDISCOVERY MEETS UK E-DISCLOSURE CRITERIA

5.1 The UK Context Compared to the US One

The preceding parts of this paper have considered the requirements of UK litigation and looked at the factors which apply so far as data collections are concerned.

Those requirements are not identical to those of the US courts. The FRCP and the case law based on it emphasise the obligation to seek out, capture and disclose every relevant non-privileged document, with merciless battles fought over every shortcoming of scope or alleged defect of process.

The CPR imposes no less onerous obligations to uncover the existence of disclosable documents, but the definition is narrower, there is more emphasis on proportionate searches, the reduction to key issues is stricter, the approach to documents is (or is getting to be) "surgical", and questions about admissibility are usually weighed at trial.

The objectives are therefore subtly different.

5.2 EnCase eDiscovery in the UK context

5.2.1 EnCase in civil litigation enabling surgical and proportional disclosure

EnCase® eDiscovery is a market-leading application in the US context. Guidance Software makes much of the fact that the use of EnCase has been validated by the courts worldwide, and of the defensibility of its processes – both vital attributes in a context where cases can be won or lost in procedural battles over the scope and manner of collection regardless of the merits of the case.

It follows from what is said about admissibility in paragraph 0 above, that these things have less resonance in the UK. In those circumstances, much of what EnCase and other forensic tools offer may seem over-elaborate as a means of collecting documents for disclosure in the UK courts.

This is, I think, to miss the point. The UK system is no less rigorous than the US one, but that rigour is applied more to early identification of the key documents in order to find the facts needed for a just decision, and less to technical arguments over the scope or manner of collection. An order for specific disclosure, or an award of costs for disclosure defects is different in kind, but little different in effect, to a sanctions order, and the fact that you may lose at trial because your disclosure is considered incomplete or unsafe is in some ways worse than being struck out at an earlier stage.

It may be rare for a case to be struck out on the strength of arguments about admissibility, but the Commercial Court has given notice of its intention to make more use of summary judgment and of its power to strike out a statement of case for failure to comply with rules and orders. There are, in addition, increasing pressures to use the most cost-effective means of managing cases.

5.2.2 EnCase® in Other UK Contexts

Although this paper's scope is limited to UK civil litigation, it is worth observing that litigation is not the only UK/EU context in which companies may need to extract, cull and preserve document collections in a targeted and documented manner at short notice. The same principles apply to:

- the powers of a regulator to demand disclosure at short notice
- the various data protection and employee privacy restrictions to which UK/EU companies are subject whilst meeting their other obligations such as audit investigations, customer complaints or allegations of work-related criminal offences[986]
- compliance with subject access requests
- the increasing range of criminal sanctions which companies may face, such as the new Corporate Manslaughter and Corporate Homicide Act of 2007

Each of these provides a powerful incentive to have a process in place to collect documents quickly and accurately.

5.3 Using EnCase to Identify and Collect Documents Centrally

The arguments above as to the value – and often necessity – of a forensic collection process apply equally to EnCase® eDiscovery and to the employment of a good third party collections expert.

Assuming a high degree of competence and accuracy on the part of such an expert, a good range of culling and de-duplicating facilities, simple exporting functions and, critically, good reporting tools, then the chief difference between the hired expert and EnCase® eDiscovery is that the latter brings the tools and skills in house, under the control of the company and capable of being run and re-run as often as needed.

The secondary – but no less important - difference is the lack of disruption. EnCase works across the network, searching workstations, laptops, file servers, user shares, other data repositories, and removable storage media for whatever combination of file metadata, keywords, and digital fingerprints have been defined in the setup. The target files can be live and open, their users unaffected by the exercise. Not all third party tools can do this, so it is worth asking. There is a relatively simple trade-off here which is summarised above in paragraph 0. If you have a one-off or only a few collection requirements, and / or if you do not have the skills and computing power in house, you hire a third party. If you anticipate several collections and are willing to buy the software and acquire the skills, you buy something like EnCase. Again, EnCase eDiscovery's payper-use option helps bridge this trade-off for companies with relatively small or uncertain collection needs, by requiring payment only when the software is used.

986 http://www.guidancesoftware.com/downloads DataProtectionComplianceinCorporateInvestigations.pdf

5.4 How it Actually Works in Practice

The heading does not connote a technical explanation of how EnCase works. For that I refer you to the product description page on the web site of Guidance Software[987]. This brief section is aimed instead at showing how a company which uses EnCase might apply it to the business of giving disclosure in UK litigation.

On the first threat of litigation, an immediate search might be made of all devices on the network on the widest reasonable range of dates, custodians and file types. The output is an EnCase Logical Evidence File (LEF) with metadata intact. The LEF is read-only and the exercise, including the search parameters, is logged.

If this proves after all not to be the crystallisation point for the threatened action, further LEFs can be made using the same search parameters either over the whole range or, perhaps, only to catch new and changed files. The exercise does not mark or affect the source files in anyway.

With the data safe, a team is assembled made up of internal and external lawyers, IT people and someone from senior management with overall responsibility. One of them will in due course be the person who signs the disclosure statement.

A list is made of all electronic sources of potentially disclosable information, including those, if any, which are not available over the network (such as PDAs, home computers or backup tapes); the costs and likely value of getting at the data on these is weighed.

The legal team defines a first-pass potential issues list – this will change as opponents and the court have input into it and considers what ought to be captured for review by reference to the definition of disclosable (Rule 31.6 CPR[988]) and starts to define what search criteria – including keywords – will limit the results appropriately.

More and more often companies test their search assumptions by using EnCase eDiscovery to perform an early case assessment, preliminary searches of potential custodians data to verify which custodians have relevant data, and to test whether the anticipated keywords and time-frames are reasonable and effective.

The upshot may be conclusions as to the size and cost of the exercise which may inform the decisions to be made thereafter, including the possibility of settlement.

The resulting information will allow the completion of the Technology Questionnaire which is likely to become compulsory shortly. The parties discuss their sources as required by paragraph 2A.2 of the Practice Direction to Part 31. The upshot may be agreement as to a smaller list of sources, alternative criteria or a different set of keywords. In default of agreement, the same facts and arguments may be put before the court.

The client may then re-run the search, varied according to the terms of the order or agreement which results. The result can be de-duplicated with EnCase®.

What happens after that depends on the circumstances. EnCase eDiscovery enables companies to conduct their own post-collection culling and processing (at no marginal cost if a perpetual license

987 http://www.guidancesoftware.com/products/ediscovery_index.aspx

988 www.justice.gov.uk/civil/procrules_fin/contents/parts/part31.htm#rule31_6

is purchased, or at below-market rates through the pay-per-use payment option). It also has push-button exports to LexisNexis Concordance and to CT Summation, and the new version allows users to create the EDRM standard XML load file which has become the standard in the industry. A copy of the LEF comprising the cut-down data rather than the whole, can be sent to a bureau, many of which are geared up to copy the data off, process it as required and import the end-result into the lawyers' review platform.

If any question arises thereafter as to the original condition of the file, or as to the larger set of documents from which the selection was made, the various LEFs can be re-examined.

6. SUMMARY

The use of EnCase eDiscovery will be overkill for some litigation clients and cases in the UK, as it is in the US. The affordability of bringing EnCase eDiscovery in house has improved with the availability of a pay-per-use payment option. Windows Explorer collections made by the client will be more than adequate for most purposes, and there are very good collections experts, for large oneoff collections or for those companies who do not want the capital cost, the staff overheads and the responsibility of handling collections in house.

For those companies, however, who anticipate several collections in a year – including, perhaps, those for the non-litigation purposes summarised in the above, the use of EnCase is well worth considering, not just for the savings in processing and lawyers' fees, but for the edge it gives in meeting the "surgical" approach to disclosure, the challenges of scale and cost, and the more rigorous climate of responsibility now being encountered in the UK courts.

Obtaining German Works Council Approval to Collect Employee E-mail and Electronic Documents

by Patrick J. Burke, Esq.
Copyright 2008 by Guidance Software.

I. Executive Summary

Companies that seek to collect German employee E-mails and electronic documents all confront the same hurdle: obtaining permission from their company's works council. Germany's works councils have earned a reputation as fierce protectors of employee privacy rights, often rejecting corporate efforts to search through employee data. Their opposition invokes the rights and protections afforded German employees pursuant to the 1995 E.U. Data Protection Directive as well as German federal and state data protection laws.

This white paper will address several questions that arise in dealing with German works councils, such as

- What is a works council and how do they function?
- What is the German data protection regime upon which the works councils can base their objections?
- What steps can a company take to maximise the probability that its data collection methodology will be approved by its works council?

II. The Works Council

Works councils have been an integral part of German business and industry since the early 20th century. The first works council provision was enacted following World War I and has existed in various forms ever since. The existing law is enshrined in the Works Constitution Act of 1972 (Betriebsverfassungsgesetz) and applies to private enterprises with more than five permanent employees of voting age.[989]

Works councils are established through democratic processes. Candidates for works councils must secure a certain amount of signatures from their fellow employees to be eligible for election.[990] Trade unions may also nominate candidates for election, but cannot compel their members to vote a specific way.[991] Works council member are elected directly by company employees through a secret ballot, though employees are not required to vote,[992] and generally serve for four years.[993] The size of

989 See Works Constitution Act (Betriebsverfassungsgesetz) §1, available at http://hikwww1.fzk.de/br/content/worksConstitutionAct-BetrVG.pdf
990 Works Constitution Act §14(2).
991 Works Constitution Act §14(5).
992 Works Constitution Act §14(1).
993 Works Constitution Act §21.

a works council depends on the number of employees within a company and the Works Constitution Act also requires works councils to proportionately represent certain types of employees.[994]

Under the Works Constitution Act, works councils have the right to co-determination in matters affecting company structure, personnel decisions, and policies regulating workplace and individual conduct within the company.[995] The rights of a works council can be categorised as follows:

> Information: The works council has the right to information regarding the implementation or change of practices or policies at the company. If necessary, the employer must provide documentation to that effect.
>
> Consultation and Cooperation: The works council has the right to consult and cooperate with management to jointly discuss and develop the topic at issue.
>
> Veto Right: A works council has the right to block certain management decisions.

The employer is required to keep the works council fully informed in matters relating to operations and personnel planning so that the council can participate in drafting company policy.[996]The purpose of this is to allow the works council to cooperate with management to avoid potential disputes and raise relevant concerns or other suggestions.

The works council resolutions require a quorum of fifty percent and resolutions are adopted by simple majority unless otherwise required by law.[997] Works councils and management may, formally or informally, enter into valid and binding agreements;[998] formal agreements are immediately binding on employer and employees and informal agreements generally require additional steps, such as the amendment of an employee contract. The works council may only enter into works bargaining agreements in those areas of business operation where the Works Constitution Act confers rights of participation on it. Collective bargaining agreements between employer associations and trade unions have absolute priority over works bargaining agreements, even if the latter are more favorable to the work force.[999]

In the event that disputes between works councils and management cannot be resolved amicably, the parties may be assisted by the conciliation board, a body with arbitration and mediation duties.[1000] Assuming that both parties agree to be bound by its decision beforehand, the conciliation board's ruling is final and binding and is appealable only on the grounds that the board has violated general principles of law.[1001]

---

994 Works Constitution Act §15(2).

995 Ingebjörg Darsow, Implemenation of Ethics Codes in Germany: The Wal-Mart Case, Universitat Pompeu Fabra, (March 2005) available at http://www.upf.edu/iuslabor/032005/art11.htm.

996 Works Constitution Act §80, 81, 85, 89.

997 Works Constitution Act §33.

998 Works Constitution Act §77.

999 Works Constitution Act §77(5).

1000 Works Constitution Act §76.

1001 Works Constitution Act §96.

III. German Data Protection

When works councils assert their right to approve or disapprove employee data collection methodologies, they are in part invoking their rights pursuant to European Union law, German federal law, and the data protection laws of their home states. The EU Data Protection Directive authorises the processing of employee data as long as it is necessary to protect the legitimate interest of another party and as long as the employee's interests and fundamental freedoms are not overridden.[1002]Each member state has enacted legislation that effectuates the general tenets of the EU Directive.

Germany's Federal Data Protection Act (Bundesdatenschutzgesetz) regulates the collection of personal data as well as the storage, alteration, transfer, blocking, deletion and use of such data.[1003] It also allows for collection of employee data under certain circumstances and calls for a balance between the legitimate business purposes of the company and the legitimate privacy interests of affected employees.[1004]In some situations, employee notification and even consent are required for collection of personal data.[1005]The Federal Data Protection Act regulates compliance with the law through company self-monitoring and external government oversight. It also differentiates between criminal and administrative violations of the law as well penalties for such infractions.

Data protection is also regulated on the state level. The German states all maintain data protection laws that mirror the Federal Data Protection Act.[1006] Each state legislative body appoints its own State Commissioner for Data Protection. The State Commissioner operates independently and is supervised by the President of the state legislature.[1007] The State Commissioner also oversees private organisations within its jurisdiction to ensure compliance with the state data protection law.[1008] Like the Federal Act, the state data protection laws provide for notification and the obtaining of consent before processing of personal data can take place.

1002 Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, Section II, art. 7, Official Journal of the European Communities 1995, No. L 281/31 [the "EU Directive"] available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

1003 Federal Data Protection Act (Bundesdatenschutzgesetz,) §1, available at http://www.bfdi.bund.de/cln_007/nn_946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzFederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/BundesdatenschutzgesetzFederalDataProtectionAct.pdf.

1004 Federal Data Protection Act §10(1).

1005 Although the Federal Data Protection Act specifies several times that notification of the data subject is required, Section 33 of the Federal Act provides exceptions to the requirement of notification and consent, including:

- if a data subject has otherwise received notification such that it is unnecessary to inform the subject a second time;
- if there is an overriding interest that requires the storage of the data in secrecy due to a legal interest of a third party;
- if the data will be erased within three months;
- if it is for a business's own purposes and can either be found from generally accessible sources or notification would "considerably impair the business purposes of the controller."

Federal Data Protection Act § 33(6)(b).

1006 See Sidebar titled "Useful Links" for links to various state data protection laws.

1007 See, e.g., Bavarian Constitution, Art. 33(a), available at http://www.bayern.landtag.de/en/bayer_verfassung_erster_hauptteil.html#4; Saxony-Anhalt Data Protection Act, §20, available at http://www.sachsenanhalt.de/LPSA/fileadmin/Elementbibliothek/Bibliothek_Politik_und_Verwaltung/Bibliothek_LFD/PDF/binary/Vorschriften/Land/dsg-lsa/English/par19_ut_to_24.pdf Saxony-Anhalt Data Protection Act, §22.

1008 Saxony-Anhalt Data Protection Act, §22.

Compliance with the German data protection regime is achieved through self-monitoring within the company and external oversight by federal and state officials. Federal and state data protection commissioners are responsible for ensuring that companies comply with the law and are empowered to investigate violations. These commissioners may also perform audits to ensure that a company's organisational and technological safeguards sufficiently comply with the applicable data protection law.[1009]

Companies are also required to self-regulate to ensure their own internal compliance; each company is required to appoint a Data Protection Officer to monitor its practices. The Data Protection Officer reports directly to corporate management and is responsible for ensuring compliance with applicable data protection laws and representing the company to the external government agencies that enforce the BDSG at the state and federal levels.[1010] The Data Protection Officer is also tasked with ensuring that deficiencies in a company's data protection regime are rectified. Employees whose data is targeted may approach the data protection officer any time they have concerns.[1011]

IV. Securing Works Council Approval to Collect Employee Data

Works councils are different in every company, and each company has an individual relationship with their works councils that will affect their presentation on this topic.

We offer the following suggestions for successful works council applications:

> Get on the works council agenda as early as possible. Usually this is handled through the company's HR department, which generally interfaces with the works council. In the case of the auto maker, it took months just to get onto the agenda for a monthly meeting.
>
> Make your presentation in German. This may sound obvious, but it's worth noting that even though the managers who run your data collection operations are English speakers, they should employ a German-speaking manager to make the presentation and field questions (the presentation materials used should be in German as well). If there is an non-German speaking manager with significant collection responsibility, they should also attend, both out of respect and to be available for tough questions.
>
> Emphasise that EnCase Enterprise can enable you to avoid collecting employee personal E-mail or documents. With EnCase Enterprise, your collections will cull through the data and preserve only those E-mails and electronic documents that meet precise search criteria, including keywords and file types. Other documents that do not meet the search criteria – including private personal data – will be left behind.

1009 Federal Data Protection Act §38.
1010 Federal Data Protection Act §4(f).
1011 Federal Data Protection Act §4(f)(5).

Assure that collections will be done "in-country". Some works councils are reassured when told that all collections will be done from within Germany, rather than operated from a location in another European member state or else outside Europe. EnCase Enterprise technology allows for an "examiner" (a laptop or workstation from which the EnCase search is operated) to be placed inside Germany, even if that is not its usual location.

Discuss how EnCase Enterprise can be configured to prevent employee data from being transferred outside Europe. EU data protection laws permit transfers to other European jurisdictions, but prevent most transfers outside Europe. EnCase Enterprise can be configured to prevent searches of European employee data from outside of Europe, and prevents the transfer of data collected to locations outside Europe.

Emphasise that existing investigative policies already approved by the works council will remain in place. For example, HR policies relating to the investigation of potential employee wrongdoing had long ago been approved by the works council and will not be affected by the use of EnCase Enterprise technology. That data would go directly to the company's HR team and would be handled the same as before.

Permit employees to create a "personal folder." If employees create a folder in their computer file structure with an agreed-upon folder name in which they can place all of their personal data, EnCase Enterprise's search criteria can be configured to leave that folder untouched, so that none of that data will be collected.

Ability to restrict searches by file type. Employees can be sensitive about certain types of files that may not be of interest to the company – personal photographs, for instance. With EnCase Enterprise, these file types can be excluded.

V. Conclusion

Companies seeking approval from works councils, particularly companies based outside of Germany, must approach their works councils with sensitivity toward the interest in the protection of the employee's personal data. This sensitivity is often not enough to obtain the works council's blessing for a collection methodology; the concerns are that the collection methodology may expose personal employee information and the employee data may be accessed from outside Germany. To gain approval, the collection methodology itself must reflect proactive strategies – including procedures and technology – to guarantee that employees need not be concerned that their private e-mail and electronic documents will be collected along with those the company requires for legal purposes.

APPENDIX I: Key Players

Federal Data Protection Commissioner:

Data Protection Commissioner who is elected by the German Parliament for a term of six years and is independent in the exercise of his duties and subject only to the law. Upon discovering violations of the German Federal Data Protection Act, the Data Protection Commissioner may object and demand correction of the violation. The Commissioner is supported in his duties by the Data Protection Commission, a group of ten members of Parliament that provide an advisory panel to the Commissioner.

State Data Protection Commissioners:

Much like the Federal Data Protection Commissioner, each state's Parliament elects a Data Protection Commissioner to monitor compliance with that state's Data Protection Act.

Company Data Protection Officer:

Companies appoint Data Protection Officers within their organisations. These officers are responsible for (1) controlling data by preventing unauthorised persons from accessing or entering personal data; (2) assuring that those who have access to the data processing system are only accessing the data they have authority to access; (3) assuring that at no point can data be collected, modified or removed without authorisation; (4) that the modification of data can be documented; (5) assuring that whenever data is disclosed it is documented; (6) assuring that the processing agent is only collecting data in accordance with a business's instructions and that such data is protected from destruction.

Works Councils:

Works councils are required for companies that normally employee five or more eligible employees. A works council is a form of workplace democracy whereby representatives elected by employees are given management functions. Works councils have the right to co-determination in matters affecting organisational structure, personnel decisions, and policies regulating workplace and individual conduct within the company. This means that any proposed policy must first be approved by the works council in order to be implemented by the company.

APPENDIX II: Useful Links

EU Directive (English version):
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

German Federal Data Protection Act (in English):
http://www.bfdi.bund.de/cln_007/nn_946430/EN/DataProtectionActs/ArtikelBundesdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf_Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf.

Works Constitution Act (in English):
http://hikwww1.fzk.de/br/content/worksConstitutionAct-BetrVG.pdf

Links to Selected German States' Data Protection Laws (unless otherwise noted, all documents in German):

Baden-Württemberg:
http://www.zv.uni-wuerzburg.de/datenschutz/Gesetze/bayer_datenschutzgesetz.htm

Bavaria:
http://byds.juris.de/byds/009_1.1_DSG_BY_1993_rahmen.html

Berlin:
http://www.datenschutz-berlin.de/content/Recht

Brandenburg (in English):
http://www.lda.brandenburg.de/sixcms/media.php/2232/bbgdsg_e.pdf

Hamburg:
http://fhh.hamburg.de/stadt/Aktuell/weitereeinrichtungen/ datenschutzbeauftragter/datenschutzrecht/hamburgisches-datenschutzgesetz-1990-07- 05-pdf,property=source.pdf

Hesse:
http://www.datenschutz.hessen.de/hdsg99.htm

Mecklenburg-Vorpommern:
http://www.lfd.m-v.de/dschutz/ges_ver/guv/guv_c_20.html

Lower Saxony:
http://cdl.niedersachsen.de/blob/images/C2643488_L20.pdf

North Rhine-Westphalia:
https://www.ldi.nrw.de/

Rhineland-Palatinate:
http://www.datenschutz.rlp.de/rgrundlagen/a1_5.html

Saarland:
http://www.lfdi.saarland.de/html/lfd-internet/datenschutzrecht/sdsg_2007.pdf

Saxony:
http://www.sachsen.de/de/bf/staatsregierung/ministerien/smi/smi/upload/SachsDSG2003.pdf

Schleswig-Holstein (in English):
https://www.datenschutzzentrum.de/material/recht/ldsg-eng.htm

Thuringia:
http://www.thueringen.de/datenschutz/gesetze_rechtsvorschriften/thueringen/datenschutzgesetz/

ABOUT PATRICK J. BURKE

Patrick J. Burke, Assistant General Counsel at Guidance Software, Inc., previously practiced in the commercial litigation department of Linklaters, where he served on the firm's eDiscovery Working Group. Patrick gratefully acknowledges the valuable contributions by his Legal Interns Lawrence Estrada and Krystal Juncosa.

ABOUT GUIDANCE SOFTWARE (GUID)

Guidance Software is recognised worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organisations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to eDiscovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing – all while maintaining the integrity of the data.

For more information about Guidance Software, visit www.guidancesoftware.com

This paper is provided as an informational resource only. The information contained in this document should not be considered or relied upon legal counsel or advice.

Using EnCase® Enterprise Solutions to Enhance Data Protection Compliance in Corporate Investigations

Copyright 2007 by Guidance Software.
April 2007

I. Executive Summary

UK companies conduct internal investigations on a daily basis, and also increasingly are asked to collect employees' email and electronic documents to satisfy litigation and regulatory requests. Although these digital investigations are necessary to meet companies' legal obligations, they also must demonstrate respect for employees' privacy rights under EU directives and UK data protection laws, which require that these investigations and collections not be excessive in relation to their legitimate purpose.

Companies can enhance their compliance with the data protection laws by utilizing EnCase® Enterprise solutions, as they enable a company to:

- Limit investigations to vastly smaller sets of employee data. EnCase Enterprise enables a company's investigators to conduct highly targeted searches of employee data – including sophisticated keyword and date-range searches – to entirely avoid reviewing or collecting the vast majority of the emails and electronic files kept by employees.
- Limit the number of people with access to employees' data. EnCase Enterprise minimizes the number of people authorized to review particular employees' – or executives' – data by providing for highly granular role-based permissioning that details exactly which examiners can access which laptops, workstations, and servers.
- Document compliance with data protection laws. EnCase Enterprise maintains a detailed log of every investigation and collection, so that the company can later prove in court precisely what employee information was reviewed and/or collected – and what was not.

This paper will address some of the salient requirements of the EU Data Protection Directive (the "EU Directive")[1012] or the UK Data Protection Act 1998 (the "UK Act")[1013]pertinent to the investigation, review, and/or collection (hereinafter "investigation") of employees' personal data. It also touches on relevant portions of the Regulation of Investigatory Powers Act 2000 ("RIPA")[1014] and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations

1012 See, Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities 1995, No. L 281/31 [the "EU Directive"] available at http://eurlex. europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

1013 See, Data Protection Act 1998 (c.29), [the "UK Act"] available at http://www.opsi.gov.uk/acts/acts1998/19980029.htm.

1014 See, Regulation of Investigatory Powers Act 2000 (c.23) ["RIPA"], available at http://www.opsi.gov.uk/Acts/acts2000/20000023.htm.

2000 (the "LBP Regulations").[1015] It is by no means a complete legal description or treatment of these laws. For a detailed analysis of your company's approach to this area of law, we suggest you consult with a solicitor.

II. Using EnCase Enterprise to Enhance Compliance with Data Protection Laws

Companies cannot avoid searching employees' data. When a corporation is made aware of internal wrongdoing, its investigators must move quickly to investigate the allegations and take appropriate responsive measures, even if that requires searching through and examining emails and electronic documents that employees maintain on their company laptops, office workstations, and corporate servers.

Companies must also meet increasing demands from their solicitors to locate potential evidence required to prepare for litigation or to meet regulatory and other legal demands. eDisclosure is likely to increase as English and Welsh courts now operate within specific guidelines for electronic disclosure provided in the October 2005 Practice Direction on Part 31 of the Civil Procedure Rules (CPR).[1016] Regulators such as the Financial Services Authority, the Heath & Safety Executive, and the Office of Fair Trading are also increasingly requesting electronic data. Companies simply are not in a position to ignore these responsibilities to locate and produce electronic information.

Whenever a UK company must search its computer systems, it must be cognizant of its bligations under EU directives and UK data protection laws, which balance the legitimate investigative needs of the company with the privacy rights of its employees. It is important that companies be able to demonstrate compliance with data protection laws.

EnCase Enterprise Solutions – which encompass the network-enabled EnCase Enterprise software as well as the EnCase eDiscovery Suite[1017] – can be a critical component in demonstrating compliance with UK data protection laws by proving that a company's investigations into employees' email and other computer data are not excessive, and are accomplished in the least-intrusive way.

For example, a conventional investigation of an employee's laptop would likely entail making a full disk image of the laptop's hard drive, which means that every single file on that laptop (both active and deleted) would be collected for examination. Using EnCase Enterprise, an investigator can instead automatically locate the small handful of files that are responsive to the search criteria, thus vastly reducing the number of files to be examined (and leaving untouched thousands of emails and documents that may contain protected classes of data).

EnCase Enterprise enables companies to demonstrate their compliance with the EU directives

1015 See, Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2669, [the "LBP Regulations"] available at http://www.opsi.gov.uk/si/si2000/20002699.htm.

1016 CPR PD 31 (electronic disclosure).

1017 EnCase Enterprise allows you to reach across the network from a central location to securely investigate multiple machines simultaneously, at the disk and memory levels. EnCase eDiscovery Suite automates 24/7 searches across the network that collect only those emails and electronic files that are responsive to the search criteria used. The individual email and files collected, withtheir metadata intact, are then stored in Logical Evidence Files (LEF), one for each custodian device. These LEFs make it possible to forensically preserve relevant data without having to capture entire hard drives.

and UK data protection laws by proving that investigative and collection procedures employed are not excessive or disproportionate to their legitimate legal purposes. Unlike other means of collecting digital evidence, EnCase Enterprise allows investigators to locate and examine only those email and electronic files that precisely match the specific search criteria identified by the company's lawyers.

Whether investigators are looking at a single computer or the entire company network, EnCase will reveal to them only the documents that meet the search criteria. No longer do investigators need to sift through large numbers of email or electronic documents to find those that are potentially relevant to the legal or regulatory issue at hand.

Part of limiting the intrusion into employees' data is limiting the number of investigators that may need to conduct the reviews. Beyond limiting the number of emails and electronic documents that need to be reviewed, EnCase software also allows a company to limit the number of investigators with access to a particular employee's data. This is accomplished through highly granular role-based permissioning to investigators, so that only certain investigators can reach certain employees' data. Moreover, EnCase software allows investigators to locate, segregate and preserve employee email responsive to search criteria without even opening and viewing the email. Because the software can read the text of the email, investigators can put them aside until it is determined that examination of the email would comply with the data protection laws.

Finally, the EnCase Enterprise software maintains a detailed record of every single search. This allows companies to document precisely what investigations were conducted, what search criteria were employed, and what data were identified as responsive to that criteria. There is no better way toprovide detailed documentation to confirm precisely what employee data were investigated, and to ensure compliance with the data protection laws.

Aside from its compliance advantages, EnCase Enterprise is prized for its robust search capabilities, which allow corporations to conduct investigations from a single central location, and search and collect data from any laptop, workstation, or server on the company's network regardless of its location anywhere in the world. Moreover, the investigation and collection can be conducted without disrupting the employees' use of their computers.

III. The EU Data Protection Directive & UK Data Protection Act

Workplace use of the EnCase Enterprise software – whether for broad eDisclosure collections, support in obtaining legal advice, or investigation of internal wrongdoing – can be accomplished in full compliance with applicable EU and UK law. The applicable law derives from the EU

Directive which is not itself a legal mandate, but rather directs EU Member States to implement its principles. In the UK, the directives principles were converted into binding law through the UK Act which is administered by the UK Information Commissioner.[1018] In addition, the UK Information

1018 See, UK Information Commissioner's Office website at http://www.ico.gov.uk/.

Commissioner issued the UK Employment Practices Code (the "UK Code") as a guide to help employers comply with the UK Act.[1019]

The EU Directive and the UK Act permit the investigation, collection, and analysis of employees' data under certain prescribed circumstances (discussed below) which generally map to companies' legitimate use of EnCase Enterprise, in particular when a company's investigation is for legal purposes. The EU Directive was issued to harmonize data protection legislation throughout the EU so as to balance (1) protection of individual employees' fundamental right to privacy as to personal data, and (2) the goal of a free flow of personal data within the EU, so as to improve the operation of a single European market.[1020] The UK Code states that its aim is:

> [T]o strike a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses.[1021]

a. What Employee Data are Protected by the Data Protection Laws?

The UK Act regulates companies' treatment of employees' "personal data," which is defined broadly to mean:

> [D]ata which relate to a living individual who can be identified — (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[1022]

For example, any email containing an employees' business email address may be deemed "personal data" where the email address clearly identifies a particular individual.[1023] In most cases, therefore,

---

1019 UK Information Commissioner, Employment Practices Code [the "UK Code"], available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code001.pdf. The UK Code states that "[i]t does not impose new legal obligations." Id. at 3.

1020 EU Directive, supra note 1, at art. 1(1)-(2).

1021 UK Code, supra note 7, at 3.

1022 UK Act, supra note 2, at s 1(1). The EU Directive defines "personal data" to mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular byreference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural orsocial identity." EU Directive, supra note 1, at art. 2(a).

1023 In the case of Durant v. FSA [2003] EWCA Civ 1746, the Court of Appeal adopted a narrow view of "personal data" under which an email address, with no additional information, would not likely be considered "personal data" within the meaning of the UK Act. However, shortly after that case was decided, the European Commission, in a letter of formal notice, called upon the UK Government to justify the narrow definition of "personal data" in Durant because it is not in conformity with the broader construction of "personal data" within the EU Directive. For a more detailed discussion of the European Commission's letter, see http://www.outlaw. com/page-4717.

it must be assumed that data reviewed or collected from employees' laptops, workstations, or shared drives would fall within the definition of "personal data."

The UK Act also defines a subset of personal data known as "sensitive personal data" – as to which the regulations are more stringent – that consists of information about the employee as to:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Sex life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed by him,
- the disposal of such proceedings or the sentence of any court in such proceedings.[1024]

b. Threshold Requirements for Investigation, Collection and Review of Employees' Personal Data: Fairness, Lawfulness & Proportionality

The EU Directive and the UK Act both require that every investigation into employees' personal data be conducted "fairly and lawfully."[1025]Fairness is only vaguely defined by the UK Act and subsequent guidance, and lawfulness is undefined.[1026] The UK Information Commissioner, using the expansive term "processing" – which includes investigation, review, and collection of data – takes the view "that in asserting fairness, the first and paramount consideration must be given to the consequences of the processing to the interests of the data subject. (…) The Commissioner will also look at the purposes and nature of the investigation in assessing fairness."[1027]

In all cases, the UK data protection regime urges "proportionality," meaning that the investigation of personal data shall be "adequate, relevant and not excessive in relation to the purpose or purposes"[1028] of the investigation. (Emphasis added.) This is particularly true in situations where a company engages in interception of employees' emails. Such monitoring is specifically regulated in the UK under the Regulation of Investigatory Powers Act 2000 ("RIPA")[1029] and the Telecommunications (Lawful

1024 UK Act, supra note 2, at s 2(2).

1025 EU Directive, supra note 1, at art. 6(1)(a). UK Act, supra note 2, at sch 1, pt 1(1).

1026 The UK Act does not provide any guidance on the meaning of "lawful," although the UK Information Commissioner's Legal Guidance refers to UK courts' broad description of "unlawful" as "something which is contrary to some law or enactment or is done without lawful justification or excuse". UK Information Commissioner, Data Protection Act 1998 -- Legal Guidance [the "Legal Guidance"], para 3.1.4, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf (quoting R v R [1991] 4All ER 481). This can include breaches of any civil or criminal statute or common law, as well as a breach of an enforceable contractual agreement. Id.

1027 Id. at para 3.1.7.

1028 UK Act, supra note 2, at sch 1, pt 1(3).

1029 See RIPA, supra note 3.

Business Practice) (Interception of Communications) Regulations 2000 (the "LBP Regulations").[1030] The LBP Regulations set forth various exceptions to RIPA's prohibitions against interception under certain circumstances that make lawful certain corporate interceptions "for the purpose of running its business."[1031]

Email monitoring also falls within the UK Act, although the UK Act is less concerned "with occasional access to records of this type in the course of an investigation into a specific problem, such as a complaint from a customer."[1032]The UK Code states:

> The Data Protection Act does not prevent monitoring. Indeed in some cases monitoring might be necessary to satisfy its requirements. However, any adverse impact of monitoring on individuals must be justified by the benefits to the employer and others. We use the term "impact assessment" to describe the process of deciding whether this is the case.[1033]

An impact assessment includes "[c]onsidering alternatives, or different methods of monitoring, [which] means asking questions such as":[1034]

> "Can the investigation of specific incidents or problems be relied on, for example, accessing stored emails to follow up on allegations of malpractice, rather than undertaking continuous monitoring?"[1035]

- The precision of EnCase Enterprise facilitates just such an alternative investigatory approach. For example, it enables companies to follow up leads of potential wrongdoing by searching stored emails, which generally is not prohibited if necessary for a valid and defined reason.[1036]

> "Can monitoring be limited to workers about whom complaints have been received, or about whom there are other grounds to suspect of wrong doing?"[1037]

- The customization of searching enabled by EnCase Enterprise technology allows companies to conduct the least intrusive investigation possible. For example, a search can be limited

1030 See LBP Regulations, supra note 4.

1031 UK Information Commissioner, Employment Practices Code - Supplementary Guidance [the "UK Code Supplementary Guidance"], pt 3 ("monitoring at work") at 58-59, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practice_code_- _supplementary_guidance.pdf

1032 UK Code, supra note 7, pt 3 ("monitoring at work"), at 56.

1033 UK Code, supra note 7, pt 3 ("monitoring at work"), at 56. When conducting interception of email without an employee's consent, the UK Code counsels companies to engage in a formal or informal "impact assessment." Id. at 56. In an impact assessment, employers judge whether a monitoring arrangement is a proportionate response to the problem they seek to address. UK Code Supplemental Guidance, supra note 19, at para 3.2.7.

1034 UK Code, supra note 7, pt 3 ("monitoring at work"), at 57.

1035 Id

1036 Legal Guidance, supra at note 14, at para 3.2.8.

1037 UK Code, supra note 7, pt 3 ("monitoring at work"), at 57.

exclusively to data belonging to a particular employee suspected of wrongdoing and – even then – only identifying emails or files containing relevant search terms only from files created or modified during relevant time periods.

"Can monitoring be targeted at areas of highest risk, e.g., can it be directed at a few individuals whose jobs mean they pose a particular risk to the business rather than at everyone?"[1038]

- When an investigation must focus on more than one individual, EnCase Enterprise allows a company to employ highly granular targeting of only those employees that pose a particular risk.

In any case, most corporate investigations are reactive and do not involve real-time interception, and thus do not implicate the highest level of privacy concern under the regulations. Nonetheless, UK regulations generally require companies to consider the "proportionality" of their investigatory approaches toward employee data. EnCase enhances any company's range of alternative investigatory options under an impact assessment. EnCase Enterprise also logs every aspect of the investigation, documenting the company's compliance with data protection regulations and adoption of less intrusive investigatory alternatives.

c. Exemption for Investigations for Legal Purposes

i. Employees' Personal Data

While prior employee consent is generally advisable in the UK if practicable (if only to buttress the company's demonstration of compliance with the data protection laws), the UK Act permits investigations into employees' personal data[1039] "for compliance with any legal obligation" to which the company is subject, other than an obligation imposed by contract.[1040] This exemption covers a significant portion of corporate investigations. The UK Information Commission takes the position that in order for a legal obligation to support an exemption, it must be based on English law or on orders issued by an English court.[1041]

ii. Employees' Sensitive Personal Data

Investigations into sensitive personal data are permissible under the UK Act when "necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the [employer] in connection with employment."[1042] (Emphasis added). For instance, where there

1038 Id

1039 Defined above in section III.a.

1040 UK Act, supra note 2, at sch 1, pt 1(1). Id. at sch 2.

1041 The authors of this white paper sought the Information Commissioner's Office view on this point on March 15, 2007.

1042 UK Act, supra note 2, at sch 3(2)(1).

is evidence that a worker is using the employer's email system to subject another worker to racial harassment, the employer may, in the absence of reasonable alternatives, process the worker's sensitive personal data to meet its legal obligation not to discriminate on the grounds of race.[1043]

In addition, the UK Act permits investigations without employee consent into sensitive personal data[1044] when the investigation:

- Is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- Is necessary for the purpose of obtaining legal advice, or
- Is otherwise necessary for the purposes of establishing, exercising or defending legal rights.[1045]

According to the Information Commissioner, "[t]his condition is most likely to be relevant in the context of prospective or actual tribunal or court proceedings."[1046]An employer may, for example, process an employee's sensitive personal information to defend itself against a claim for unfair dismissal or unlawful discrimination.[1047] Under this exemption, personal data and sensitive personal data may be freely investigated, collected, and transferred by the order of a UK court.[1048] This exception may only reach data sought in connection with legal proceedings before UK courts.[1049] This begs the question of whether UK companies can lawfully search and collect data sought in connection with non-UK litigations or by regulators from other Member States, the US, or other countries. When a company has been ordered to collect data from UK operations in connection with litigation in non-UK courts, UK law provides a means to seek the endorsement of a UK court and thereby come under the exception.

iii. Converting Foreign Legal Obligations Into UK Legal Obligations

Litigators seeking the disclosure of documents or data in foreign countries usually turn to the Hague Conventions. The Hague Evidence Convention[1050] is the primary treaty covering international disclosure in civil and commercial proceedings. Working through the judiciary of contracting states,[1051]litigants are able to obtain local court orders compelling the production of evidence where it is located. In relevant part, the Hague Evidence Convention requires litigants seeking foreign evidence

1043 UK Code Supplementary Guidance, supra note 19, at 72.

1044 Defined above in section III.a.

1045 UK Act, supra note 2, at sch 1, Pt 1(1) and sch 3(6)(a)-(c). See also, Id. at s 35(2) where the identical language is used to indicate that certain "non-disclosure" provisions of the UK Act do not apply.

1046 UK Code Supplementary Guidance, supra note 19, at 73.

1047 Id

1048 UK Act, supra note 2, at s 35(1).

1049 Elizabeth Bowes, None of Your Business, C.T.L.R. 2003 9(3), 87-91, at 88.

1050 See, Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters, signed Mar. 18, 1970, 23 U.S.T. 2555, [the "Hague Evidence Convention"] available at http://www.hcch.net/index_en.php?act=conventions.text&cid=82

1051 For a complete list of contracting states see http://www.hcch.net/index_en.php?act=conventions.status&cid=82#legend

to obtain permission from that country's government,[1052] and to comply with that country's disclosure rules.[1053]

When evidence is sought for use in non-EU proceedings, the UK Evidence Act,[1054] together with Part 34 of the Civil Procedure Rules,[1055] implements[1056] the Hague Evidence Convention by providing the legal framework for compelling evidence located in the UK for use in non-EU foreign proceedings.[1057]

For disclosure requests relating to proceedings in other EU Member States,[1058]the Hague Evidence Convention is supplanted by the "Taking of Evidence Regulation."[1059] Through a standardized form, the court of the Member State before which the proceedings are commenced or contemplated requests the court of the Member State in which the evidence is located to compel production of the desired documents.[1060] Proceeding in accordance with the laws of the Member State where the evidence is located, the court receiving the request is to execute it within 90 days.[1061]

d. Exemption for Legitimate Interests of the Company

A company can also lawfully investigate employee data under the UK Act if is "necessary to meet the legitimate interests pursued by the [company] or by a third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the [employee]."[1062] This exemption is not well defined, and special care must be taken that the data not be used in a manner that would "unjustifiably prejudice the rights and freedoms" of the employee. As an example, a company's collection of information for use in an employee's performance

1052 Hague Evidence Convention, supra note 38, at art. 1.

1053 Id. at art. 2.

1054 See, Evidence (Proceedings in Other Jurisdictions) Act 1975 (c.34) [the "Evidence Act"] available at http://www.statutelaw.gov.uk/legResults.aspx?LegType=All%20Primary&PageNumber=6&BrowseLetter=E&NavFrom=1&activeTextDocId=1218650.

1055 See, CPR 34 available at http://www.dca.gov.uk/civil/procrules_fin/contents/parts/part34.htm.

1056 Although it is widely assumed that the Evidence Act implemented the Hague Evidence Convention, the Act was enacted prior to the Convention's entry into force in the United Kingdom on 15 September 1976. However, the Evidence Act is frequently considered an implementing statute because Parliament was very aware of the Hague Evidence Convention and because its provisions are in complete conformity with it. (See, Cynthia Day Wallace, "Extraterritorial" Discovery: Ongoing Challenges for Antitrust Litigation in an Environment of Global Investment, 5 J. Int'l Econ. L. 353 at n 138).

1057 See Evidence Act, supra note 42, at s 1(a)(b).

1058 With the exception of Denmark, in which the Hague Evidence Convention continues to apply.

1059 See, Council Regulation (EC) No. 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters, Official Journal of the European Communities 2001, No. L174/1 [the "Taking of Evidence Regulation"] available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/l_174/l_17420010627en00010024.pdf.

1060 Id. at art. 2(1).

1061 Id. at art. 10(1).

1062 UK Act, supra note 2, at sch 2(6).

evaluation may be found to be for a legitimate purpose.[1063] The UK Information Commissioner's Office states in its guidance document that it:

> [T]akes a wide view of the legitimate interests condition and recommends that two tests be applied to establish whether this condition may be appropriate in a particular case. The first is the establishment of the legitimacy of the interests pursued by the data controller or the third party to whom the data are to be disclosed and the second is whether the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the [employee] whose interests override those of the [company]. The fact that the processing of the personal data may prejudice a particular [employee] does not necessarily render the whole processing operatioprejudicial to all the [employees].[1064]

e. Exemptions for Prevention or Detection of a Crime or any Unlawful Act

Employers are permitted to investigate and collect employees' personal data for purposes of the prevention or detection of crime or the apprehension or prosecution of offenders.[1065] Such activities are justified without first informing the employee only if openness would be likely to prejudice the prevention or detection of the crime under investigation or the apprehension or prosecution of the alleged offender.[1066] In all cases, companies are expected to have sufficient grounds for suspecting criminal activity or sufficient malpractice before performing a given investigation or collection.[1067] The UK Act additionally permits the investigation or collection of sensitive personal data:

- When it is in the substantial public interest,
- When it is necessary for the purposes of the prevention or detection of any unlawful act, and
- When it must necessarily be carried out without the explicit consent of the [employee] being sought so as not to prejudice those purposes."[1068]

Unlawful acts have been interpreted to include criminal matters, breaches of other common law or statutory obligations,[1069] as well as unlawful failures to act.[1070] For example, employers may investigate allegations of work-related criminal offenses indicated as a result of audit investigations or complaints

1063 UK Code, supra note 7, at 55.

1064 Legal Guidance, supra at note 14, at para 3.1.1.

1065 UK Act, supra note 2, at s 29(3). See also, Id. at s (1)(a)-(b).

1066 Id. at s 29(3)(b).

1067 The Commissioner has expressed the view "that, for any of these […] exemptions to apply there would have to be a substantial chance rather than a mere risk that in a particular case the purposes would be noticeably damaged. The data controller needs to make a judgement as to whether or not prejudice is likely in relation to the circumstances of each individual case. (Emphasis added). Legal Guidance, supra note 14, at 62.

1068 Data Protection (Processing of Sensitive Personal Data) Order 2000 SI 2000/415 s 1(1), [the "Data Protection Order"] available at http://www.opsi.gov.uk/si/si2000/20000417.htm.

1069 UK Code Supplementary Guidance, supra note 19, at 74.

1070 Data Protection Order, supra note 56, at s 1(2).

from customers.[1071] Such investigations may be carried out covertly if seeking an employee's consent would amount to a "tip off."[1072]

f. The Employee's Consent Can Authorize Investigation and Collection of

That Employee's Personal Data Employee consent is a desirable – although often not a mandatory – element of lawful corporate investigations of employees' personal data under the UK Act. For consent to be legally effective, it must be appropriate to the particular circumstances of the investigation. In addition, the consent must be "freely given."

The UK Code states:

> [T]here are limitations as to how far consent can be relied on in the employment context to justify the processing of personal information. To be valid, for the purposes of the [UK Act], consent must be 'freely given', which may not be the case in the employment environment. Once given, consent can be withdrawn.[1073]

For consent to be freely given, there must be no penalty attached to either the withholding or the withdrawal of consent. Imposing a penalty in either case effectively revokes the employee's original consent.[1074]

In the case of personal data, the employee must give "his consent to the processing."[1075] With respect to personal data, where there is no other legal justification (i.e. compliance with a legal obligation of the company), it may be sufficient for the employee to consent orally. In contrast, the investigation of sensitive personal data without a legal justification requires the employee to give his "explicit consent to the processing of personal data."[1076] (Emphasis added). Again, while obtaining consent may be a best practice in any case, with the appropriate legal justification for the investigation, employee consent is not required.

g. Transfers of Employee Data outside the EU

EU and UK laws restrict transfers of personal data outside the EU. This creates compliance headaches for companies whose networks reach across the EU border because they must be careful to ensure that personal data from EU employees are not moved or stored to computers in non-EU portions of their company network. Query whether a company investigator located outside the EU can lawfully have a UK employee's personal data even visible on his or her monitor if not within the EU.

Investigators can ensure compliance with transfer laws by using EnCase Enterprise. EnCase's granular role-based permissions allows companies to build a virtual barrier protecting all EU data

1071 UK Code Supplementary Guidance, supra note 19, at 74.
1072 Id
1073 UK Code, supra note 7, at 59.
1074 UK Code Supplementary Guidance, supra note 19, at 75.
1075 UK Act, supra note 2, at sch 2(1).
1076 Id. at sch 3(1).

from the reach of investigators outside the EU. Companies can also engineer their EnCase Enterprise configuration to assure that data is not inadvertently transferred in violation of EU or UK law.

i. Countries Providing Adequate Protection for Transfers of Employee Data

While employee data can flow freely between EU Member States,[1077] transfers to countries outside the EU may take place only if the receiving country ensures "an adequate level of protection"[1078] for the data (unless one of the exceptions below applies). To date, the European Commission has found that Argentina, Canada, Guernsey, the Isle of Man, and Switzerland ensure an adequate level of protection.[1079]

ii. Exceptions to a Finding of Adequacy for Transfers of Employee Data

Data can be transferred to non-EU locations other than the five listed above (1) when the employee gives unambiguous consent to the transfer, or (2) when the transfer is necessary for the establishment or defense of legal claims,[1080] for example, in connection with pending legal proceedings. The UK Information Commissioner interprets this exception to include legal proceedings outside of the UK.[1081]

iii. Contractual Solutions

For transfers between two separate companies or between different branches of the same corporate group, pre-approved standard contractual clauses can be used to transfer personal data from within EU Member States to non-EU countries.[1082] In the alternative, ad hoc contractual agreements are available. Most Member States require that their domestic Data Protection Authority ("DPA") approve these individually negotiated contracts for transfers originating in that Member State. If approved, the contracts must also be notified to the European Commission and to other Member States.

iv. Binding Corporate Rules ("BCR")

Corporations that are found to have implemented a comprehensive global policy on data protection -- commonly known as Binding Corporate Rules (BCR) -- may perform intra-company transfers of personal data that cross EU borders. To take advantage of BCR, a corporation's data protection policy

1077 Personal data may also flow freely between the EU and European Economic Area (EEA) member countries (Iceland, Liechtenstein and Norway).

1078 EU Directive, supra note 1, at art. 25(1).

1079 Id. at art. 25(6). See also, European Commission, Commission decisions on the adequacy of the protection of personal data in third countries, http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

1080 Id. at art. 26(a), (d).

1081 UK Information Commissioner, The Eighth Data Protection Principle and international data transfers, s 4.51 available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/international_transfers_legal_guidance_ v2.0_300606.pdf

1082 For additional information regarding model contracts see http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm

must be approved by the DPA in each exporting Member State and also (1) satisfy the data protection principles established in the EU Directive, (2) legally bind the corporation to its terms, and (3) allow employees to enforce compliance through courts and DPAs.

v. Safe Harbor

In addition, US companies may enroll in an EU-approved "Safe Harbor" program that permits the receipt of personal data transfers from the EU. When a non-EU company becomes certified under the safe harbor, it assures EU organizations that it provides adequate data protection within the meaning of the EU Directive.[1083]

IV. Conclusion

With EnCase Enterprise, companies have the capability to implement less intrusive corporate and legal investigative, collection and preservation processes in compliance with EU and UK data protection laws. EnCase Enterprise enables corporate investigators and litigation support personnel to collect and preserve only the employee data that meets precise search criteria, while still conducting robust searches for data demanded by regulators and the company's lawyers. Because EnCase Enterprise logs each search and its results, company's can document the proportionality of their investigations and its compliance with data protection laws. Use of EnCase Enterprise also assists global corporations in their compliance with data transfer prohibitions through its stringent permissioning capability.

1083 For additional information on the US Safe Harbor program see http://www.export.gov/safeharbor/SH_Overview.asp.

Seeking a Balance in the Discovery Equation: Pre-trial Disclosure/ Discovery in UK and US Civil Litigation of European-Based Data

by Denise Backhouse, Morgan Lewis
and Patrick Burke,Guidance Software
Copyright 2009 by Gudiance Software and Morgan Lewis, Reprinted with permission.

1 INTRODUCTION

Companies operating in the global economy routinely generate, move and store dataaround the world. When litigation arises in the UK or US that implicates data residing in Europe, basic actions required to satisfy British and American disclosure or discovery obligations may put the company in violation of European laws that recognise and protect individual privacy rights in employee workplace data. For example, under the uropean Union ("EU") Data Protection Directive[1084] and related national enabling egislation, measures taken simply to preserve emails and electronic records for potential use in a UK or US lawsuit under a litigation hold directive are in themselves likely to violate protected European employee privacy rights.

With no established protocol available for handling international disclosure/discovery (hereinafter "disclosure") responses, little published decisional law and scattered official guidance, corporations and their counsel have struggled for years to balance competing legal obligations under US and European law. These issues have taken centre stage in the past year with the publication of significant guidelines and recommendations by authorities in the EU regarding the proper handling of EU data in the US discovery process.

This White Paper examines these recent developments in the broad context of the EU Directive. With the dialogue underway, this Paper analyses special precautions that a party should consider implementing under the still-emerging protocols, and looks for potential ways forward.

2 THE EU DIRECTIVE – AN OVERVIEW

In principle, absent specific justification the EU Directive restricts the "processing" and subsequent transfer outside of the EEA of "personal data" by "data controllers" and "data processors." These terms, deceptively familiar to the ears of US litigators, take on special meanings under the EU Directive and associated national laws.[1085] Understanding them is key to comprehending the reach of the EU data protection laws.

Under the EU Directive, "personal data" is defined as:

1084 Directive 95/46/EC of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personnel Data and on the Free Movement of Such Data (O.J. 95/L281) (the "EU Directive").

1085 The EU Directive does not itself have the force of law; rather, it provides the overarching framework for the data protection laws required to be enacted by each of the EU member states. National ata protection legislation may differ from and expand significantly upon the EU Directive. In addition, other ational laws and regulations may have a direct bearing on the handling data sought in US discovery. Because of the number of possible sources of rules affecting disclosure/discovery in the UK andUS of data esiding in Europe, we recommend that local counsel be consulted in any such circumstances.

> "any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." EU Directive, Art. 2(a).

This encompassing definition is generally interpreted to include business email and electronic records which by their nature contain identifying information in fielded metadata. Further, heightened protections are afforded to subclasses of "sensitive personal data" that concern the data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or pertaining to the subject's health or sex life. EU Directive, Art. 8(1).[1086] The scope of activity that constitutes "processing" is similarly expansive, including:

> "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." EU Directive, Art. 2(b).

Consequently, "processing" covers almost any activity undertaken by a data controller or data processor using automatic means regarding personal data. This includes the acts of preserving and storing electronic data for litigation purposes. Furthermore, the term "processing" extends to hard-copy files that are part of an organised filing system. Accordingly, many activities that are typically associated with discovery compliance or with conducting an internal investigation in general, such as the collection, preservation and organisation of data belonging to selected company personnel, applying search terms, and the review of selected data, would all fall within the broad definition of "processing."

A "data controller" is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." EU Directive, Art. 2(d). Many key provisions of the data protection legislation focus on the data controller. Moreover, "the law of the EEA country where the 'data controller' is established will apply to the question of whether the relevant personal data can be legitimately 'processed' under the EU Directive and the local laws which implement the [EU] Directive." The Sedona Conference, Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery at (Public Comment Version Aug. 2008) (the

1086 Article 8's prohibitions do not apply if the data subject gives explicit consent to the processing of the data or where the processing is necessary to meet the obligations of the controller in the field of employment law or to protect the vital interests of the data subject or another person where the data subject is incapable of giving his or her consent. EU Directive, Art. 8(2)(a)-(c). Similarly, processing by certain types of foundations or trade unions may be excepted from the general proscriptions of the directive, as is the processing of data made public by the data subject. *Id.* Art. 8(2)(d), (e). Other exceptions exist in the context of medical treatment and law enforcement. *See id.* Art. 8(3)-(7).

"Sedona Framework)") at 12. Furthermore, if separate entities in a corporate group are established in several countries with different personal data processing laws, the laws of each country could apply to the processing of personal data. See id.

A "processor" is a "natural or legal person . . . or any other body which processes personal data on behalf of the controller." EU Directive, Art. 2(e). As with "processing," the term "processor" has a much broader meaning than in the United States, where typically it refers to a technology service provider retained to prepare electronically stored information for use in discovery. In contrast, under the European laws the term includes any entity that stores or processes data in its ordinary course of business.

The EU Directive and member nation data protection acts ("DPA"s) set out certain exceptions to the general prohibition on processing and transferring personal data outside of the EEA, and to the extent that it is permitted, establish criteria for proceeding with data processing and transfer. Although several of the exceptions grounds appear on their face to provide adequate justification to proceed with UK or US discovery, piecemeal guidance over many years warned practitioners to be cautious in their reading of the provisions, particularly when the case is litigated from a non-European court. This year, these issues were addressed in a consolidated effort seeking uniformity of approach to civil litigation across EU member states.

3 DATE PROCESSING AND TRANSFER ISSUES IN CROSS-BORDER PRETRIAL DISCOVERY – GUIDANCE FROM THE ARTICLE 29 DATA PROTECTION WORKING PARTY[1087]

Article 29 of the EU Directive established an independent Working Party with advisory status, composed of a representative of each EU member state's data protection and privacy authority. Over many years, the Article 29 Working Party has provided piecemeal guidance on a variety of issues concerning cross-border discovery. In February 2009, the Article 29 Working Party issued WP 1584 in which it recognises the tension between US disclosure obligations and European data protection requirements. The document focuses on US, not UK, electronic disclosure requirements, which hew to more "proportionate" obligations and have yet to create the same level of conflict with EU data privacy restrictions. However, while explicitly acknowledging that "the parties involved in litigation have a legitimate interest in accessing information that is necessary o make or defend a claim," the Working Party cautioned that "this must be balanced with the rights of the individual whose personal data is being sought." Id. at 2. The following is an analysis of guidance in interpreting the EU Directive and related national legislation provided by the Article 29 Working Party in WP 158 and earlier publications.

To the extent that company records contain employee "personal data," any "processing" of that data must be "lawful" and in accord with the EU Directive and the national DPA. Moreover, Article 6 of the EU Directive requires that data controllers ensure that personal data is:

1087 Article 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation (Feb. 11, 2009), (00339/09/EN/WP 1588) (WP 158), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

a) processed fairly and lawfully
b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical, or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards
c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
d) ccurate and, where necessary, kept up to date; every reasonable stepmust be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified
e) kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member states shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical, or scientific use.

The Article 29 Working Party has examined the concept of lawful processing in detail. Lawful processing must address the principles of finality, legitimacy, proportionality, and transparency. See Article 29 Data Protection Working Party, Opinion 8/2001 on the Processing of Personal Data in the Employment Context (Sept. 13, 2001), (5062/01/EN/Final WP 48) (WP 48) at 3, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf. Here,

> "finality" requires that personal data "must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes." Id. "Legitimacy" requires that data only be processed for legitimate purposes and in accord with the provisions of Article 7 of the EU Directive. Id. "Proportionality" forbids the processing of data for a purpose beyond that for which it was collected and requires that the processing of personal data so collected "still [be] fair to the worker." "Transparency" requires that employers notify employees of the data they are collecting about them, give employees access to and as the case may be, update such data upon request, and inform employees of why the data is being processed, the categories of entities to which the data may be disclosed, and the eventual transfer/disclosure of their personal data outside of the EU.

While Article 6 of the EU Directive spells out what a controller must consider when it is permitted to process personal data, Article 7 enumerates the circumstances in which processing can take place at all. See EU Directive, Art. 7(a)-(f).[1088] On their face, provisions regarding consent (Art. 7(a)), compliance with a legal obligation (Art. 7(c)), and legitimate interests (Art. 7(f)) appear to provide sufficient bases for processing employee data in the context of discovery compliance. However, these

1088 Although the legislation of member nations generally track Article 7's admonitions, counsel and their clients should consult the particular Data Protection Act of the member nation at issue for any nuances that may be present.

provisions are construed narrowly. While meeting a legal obligation (Art. 7(c)) looks like a good fit for proceeding with US discovery compliance, in fact the legal obligations must arise under domestic or communitywide legal obligations. See Article 29 Data Protection Working Party, Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime (Feb. 1, 2006), (00195/06EN WP 117) (WP 117) (finding that "any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive 95/46/EC").

Regarding consent, the Article 29 Data Protection Working Party has stated that it must be freely given and rescindable at will. See WP 48 at 23. Furthermore, fully informed consent is required.[1089] Id. Thus, if a controller seeks consent from a data subject regarding the processing of his or her personal data, the controller will need to specify the purpose for which the data is to be processed and the means and manner of the data processing. See id. Furthermore, the controller can process the data only for the specific purpose for which the data was collected and may not commingle the data with ther data collected for some other purpose. See id.Obtaining "consent" is one of the few promising approaches for US (and UK) litigators to effectuate collection and production ofEuropean employees' ESI within the bounds of EU data privacy. Relying n consent, however, can be problematic. Even in those matters where consent is a strategic possibility, the need to obtain consent from all data subjects—not just the record custodian—and the right of data subjects to withdraw their consent or to cure any incomplete or inaccurate information poses substantial hurdles for parties relying on consent as a basis for processing. See EU Directive, Art. 12(b) (data subject has the right to rectify incomplete or inaccurate data); EU Directive, Art. 14(a) (data subject's right "to object at any time").

In WP 158, the Article 29 Data Protection Working Party stated that it considers it "unlikely that in most cases consent would provide a good basis for processing." Id. at 8. In reaching this conclusion, the Working Party explained that the consent of third parties identified in the data (for example, customers) is required and assessed the relatd practical difficulties. Id. The Working Party also noted that for consent tobe freely given, data subjects "must have a real opportunity to wihhold . . . consent without suffering any penalty, or to withdraw it subsequently if [the data subject] changes his mind." Id. at 9. For these reasons, the Working Party reiterated its earlier conclusion that "[r]elying on consent may . . . . prove to be a 'false good solution,' simple at first glance but in reality complex and cumbersome." Id. (quoting Article 29 Data Protection Working Party, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (Nov. 25, 2005), (2093/05/EN WP 114) (WP 114) at 11, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

The Working Party observed that "the requirements of the litigation process may be found to be necessary for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed under Article 7(f)" and thus justify the processing of personal data. See

1089 Although the EU Directive does not expressly mandate that consent be in writing, some EEA jurisdictions, e.g., Germany, do require a writing for consent to be effective. Because of this possibility and ue to the detail required for consent, we believe that a party using consent as a means for legitimising the processing of personal data should seek to have the consent in writing.

WP 158 at 9. The authors also state, however, that "[t]his basis would only be acceptable where such legitimate interests are not overridden by the interests of fundamental rights and freedoms of the data subject." Id. Factors in the necessary balance of interests test between the controller and the data subject require examining the fundamental concepts of proportionality, transparency and notice, data access and the right to cure, and data security.

Proportionality is derived from Article 6 of the EU Directive, which requires the fair and lawful processing of data and that data be collected for "specified, explicit, and legitimate" purposes. This requires "data controllers involved in litigation to take such steps as are appropriate . . . to limit the discovery of personal data to that which is objectively relevant to the issues being litigated." WP 158 at 10.

To accomplish this, the Working Party recommends applying filters to limit the processing of data not called for in the litigation. Id. at 11. It also observed that filtering should take place locally, where the personal data resides, before the portion deemed relevant to the litigation is transferred to another, non-EEA jurisdiction. Id. For a discussion of how companies have used EnCase® network-based filtering and collection technology to accomplish "surgically" targeted collection of German employees' ESI to the satisfaction of certain German works councils, see Guidance's prior White Paper entitled "Obtaining German Works Council Approval to Collect Employee E-mail and Electronic Documents".

Companies use EnCase® eDiscovery technology to search European employees' ESI and collect only that ESI which contains certain keywords and falls within relevant timeframes, leaving the remaining non-responsive ESI untouched. These companies re able to provide employees with reassurance that truly personal communications are not being swept up, reviewed and disseminated.

Once implemented, the surgically targeted collections can be made transparent to employee representatives, who can receive notification each time the search technology is used. This provides employees with the opportunity to decide – on a case-by-case basis – whether, and to what extent, their privacy rights have been implicated.

Companies can also build trust with their European employees through transparency of process and technology. Before implementing a collection approach, companies are well advised to sit down with employee representatives, unions and/or works councils to explain the techniques and privacy safeguards being employed. Such advance notice, and invitations for employee feedback, can go a long way.

The Working Party suggests, where possible, the use of anonymization or redaction techniques. Id. These tools attempt to "scrub out" the names, email addresses and other personal information through the use of searchalgorithms. Some UK and US litigators have followed this approach, finding ways to use the content of the ESI while adapting to their inability to know the identities of the authors and recipients of ommunications, as well as the other scrubbed-out content. The Working Party considered the issue of who could make the objective determination of relevancy, including the possibility of outsourcing this role to a trusted third party:

> The Working Party recognises that [filtering] may cause difficulties in determining who is the appropriate person to decide on the relevance of the information taking into account the strict time limits laid down in the US Federal Rules of Civil Procedure to disclose the information requested. Clearly it would have to be someone with sufficient knowledge of the litigation process in the relevant jurisdiction. It may be that this would require the services of a trusted third party in a Member State who does not have a role in the litigation but has the sufficient level of independence and trustworthiness to reach a proper determination on the relevance of the personal data.

WP 158 at 11. The Working Party also recommended that parties in this situation should explain to the relevant US court the difficulties posed by a production request and seek a protective order to comply with EU and national rules. Id.

Transparency addresses the kind and timing of information that must be provided to a data subject when his or her data is being processed in accord with Article 7(f) of the EU Directive. Relying on Article 10 of the EU Directive, the Working Party opined that, in the context of pre-trial discovery, data subjects should receive advance, general notice of the possibility of personal data being processed for litigation in the United States and hat once personal data was processed for discovery purposes, the identity of any ecipients of the data should be given to the data subject; the purposes of the processing and the categories of data at issue should be identified, and data subject should be informed of their rights with respect to that data. Id.

Similarly, under Article 11, notice should be provided to data subjects "as soon as is reasonably practicable after the data is processed" in those situations where the data is collected from a third party (e.g., computer data off their employer's network) and not directly from the subject. Id. Interestingly, the Working Party also observed that the iming of notice contemplated by Article 11 concerning data in the possession of a third party could be delayed if there is a risk that such notice would jeopardise the safety or integrity of the data and/or impede the company's ability to investigate matters. Id. at 12. The Working Party cautioned that such an exception regarding notice "must be applied restrictively on a case by case basis." Id.; see also WP 117 at 13 (discussion of Article 11 notice in the context of the establishment of whistleblower hotlines).

This notice is more than an informational tool. It provides the data subject with an opportunity to exercise his or her "right to object at any time on compelling legitimate grounds to the processing of the data relating to them" under Article 14 of the EU Directive. WP 158 at 12; see also WP 117 at 9. Compelling legitimate grounds for such objection would include violations of the EU Directive's principles of data quality and proportionality (as found in Article 6 of the EU Directive and discussed supra), notice (as addressed by Articles 10 and 11), rights of access, rectification, and erasure under Article 12, and the secure handling of data as required by Article 17. See WP 117 at 9- 15.

The data subject's right to access his or her data and to cure inaccurate or incomplete data is another fundamental right that must be balanced when assessing the feasibility f processing data under Article 7(f) of the EU Directive. Moreover, Article 12 gives the data subject the right to have access to the data held about him or her in order to check its accuracy and rectify it if it is inaccurate,

incomplete, or outdated. And, as noted by the Working Party, the right to access and to cure allows a data subject to check the personal data that has been processed and to satisfy himself or herself that the data to be transferred "is not excessive." WP 158 at 12.

Of all the rights examined thus far when considering whether the processing of personal data under Article 7(f) is a possibility, the right to data access and cure poses significant issues for counsel conducting an internal investigation or, worse yet, responding to a disclosure or discovery demand or investigative subpoena. For example, giving document custodians the ability to winnow out "excessive" materials raises compliance concerns about the completeness of a US production and could lead to the expenditure of a great deal of time, effort, and money validating the decisions made by custodians. This problem is circumvented by companies that have the capability – provided by nCase® eDiscovery – to apply targeted search and collection technology against the various locations on the network where employees' ESI resides. Similarly, altering or removing data from a "production set" of materials as a result of withdrawals of employees' consents could give rise to allegations of spoliation or obstruction. Indeed, the Working Party, with measured understatement, noted that "this right could give rise to a conflictwith the requirements of the litigation process to retain data as at a particular date in time and changes (whilst only for correction purposes) would have the effect of altering the evidence in the litigation." See WP 158 at 12.

The final factor to be weighed concerns the need for the data controller to "take all reasonable technical and organisational precautions to preserve the security of the data to protect it from accidental or unlawful destruction or accidental loss and unauthorised disclosure or access" as mandated by Article 17 of the EU Directive. Id. Th aforementioned precautions apply not only to the controller, but to other actors in the litigation drama, including the law firms involved inthe matter, the court adjudicating the matter, and retained experts, who must also comply with the principles of the EU Directive. Id. at 12-13.

Given the complexities associated with processing personal data, passage along the road to the lawful and fair processing of employee data subject to the rules established by the EU Directive and the laws enacted by EEA countries is neither easy nor quick. Because of this, companies and their counsel should begin assessing avenues for the processing of data in the EU before an immediate need arises, if at all possible. uances in the local statutory regime, nation-specific case law on the topic of personal data protection, formal and/or informal rulings or guidance offered by national data protection bodies, as well as the applicability of regulations outside the context of data protection,[1090] must be considered by companies facing the data processing challenge posed by the European rules and regimes. Assuming that a mechanism can be found to process personal data, a means must be found to facilitate the onward transfer of that data from its home to the United States so that it can be examined by counsel or produced in litigation. As was the case with processing, the onward transfer of personal data from the EEA to the United States has its own labyrinth of rules that must be negotiated. Transfer to the UK is, over course, less problematic, although not always without legal obstacles.

Turning to the concept of onward transfer, the EU Directive and national DPAs significantly

1090 Other applicable restrictions may arise under, for example, blocking statutes, industry- or subject matter specific laws, and labor land workplace laws and regulations

restrict the transfer of personal data to locations outside of the EEA. With a few exceptions, transfer of data to countries lacking an adequate level of protection for personal data is prohibited; specifically, the United States is deemed to provide inadequate protection. See EU Directive, Art. 25. It is not, usually, an issue with regard to transfers to the UK. Although the term "transfer" is not defined, the EC has stated that "all the cases where a controller takes action in order to make personal data available to a third party located in a third country" could be deemed a transfer of personal data.[1091] Article 26 of the EU Directive addresses derogations to that general prohibition. Possible grounds for onward transfer of data from the EEA to a location like the United States, include apparently promising grounds of unambiguous consent by the data subject (Art. 26(1)(a)) and/or that the onward transfer is "necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims." (Art. 26(1)(d)).

Unfortunately, both exceptions, like those relating to processing, are limited as to transfers to the US. For example, consent in this context must be given prior to the transfer, and be unambiguous, specific to the transfer at issue, freely given, and informed. See EU Directive, Arts. 2(h), 26(a). Furthermore, consent must be obtained from all identifiable data subjects, and not just the data custodian. The conditions under which an onward transfer can be justified as being "legally required" are also interpreted narrowly[1092] by the Article 29 Data Protection Working Party:

> The Working Party emphasises that the concept of "establishment, safeguarding or defence of legal claims" must here again be subject to strict interpretation. Thus, for example, the parent company of a multinational group, established in a hird country, might be sued by an employee of the group currently posted to one of its European subsidiaries. The exception in Article 26(1)(d) appears to allow the company to legally request the European subsidiary to transfer certain data relating to the employee if these data are necessary for its defence.
>
> . . . .
>
> In addition, this exception can only be applied if the rules governing criminal or civil proceedings applicable to this type of international situation have been complied with, notably as they derive from the provisions of the Hague Conventions of 18 March 1970 ("Taking of Evidence" convention) and of 25 October 1980 ("Access to Justice" Convention). WP 114 at 15.

The Working Party members recently revisited these issues in WP 158, stating that "[w]here

1091 To the extent the data controller is located in a Member State, the laws of that state will dictate whether and how personal data can be transferred outside the European Community. Transfer FAQ, page 19. If the data controller is located outside the Community, the laws of the Member State where the processing equipment is used will apply. Id.

1092 Even if this exception could be used to justify the onward transfer of data to the United States, the Article 29 Data Protection Working Party has opined that "other relevant provisions of the Directive need to be respected." Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 at 8, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/2005/2p114_en.pdf.

the transfer of personal data for litigation purposes is likely to be a single transfer of all relevant information, then there would be a possible ground for processing under Article 26(1)(d) of the Directive where it is necessary or legally required for the establishment, exercise or defence of legal claims."

This potentially helpful exception, however, is very limited. First, this applies in the context of "litigation": a transfer based on Article 26(1)(d) cannot be premised "on the grounds of the possibility that legal proceedings may be brought one day in US courts." P 158 at 13 (citing WP 114 at 15). Second, a requirement of a single delivery of data, although possible in some matters, does not allow for supplemental prodution or future additional custodians. Third, the reference to "relevant" presupposes that a relevancy review has taken place within the EEA member nation in which the data is located.

Nevertheless, WP 158 may suggest a softened approach to the use of the Hague Convention[1093] as a necessary step to using Article 26(1)(d) as a basis for the onward transfer of data appears to have changed somewhat from that stated in WP 114, which is quoted above. In WP 158 Working Party authors recognise that resorting to the Hague Convention cannot be an absolute precondition for the onward transfer of personal data because some EEA member nations have not signed the Hague Convention and other members that have signed it did so with reservations under Article 23 of the treaty[1094] with respect to compliance with discovery demands arising from foreign—i.e., US—litigation. See WP 158 at 13. As a result of this recognition, the Working Party now notes that resorting to the treaty for data found in countries that (1) are signatories to the treaty and (2) have not signed with reservations about US (or other foreign) discovery is an apparently independent basis for the onward transfer of personal data: "Where it is possible for the Hague Convention to be used, the Working Party urges that this approach should be considered first as a method of providing for the transfer of information for litigation purposes." WP 158 at 14.

1093 Hague Evidence Convention on the Taking of Evidence Abroad in Civil or Commercial Matters Mar. 18, 1970, 23 U.S.T. 2555, T.I.A.S. No. 7444, 847 U.N.T.S. (1972). Although a discussion of all the issues associated with reliance on the Hague Convention as a means of facilitating discovery is beyond the scope of this paper, the Working Party's take on the efficacy of resort to the Hague—"[w]hilst there may be some concerns about the length of time such a procedure could take, the courts, for example in the U.S., are experienced in the use of the Hague and such timescales can be built into the litigation process"—seems optimistic. Moreover, US courts take the view that the procedures afforded by the Hague Convention are but "one method of seeking evidence [abroad] that a court may elect to deploy." *Societe Nationale Industrielle Aerospatiale v. United States District Court for the Southern District of Iowa,* 482 U.S. 522, 541 (1987). Indeed, the complexities associated with invoking the Hague Convention, the time frame associated with achieving results under the Hague, and the convention's requirements for specificity with respect to how document requests must be made are among the reasons cited by U.S. litigants for proceeding abroad under the Federal Rules of Civil Procedure, without resort to the treaty. Furthermore, resort to the Hague treaty would not be an option in matters that had not yet ripened into an actual case.

1094 For example, France limits discovery in that country to only those means referenced expressly in the treaty, i.e., letters rogatory, depositions before a diplomatic official, or depositions before a duly appointed commissioner. See ABA Section of Antitrust Law, Obtaining Discovery Abroad 112 (2d ed. 2005). Similarly, Germany does not appear to permit pre-trial document discovery under the Hague Convention, id. at 137, while Italy limits pre-trial discovery to only the tools afforded by the treaty and furthe limits discovery to those matters deemed "civil or commercial" under Italian law. Id. at 158; see generally, Sedona Framework at 17 (citing Soiret, The Foreign Defendant: Overview of Principles Governing Jurisdiction, Venue, Extraterritorial Service of Process and Extraterritorial Discovery in U.S. Courts, 28 Torts & Ins. L.J. 533 (1993)).

Given the limitations on invoking the Hague Convention, for a company trying to review materials in order to meet regulatory obligations or to detect internal wrongdoing, compliance with Article 26(1)(d) or a handful of narrowly tailored alternative avenues for the onward transfer of data are the only options available for now.

Furthermore, the French Commission nationale de l'informatique et des libertés, CNIL, has recently published its own recommendations on the transfer of personal data specifically in the context of American discovery proceedings. The official text in French is available at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000020981625&dateTexte=&oldAction=rechJO&categorieLien=id

In its Recommendations, CNIL generally endorses the data processing principles explained above, but also confirms that all US discovery requests must comply not only with applicable French data protection laws, but must also be made through the Hague Convention, in accordance with the French blocking statute.[1095]

4 A WAY FORWARD?

4.1 Looking Behind the Buzzwords

Companies and counsel subject to UK disclosure and US discovery obligations are actively seeking a way forward that respects the privacy rights of Europeans. The Article 29 Working Party cited The Sedona Framework in WP 158 and is engaged in the early stages of a dialogue with The Sedona Conference, which it is hoped will eventually result in a more nuanced appreciation and understanding of the issues on both sides of the discovery equation. Such endeavours highlight the points of similarity in the different systems.

In the absence of agreed-upon protocols, a company with data residing in Europe that might be used in or transferred to the United States should consider taking the following data protection "readiness" steps to position itself to best address the dictates of the EU Directive:

1. Implement audited and certified data management policies and proceduresdesigned to minimize the potential for privacy infringement. These measures should include:

    a. Structuring or segregating data to facilitate the ready identification of personal data, especially data of a highly personal or sensitive nature.
    b. Implementing in-house technology – such as EnCase® eDiscovery – that enables companies to conduct surgical collections of European employees' ESI that protects against collection of employees personal data except that which meets targeted search criteria.
    c. Availing themselves of technologies that can be used to anonymize or redact data (to the extent the use of such technology is otherwise consistent with discovery or other legal obligations).

1095 Law no. 68-678 of July 27, 1968, created by law no. 80-538 of July 16, 1980.

d. Informing data subjects and their representatives, through their respective European employers, of any further transfer of their personal data, for company management purposes and/or compliance with US mandatory laws.
e. Implementing computer systems and email usage policies that clearlydefine acceptable usage of computers and networks and the ownership of that equipment and data on that equipment, and that set users' expectations of privacy for the data stored on the machine or device they use.
f. Obtaining, when necessary, general and matter-specific consent from employees/data custodians.[1096]

2. The company should consider taking steps to familiarize itself with the nuances of the applicable legislation and with existing means that can be used to facilitate the flow of data between Europe and the United States and/or among EU member states. For example, the company might:

   a. Designate an employee or select counsel to liaise with local data protection officials in an effort to make sure any local authorisation or certification is received for transfers of data; and/or
   b. Take advantage of existing mechanisms for the transfer of data from the European Economic Area (EEA) to the United States. These mechanisms include enrolling in the Safe Harbor certification program sponsored by the US Department of Commerce, the use of Standard Contractual Clauses, and/or the implementation of Binding Corporate Rules (BCRs) governing intercompany data transfers.[1097]

3. In the context of responding specifically to US discovery requests, a company should consider the following options:

   a. Carefully consider the nature of the discovery request to determine ifsome portion of the information sought resides in the United States or isotherwise available from a source that does not implicate EU data protection issues
   b. Work closely with local in-house IT or IT Security personnel or, where appropriate, third-party service providers resident in the member nation, to filter or cull the data (e.g., by the use of key terms) so that extraneous information is eliminated before it is used in or transferred to the United States.[1098]

1096 While as previously discussed, consent in itself may be of limited value, it may have the practical effect of setting expectations and reducing the likelihood of surprise and complaints.

1097 While a full discussion of these mechanisms is beyond the scope of this Paper, it should be noted that each of them requires adherence to strict rules that may severely limit their application to a situation in which information is being gathered in Europe and then transferred to the United States for disclosure to a third party, such as a federal investigating agency or an adverse party in a litigation matter.

1098 Both WP 158 and the CNIL Recommendations contemplate the leveraging of trusted third-party service providers in managing the discovery process.

c. Alert the US court or agency to the data protection issues and seek a protective order or confidentiality agreement pertaining to the materials.
d. Work with opposing counsel or the agency requesting the data in an effort to narrow the scope of the request as much as possible and to agree to a court order setting protocols for tighter security and confidentiality for European employees' data produced, even when used as evidence in the case.
e. Consider the use of Standard Contractual Clauses to facilitate the onward transfer of data to third parties.
f. Carefully consider whether there are any additional national laws and rules, especially those aimed at thwarting "foreign" discovery, that might come into play.

ABOUT GUIDANCE SOFTWARE (GUID)

Guidance Software is recognised worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organisations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to eDiscovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing - all while maintaining the integrity of the data. There are more than 28,000 licensed users of the EnCase technology worldwide, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organisations worldwide, EnCase has been honored with industry awards and recognition from eWEEK, SC Magazine, Network Computing, and the Socha- Gelbmann survey. For more information about Guidance Software, visit www.guidancesoftware.com.

eDisclosure after Jackson: Developements in electronic Disclosure in England & Wales (with an Update on US eDiscovery law)

by Chris Dale, e-Disclosure Information Project,
Denise Backhouse, Associate, Morgan Lewis,
and Patrick Burke, Senior Director & Assistant General Counsel, Guidance Software
Copyright 2010 by Guidance Software.

1. INTRODUCTION

1.1 Executive Summary

This is one of a series of white papers written by Chris Dale of the UK-based. Its purpose is to summarise the developments in thinking and in case law relevant to the management of electronic disclosure in the courts of England & Wales, and also to provide a brief overview of recent developments in US eDiscovery. The word "thinking" is used advisedly – recent months have seen both the Report on Litigation Costs produced by Lord Justice Jackson and a draft Practice Direction and ESI Questionnaire produced by a working party led by Senior Master Whitaker. Between them, they contain a great deal of thoughtful work on e-Disclosure. None of that is likely to reach the rule book until the Autumn of 2010. It is, nevertheless, influential in the true sense of that word – its influence is being felt in practice and not merely discussed in theory. The cases are based on existing law. It is part of the purpose of this paper to show that there is a short and straight line from the rules as they stand to the proposed changes; they are important, but they serve more to emphasise existing obligations than to create new ones.

1.2 The E-Disclosure Information Project

The e-Disclosure Information Project disseminates information for those with an interest in electronic disclosure in the UK courts, including judges, practitioners, suppliers and corporate clients. Its aim is the reduction of the expense of litigation. It is run by Chris Dale, a former commercial litigation solicitor and adviser on all aspects of electronic disclosure, including the court rules, the practical issues which arise and the solutions which exist to tackle them. The main expectations of such a project are that it is knowledgeable, independent and objective. It has no client and can exist only if it is funded by sponsorship. The sponsors have in common that they are interested in and knowledgeable about aspects of e-Disclosure wider than their own commercial advantage, and that they are willing to pool resources in this indirect way to raise understanding of the issues. Guidance Software is a sponsor of the Project.

1.3 What is EnCase® eDiscovery?

EnCase® eDiscovery is a software application which can be implemented internally by a corporation to search, identify, collect, and process electronically stored information ("ESI") from servers, laptops and work stations across their global network from a central location without interfering with employees'

use of their computers. The software gives companies the option of automated over-the-network collection of only those e-mails or documents responsive to search criteria (keywords, time-frames, file types etc), of all user-created files, or of full-disk images. Companies with EnCase can also process the collected e-mail and electronic documents, culling them down and creating load file formats for loading into any lawyer review platform, thus avoiding or reducing the expense of processing by outside bureaux.

The EnCase® collection technology has substantial court validation in the United States and other jurisdictions, and is well-known world-wide as the collection and preservation technology of choice for law enforcement and regulators and various intelligence and military entities. EnCase technology has also been adopted at over 500 major companies worldwide. For these and many other major corporations, EnCase eDiscovery is a key component of an in-house, systematised, repeatable, and defensible process. It is described on the Guidance Software website at www.guidancesoftware.com/ediscovery/discovery.aspx

1.4 Disclaimer

This white paper is written by Chris Dale in conjunction with Guidance Software as an informational resource only. It is not intended to be relied upon as a source of legal or technical advice.

2. PURPOSE OF PAPER

2.1 Update for US and UK Judges

The origin of this paper lies in the wish to summarise developments in e-Disclosure in England and Wales for a group of US Magistrate Judges – and similarly for UK judges – attending IQPC's Information Retention and e-Disclosure Management Summit in London on 17 to 19 May 2010 as part of a judicial panel comprising the best of US and UK judicial thinkers (and doers) from both sides of the Atlantic to discuss developments in our respective jurisdictions. The participants in the panel and in a subsequent mock case management session are listed in Annexe 1. The panel moderator on these occasions is Patrick Burke, Senior Director and Assistant General Counsel at Guidance Software. Chris Dale's role on the panel is to explain the value of this meeting of trans-Atlantic minds.

The developments fall under two broad headings, procedural matters and cases. Lord Justice Jackson's Report on Civil Litigation Costs, and the proposed Practice Direction and ESI Questionnaire are prospective procedural developments whose influence is already significant notwithstanding that none of them has yet passed into the rules. By UK standards, we have had a good number of important cases. Their significance, separately and together, outweighs their mere number - they bring significant implications for all those who practice litigation as lawyers or who manage it as judges.

2.2 US-UK commonality

The most important themes in the UK are the following:

- Education as to the rules and practice
- The need to understand the technology
- The duty of cooperation
- The primacy of original documents as evidence
- Preservation of evidence
- The role of the court in case management

An agenda prepared for US purposes would look very similar. There is a perception in the UK that the US experience is simultaneously irrelevant and an awful warning to UK courts and lawyers. It cannot be both irrelevant and salutary and is in fact neither. There are indeed many aspects of US e-Discovery which serve as warnings. They are, however, warnings as how to do things better, not encouragement to avoid the subject altogether. In the UK as in the US, the subject cannot be avoided anyway.

Quotations from two sources illustrate this. The first comes from Lord Justice Jackson's Final Report[1099]:

> *The first point which needs to be made about e-disclosure is that it is inevitable in cases where the parties hold the relevant material electronically. For the parties to print all the material out and then exchange it in hard copy would often be impracticable. With all but the smallest volumes of material, that course would not be cost effective. Thus in cases where edisclosure is a consideration, it is often a practical necessity rather than an optional course.* [Para 2.1 on page 365]

The same point recurs in two quotations from Earles v Barclays Bank Plc [2009] EWHC 2500 (Mercantile) (08 October 2009)[1100]:

> *Since 2000 most key contemporaneous commercial documents are contained in Electronically Stored Information ["ESI"] – today over 90% of communications are recorded in that form phone records, texts, e-mail, bank records etc. ESI are "documents" under the Civil Procedure Rules: CPR 31.4 and 31PD.2A. Accordingly, the rules for "Standard Disclosure" apply: CPR 31.6. i.e. "only" those documents that are "supportive" or "adverse" to each party's cases. The abundance of this ESI in cyberspace means that potential litigants, in particular organisations such as Banks at the current time, need to anticipate having to give disclosure of specifically relevant electronic documentation and the means of doing so efficiently and effectively. [Para 21]*

1099 http://www.judiciary.gov.uk/about_judiciary/cost-review/jan2010/final-report-140110.pdf.
1100 http://www.bailii.org/ew/cases/EWHC/Mercantile/2009/2500.html

It might be contended that CPR 31PD 2A and electronic disclosure are little known or practised outside the Admiralty and Commercial Court. If so, such myth needs to be swiftly dispelled when over 90% of business documentation is electronic in form. The Practice Direction is in the Civil Procedure Rules and those practising in civil courts are expected to know the rules and practice them; it is gross incompetence not to. [Para 71]

US practitioners and judges who read (or write) e-Discovery Opinions will recognise both the sentiments and the language here, and in particular the slightly despairing tone which comes of having to say this any of this at all – that most documents are electronic, that it is cheaper to handle electronic documents electronically, that the disclosure rules cover them and that ignorance of the rules is unacceptable. If any of this surprises UK lawyers (and it will), the discovery that US lawyers have the same difficulty will surprise them more.

3. UK PROCEDURAL MATTERS

As stated above, the sources for current thinking on the rules and procedures are the disclosure and e-Disclosure sections of Lord Justice Jackson's report on litigation costs, and a draft practice direction and ESI questionnaire. There is overlap between them both in intent and in the fact that Lord Justice Jackson endorsed the Practice Direction and expressed himself relieved of the need to make procedural recommendations because of the work which had gone into the Practice Direction.

3.1 The present UK Rules relevant to Disclosure and e-Disclosure

Before we get into recent developments, it is worth briefly summarising the present rules, both those specifically relating to disclosure and those about case management and discretion which govern electronic disclosure.

A "document" means "anything in which information of any description is recorded" (Rule 31.4). The usual order for is for "standard disclosure" which requires that a party disclose only the documents on which he relies, those which adversely affect his own or another party's case those which support another party's case (Rule 31.6). A party is required only to make a reasonable search, "reasonable" being judged by a set of factors set out in Rule 31.7 and in the Practice Direction to Part 31. Paragraph 2 of the Practice Direction, inserted in 2005, imposes obligations specific to electronic disclosure, including an obligation to discuss sources with opponents before the first case management conference, the form in which documentsare to be exchanged and the keyword or other forms of electronic search which may be used. The first two of these but, uriously, not the third, expressly provides that difficulty or disagreement must be referred to the judge at the earliest practical date, if possible at the first case management conference. The absence of such an obligation in respect of keyword searches does not prevent it being raised as an issue before the court.

It is generally assumed that standard disclosure is automatic. Whilst this may be what actually happens, the strict position is that standard disclosure follows an order to that effect made usually

at the first CMC. It is open to the parties to agree that there be no disclosure, disclosure in stages or disclosure on a basis wider than standard disclosure; any such order is subject to the court's approval.

The court has a general duty of active management (Rule 1.4) in pursuit of the overriding objective (Rule 1) and, as a general matter may, in addition to any specific powers and duties, "take any other step or make any other order for the purpose of managing the case and furthering the overriding objective".

In relation to these rules, it would be fair to say that few lawyers are aware of, still less understand, the narrowed scope of disclosure; that most case managing judges are content simply to tick a box for standard disclosure without any enquiry as to what is likely to be involved; that the scope of search point is ignored in both directions (that is, many lawyers either neglect whole bodies of documents or set about retrieving material without regard to the relationship between costs and likely value; that the whole Practice Direction is unknown to both lawyers and judges; and that the concept of "active management" is not properly understood or practised by most judges at least in respect of disclosure.

These omissions and failures set the scene for the developments described in the ensuing sections.

3.2 The draft Practice Direction and ESI Questionnaire

The invisibility of the practice direction to Part 31 CPR, and in particular the absence of both inter-party discussion and judicial management, was highlighted in 2008 by Digicel (St. Lucia) Ltd & Ors v Cable & Wireless Plc & Ors [2008] EWHC 2522 (Ch) (23 October 2008). There was no discussion between the parties before the CMC, and the judge hearing it simply made an order for standard disclosure. After disclosure, the claimants brought two applications, one as to the scope of the keywords used by the defendants to reduce their document population and one as to 800 or so backup tapes which the defendants disclosed as existing but said of them that it was disproportionate to investigate them. Both of these subjects should, of course, have been discussed pursuant to the practice direction quite apart from the general duty of cooperation imposed by the rules. The result in that case was an order that the defendants redo their searches using a set of keywords decided on by the judge and that they should begin immediate discussions as to the tapes. In the wider sense, the result of the case was a new focus on the disclosure obligations. That, it has to be said, did not attract the attention it deserved, in the sense that it remained possible a year later to ask an audience if they had heard of either the practice direction or Digicel and get almost no response, even amongst those who had self-selected as being interested in the subject. At a high judicial level, Digicel was undoubtedly one of the factors which prompted the Deputy Head of Civil Justice to ask Senior Master Whitaker to devise a questionnaire whose function was to provide a formal framework for the discussions required by Paragraph 2A.2 of the practice direction. Master Whitaker set up a working party, of which I am a member, to work on devising such a questionnaire. We were subsequently asked in addition to produce a new practice direction specifically devoted to electronic disclosure. It is important, in the light of the outcome as it stands at the moment, to flag the fact that the work on these documents was done pursuant to an express request from on high.

The best summary of what was intended by the practice direction and questionnaire is contained

in the final report of Lord Justice Jackson into litigation costs. That report is covered in the next section of this paper, but it is appropriate to set out here what the summary said[1101]:

- Parties and their legal representatives should consider, at an early stage, the use of technology in order to identify potentially relevant material, to collect, analyse and review it. Subsequently this will assist with the creation of lists of documents to be disclosed and giving disclosure by providing documents in electronic format.

- Unless a party intends to request that the action be allocated to the small claims track or the fast track, that party must exchange with the other party or parties and file with the court Answers to the ESI Questionnaire attached to the Practice Direction.

- The ESI Questionnaire requires the parties to provide information about any documents which they hold in electronic form and which are to be disclosed in the proceedings, long with details of their electronic storage systems. They are also asked to detail any issues that may arise about the accessibility of such documents. The Answers to the ESI Questionnaire must be supported by a statement of truth.

- After exchange of Answers to the ESI Questionnaire and before the first CMC, the parties must discuss the disclosure of ESI, including the scope of the reasonable search for ESI and any tools and techniques which might reduce the burden and cost of disclosure of ESI.

- If the parties encounter difficulties or cannot reach agreement, issues arising in relation to the disclosure and inspection of ESI should be referred to a judge for directions, if ossible at the first CMC.

- The extent of the reasonable search will depend upon the circumstances of the case. The parties should bear in mind the overriding principle of proportionality. Many of the factors that may be relevant in deciding the reasonableness of a search for ESI are listed in paragraph 2A.4 of the current practice direction supplementing CPRPart 31.

- Where a party is giving disclosure of ESI, a List of Documents may by agreement between the parties be an electronic file in a defined and agreed format.

- Unless the parties agree otherwise or the court directs otherwise, where electronic copies of disclosed documents are provided to another party, the electronic copies should, unless this is not reasonably practicable, be provided in their native format.

1101 Para 2.4 on page 365

Having thus recited the purpose of the practice direction and questionnaire, Lord Justice Jackson went on to say[1102]:

> In my view, the substance of this practice direction is excellent and it makes appropriate provision for e-disclosure. On the assumption that this practice direction will be approved in substantially its present form by the Rule Committee, I do not make any recommendation for procedural reform in relation to e-disclosure.
>
> To anticipate a little, the present status of those documents, after three appearances before the Civil Procedure Rule Committee, is that they have been referred to a sub-committee. It is perhaps politic, in the present context, to refrain from comment on this.

3.2 Lord Justice Jackson's Report on Litigation Costs

Disclosure and electronic disclosure are treated as separate subjects in both the preliminary report and the final report on litigation costs by Lord Justice Jackson. One is left in no doubt as to the importance which he attaches to the subject from his opening paragraph about it[1103] which is quoted above.

He made only one express recommendation as to eDisclosure, which was for education, expressed in the following terms:

I recommend that e-disclosure as a topic should form a substantial part of (a) Continuing Professional Development ("CPD") for solicitors and barristers who will have to deal with edisclosure in practice and (b) the training of judges who will have to deal with e-disclosure on the bench. Service providers will have a part to play in such CPD or training. Indeed they will have a commercial interest in contributing to the process. However, they should do so within the context of a well structured programme, which is provided or approved by the relevant professional bodies.

Lord Justice Jackson was in no doubt as to the role which technology must play in the handling of electronic documents. His reiterated theme in both his reports is that it is essential to reduce document populations as early as possible by a combination of case management and the proper use of technology. He said this:

I attended an e-disclosure demonstration at 4 Pump Court chambers. Three different specialist providers each took data from the Enron case and demonstrated how their respective software systems could search, sample, categorise and organise the data. The object of each of these\ systems is (i) to whittle down as far as possible the potentially relevant documents which will be passed to the lawyers for review and (ii) to enable the lawyers to search and organise documents passed to them. I am bound to say that the systems developed by each of those specialist providers are extremely impressive. I am sure that it would assist other members of the judiciary to know what technological help is available to the parties, to enable them to manage the disclosure process.

1102 Para 2.5 on page 366

1103 Para 2.1 on page 364

Many of those who submitted observations to him during the consultation phase emphasised the vital role of the judge in managing cases. The primary purpose of case management is the management of time and costs, and Lord Justice Jackson considered carefully how best to encourage judges to play their part in this. Apart from his fairly stern references to present defects, he proposed a new Rule 31.5A, known as the "menu option" – his only other formal disclosure recommendation apart from the one about education. In addition to setting out proposed procedural matters (some of which overlap with what is proposed in the Whitaker draft practice direction) he set out expressly a range of options which judges and parties must consider, with the starting point is that none of them is the default. The options[1104] include:

a) an order dispensing with disclosure; or
b) an order that a party disclose the documents on which it relies, and at the same time requests any specific disclosure it requires from any other party; or
c) an order that (where practical) directs, on an issue by issue basis, the disclosure to be given by a party on the material issues in the case; or
d) an order that a party give standard disclosure;
e) an order that a party disclose any documents which it is reasonable to suppose may contain information which may (i) enable the party applying for disclosure either to advance his own case or to damage that of the party giving disclosure, or (ii) lead to a train of enquiry which has either of those consequences; or
f) any other order in relation to disclosure that, having regard to the overriding objective, the court considers appropriate.

Some specific powers are then recited, with the concluding recital that:

> In exercising its discretion …. the court will consider what disclosure would be proportionate to the circumstances of the case."

It would be right to observe that any one of these orders could be made under the rules as they stand, having regard to what is said above about the existing scope of discretion. Lord Justice Jackson made it clear that his primary purpose here is to force a proper appraisal of cost against value to meet a test which, under the present rules, is one of proportionality. I emphasise the reference to the present rules, because another part of Lord Justice Jackson's report examines, in learned but lucid style, whether the proportionality test is the right one to apply. The alternative test is one of "necessity" with the suggestion that the costs recoverable between parties should turn on whether the work done and claimed for was really necessary for justice to be achieved. Although this is not narrowly a disclosure point, the potential impact of such a change on, for example, the scope of the search is significant.

Given the express commendation of the practice and questionnaire referred to in the preceding section, it may appear to some that the Rule Committee's reluctance to adopt them is something of a

1104 Para 3.11(6) on page 371

rebuff to Lord Justice Jackson. After all, the obvious implication from what he said is that he would have made recommendations about procedure if the draft practice direction did not already provided adequate recommendations. If the Rule Committee proves too timid to implement the practice direction, then its fall-back is to make its provisions and the use of the questionnaire merely matters of best practice. Given that the existing practice direction provisions have been ignored for over five years, this would scarcely be an adequate way of changing the culture. Whatever the outcome of the deliberations of the Rule Committee's subcommittee, it is already clear that the Lord Justice Jackson's long awaited report is having influence in relation to e- Disclosure. Until its provisions are adopted, it remains of persuasive value only, but when you have regard to the fact that so much of it is designed primarily to emphasise existing obligations, its effect must be considerable. That is reinforced by a number of cases which point in the same direction.

4. UK eDisclosure Cases

There are two cases from earlier years whose influence persists:

Nichia Corp v Argos Ltd[1105] [2007] EWCA Civ 741 (19 July 2007)

The principles described by Lord Justice Jacob in paragraphs 46 to 54 of Nichia have been created in subsequent cases. Some quotations will suffice to give the flavour of it

> It is wrong just to disclose a mass of background documents which do not really take the case one way or another. And there is a real vice in doing so: it compels the mass reading by the lawyers on the other side, and is followed usually by the importation of the documents into the whole case thereafter – hence trial bundles most of which are never looked at. For it is the downstream costs caused by overdisclosure which so often are so substantial and so pointless. It can even be said, in cases of massive overdisclosure, that there is a real risk that the really important documents will get overlooked – where does a wise man hide a leaf?

"Perfect justice" in one sense involves a tribunal examining every conceivable aspect of a dispute. All relevant witness and all relevant documents need to be considered. And each party must be given a full opportunity of considering everything and challenging anything it wishes. No stone, however small, should remain unturned.

But a system which sought such "perfect justice" in every case would actually defeat justice. The cost and time involved would make it impossible to decide all but the most vastly funded cases. The cost of nearly every case would be greater than what it is about. Life is too short to investigate everything in that way.

1105 *http://www.bailii.org/ew/cases/EWCA/Civ/2007/741.html*

Subsequent cases have involved more specific reliance on particular rules, but the paragraphs in Nichia from which these extracts come remain the best summary of the principles.

Digicel (St Lucia) v Cable & Wireless[1106] [2008] EWHC 2522 (Ch) (23 October 2008)

The importance of Digicel has been described above. It is important not just for its conclusion, but for the workmanlike summary of what the practice direction are the one says and means and, almost incidentally, for its recital of the steps taken by each party which are illuminating for those with no understanding of what is involved in handling large volumes of documents. The importance of the practice direction is described in paragraph 47 in these terms:

This case provides an opportunity for the Court to emphasise something mentioned in Part 31 Practice Direction which the parties in the present case disregarded. Paragraph 2A.2 of the Practice Direction states that the parties should at an early stage in the litigation discuss issues that may arise regarding searches for electronic documents. Paragraph 2A.5 of the PD states that where key word searches are used they should be agreed as far as possible between the parties. Neither side paid attention to this advice. In this application the focus is upon the steps taken by the Defendants. They did not discuss the issues that might arise regarding searches for electronic documents and they used key word searches which they had not agreed in advance or attempted to agree in advance with the Claimants. The result is that the unilateral decisions made by the Defendants' solicitors are now under challenge and need to be scrutinised by the Court. If the Court takes the view that the Defendants' solicitors' key word searches were inadequate when they were first carried out and that a wider search should have been carried out, the Defendants' solicitors' unilateral action has exposed the Defendants to the risk that the Court may require the exercise of searching to be done a second time, with the verall cost of two searches being significantly higher than the cost of a wider search carried out on the first occasion.

Is the judge also gave a reminder of why proper searches for electronic documents is important as a matter of evidence. He said in paragraph 46:

> it must be remembered that what is generally required by an order for standard disclosure is "a reasonable search" for relevant documents. Thus, the rules do not require that no stone should be left unturned. This may mean that a relevant document, even "a smoking gun" is not found. This attitude is justified by considerations of proportionality. This point is well made by Jacob LJ in Nichia Corporation v Argos Limited [2007] EWCA Civ 741 at [50] to [52].

This paragraph has particular resonance in the light of two at least of the cases which we will come on to, Earles v Barclays, which stressed the primacy of contemporaneous documents and the Ofsted

1106 *http://www.bailii.org/ew/cases/EWHC/Ch/2008/2522.html*

case where the documents produced at a late stage included prior drafts of the report on which the central issues turned.

The new cases are:

Earles v Barclays Bank Plc[1107]
[2009] EWHC 2500 (Mercantile) (08 October 2009)

Earles v Barclays, decided by His Honour Judge Simon Brown QC, is important chiefly for the criticism made by the judge of the defendants and its lawyers for the failure to disclose documents central to the issues. The claim concerned transfers between accounts of £265,000, and the central issue was whether the bank had authority to make such transfers. The judgment drew attention to the relevant rules and the lawyers' duty to know and comply with them (the relevant passage, with its reference to "gross incompetence" is quoted at the beginning of this paper) but emphasised still more the fact that time and money had actually been wasted because of the need to examine witnesses on points which would have been disposed of quickly and easily with the documents had been available.

As regards disclosure, the Bank failed to give disclosure of the Transfer Sheets referred to in paragraph 53 of the witness statement of Katharine Shelley. They were clearly relevant under the narrow test of CPR 31.6 to the primary issue in the case. The very fact that they were referred to in the carefully crafted witness statement proves that and it ought to have been obvious to the Defendants lawyers. Their absence made the task of the Court immeasurably harder to the extent that it considered lengthy submission as to whether or to draw adverse inferences against the Bank itself. I am satisfied that it was a decision of the legal team on the erroneous grounds of disproportionality[1108].

The judgment is important also for its summary of the primacy of documentary evidence in circumstances where witnesses are unlikely to be able to remember what happened. It is not realistic to expect any human beings to recall with any reliability what they said 3 years ago about run of the mill business transactions. Therefore it is crucial to follow the guidance of these very eminent jurists and in particular those emphasized regarding the analysis of contemporaneous documents; objective facts and documents; witnesses motives and overall probabilities[1109]. Lastly, the Earles judgment raised interesting points about the duty to preserve documents, an area which is less advanced in English law than in the US. Although the defendants were successful, the costs awarded to them were substantially reduced as a result of their conduct in relation to disclosure.

Goodale v The Ministry of Justice[1110]
[2009] EWHC B41 (QB) (05 November 2009)

This is a judgment of Senior Master Whitaker, and provides a copybook example of the approach which a case management judge should take where the only thing known about the document

1107 *http://www.bailii.org/ew/cases/EWHC/Mercantile/2009/2500.html*
1108 Para 68
1109 Para 21
1110 *http://www.bailii.org/ew/cases/EWHC/QB/2009/B41.html*

populations is that they are potentially very large. The Ministry approached the case management conference asserting that they did not intend to give disclosure of any electronic documents – not that they did not have any, not that they had none which were relevant, not that they had weighed the costs against the value in any real sense, but merely that they did not intend to disclose them. Since the point at issue (the government's policy in dealing with opiatedependent prisoners) necessarily involved evidence of treatment across a wide range of people and places, as well as matters of policy, it was inevitable that such an approach would be deemed unacceptable by the senior master.

The chief significance of the judgment is that the Senior Master ordered the use of the ESI questionnaire in the event that the parties needed to come back to court. The questionnaire was, as it remains, a draft under consideration by the Rule Committee, and its use is a good example of a judge taking a hands-on and pragmatic approach to helping the parties to satisfy their obligations to the court.

The judgment is important, however, beyond the fact that it was the first public appearance of the questionnaire. Two things in particular stand out - an order for a staged and iterative approach to identifying the scope of the problem before making final decisions, and the recommendation that technology be used to reduce the volumes to a manageable size.

The first of these points is illustrated by this quotation:

It seems to me that the proper way of going about this in respect of the individuals is that the limited searches that could be run on the MEDS system should be run but without the actual physical review and production of those documents in the first place. We need to know how many documents each of the 31 terms are going to turn up to establish whether any may require a degree of fine-tuning. We also need to know the total number of documents that respond to this collection of search terms (acknowledging that the same documents may respond to more than one search term in many cases). There is probably going to be some question over whether all the 31 key words are necessary, because what little bit of sampling that has been done seems to reveal, that quite a few of them produce nil returns anyway. We shall see whether that is the case in respect of Palmer, Bradshaw and Piper as well as Marteau when those searches are run[1111].

What Master Whitaker said about technology is an illustration of what Lord Justice Jackson said about the need for judges to know something of the available technology : At the moment we are just staring into open space as to what the volume of the documents produced by a search is going to be. I suspect that in the long run this crude search will not throw up more than a few hundred thousand documents. If that is the case, then this is a prime candidate for the application of software that providers now have, which can de-duplicate that material and render it down to a more sensible size and search it by computer to produce a manageable corpus for human review – which is of course the most expensive part of the exercise. Indeed, when it comes to review, I am aware of software that will effectively score each document as to its likely relevance and which will enable a prioritisation of categories within the entire document set[1112].

1111 Para 25

1112 Para 27

Vector Investments v Williams[1113]
[2009] EWHC 3601 (TCC) (05 November 2009)

This was not an e- disclosure case. It is worth mentioning briefly, however, because it provides another example of a successful party losing a proportion of the costs which would otherwise be recoverable, in this case £20,000, because of the manner in which it gave disclosure. The defects in that case involved duplication, lack of order and the inclusion of documents which were irrelevant to the issues. The application of these principles to electronic documents is obvious.

Shoesmith, R (on the application of) v OFSTED & Ors[1114]
[2009] EWHC B35 (Admin) (10 November 2009)

The Shoesmith case attracted attention because the underlying story was a matter of deep public interest. Sharon Shoesmith was Head of Children's Services at the London Borough of Haringey when a child known as Baby P died at the hands of those with whom he lived. A report was prepared by Ofsted, the regulating authority, for submission to Ed Balls, the Secretary of State for Education. Shoesmith was summarily dismissed by the Minister immediately on the publication of the report. Her application was for judicial review of the decision to dismiss her, and the report itself was obviously of critical importance, not least because of the suggestion that the "right" result was needed by Ed Balls in order to justify the dismissal.

After closing speeches but before judgment, Ofsted confessed that it had found nearly 2,000 pages of documents which should have been disclosed. When finally produced, these proved to include 17 earlier drafts of the report. Shoesmith's lawyers made much of the fact that each succeeding draft moved closer to blaming Shoesmith personally for the shortcomings of her department and the death of Baby P. The suggestion of foul play in the conduct of the dismissal procedures was reinforced by the existence of an Ofsted memo ordering staff to delete emails containing the words "Baby P" and "Haringey". That order was apparently rescinded on the day it was given, but it is not known whether anyone had acted on it in the interim and it hardly indicates the right institutional spirit where the duties to the court are concerned.

Whatever effect the disclosure defects have on the finding, the case is important as illustrating the reputational disadvantages of improper disclosure, for drawing public attention to the importance of a proper collection appropriate to the circumstances and, not least, the costs implications of a failure to comply with the rules the first time round.

1113 *http://www.bailii.org/ew/cases/EWHC/TCC/2009/3601.html*
1114 http://www.bailii.org/ew/cases/EWHC/Admin/2009/B35.html

Al-Sweady & Ors, R (on the application of) v Secretary of State for Defence [2009] EWHC 2387 (Admin) (02 October 2009)

This judgment of the Court of Appeal should also bring home to lawyers the downside of getting it wrong. The case involved matters of public interest - the evidential point was as to whether a particular Iraqi died on the battlefield or in British custody - and concerned multiple defects in the disclosure given by the Treasury Solicitor on behalf the Ministry of Defence. These are not set out in what is a short judgment, but the key points for those responsible for disclosure include: the extreme importance of documents in judicial review cases where the respondent almost inevitably holds the documents which matter; the consequences in terms of costs (an interim order for payment of £1 million calculated on an indemnity basis was made); and the reputational issues - the Treasury Solicitor himself was "invited", along with the Provost Marshal of the Royal Military Police, to appear before the court to explain the disclosure defects, and a senior officer was described in terms which are likely to further his career, namely: if Colonel Giles continues to be put forward as a principal or even a significant witness in judicial review proceedings or if he is in any way responsible for disclosure, it is our view that any Court seized of those proceedings should approach his evidence with the greatest caution[1115]

The key part of this judgment for the purpose of this paper's themes lies in a passage about a curious volte face made by the Treasury Solicitor. It had been said consistently on behalf of the Department that no further documents existed under a particular head. The judgment describes what happened next[1116]:

Much to our surprise in the light of the Secretary of State's previous stance, it was then asserted for the first time that:

> *"the sheer volume of the material… together with the technical difficulties in framing meaningful search parameters, means that it would be impractical and disproportionate to conduct broad based searches of the exchange servers themselves, and that to do so would be disproportionate".*

No reason has been put forward to explain why this response had not been made at any time since the original request which had been made more than eight months earlier on 16 October 2008. We conclude that the Secretary of State's agents had simply failed for no good reason during that lengthy period to carry out these critically important and obviously highly relevant searches and this failure in our view constitutes a serious breach of their duty to give proper disclosure. It must not be forgotten that Salmon J explained in Woods v Martins Bank [1959] 1 QB 55 at page 60 that "it cannot be too clearly understood that solicitors owe a duty to the court, as officers of the court, to go through the documents disclosed by their client to make sure, as far as possible, that no relevant documents have

1115 Para 60
1116 Para 41

been omitted from their client's [list]". This duty requires a solicitor to take steps to ensure that their client knows what documents have to be disclosed.

If one needed confirmation that a more rigorous approach is needed to the early stages of electronic disclosure, including a questionnaire signed by the solicitor or his client, a case in which a party can veer from claiming that it holds no documents to being apparently overwhelmed by their volume certainly provides it.

4.1 Summary as to the UK cases

In a sense, the cases alone need no procedural reforms to back them. Between them, they cover every aspect of electronic disclosure - compliance with the rules, the importance of contemporaneous documents, the need for active case management, the duty to preserve documents, the obligations of transparency and co-operation, the need to use technology and the costs and reputational issues of getting it wrong.

None of these cases refer expressly to Lord Justice Jackson's report nor, save for Goodale, to the proposed new practice direction and questionnaire. They were all decided on the rules as they stand. Lawyers have been slow to grasp the implication of the cases (if they know of them at all) whereas the Jackson report and the practice direction have attracted much attention. The difficulty, perhaps, is that the cases all appear to relate to circumstances beyond the everyday experience of lawyers conducting conventional commercial litigation - cases involving banks, ministers and wars are not seen as directly relevant to the daily grind.

Whether this conclusion by the lawyers is a conscious one or, as is more likely, a subconscious closing of minds, it is a mistake to think that these cases have application only in extreme circumstances. They are all founded in a set of rules which are neither extensive nor difficult to understand. Whether the dominant theme is competence, proportionality or both, the principles apply to everyone in every case.

The Court of Appeal, in a 2007 case called Hedrich & Anor v Standard Bank London Ltd & Anor [2008] EWCA Civ 905 (30 July 2008)[1117], appeared to suggest that a lower standard of competence might be expected of High Street solicitors. This cannot be right, at least at the level of non-compliance with the rules. It is equally wrong to approach e-disclosure as if it applied only in certain courts or to certain types or size of case. The level of skill and competence required is that lawyers must know enough to recognise what is required in any case. The concept of proportionality requires that an assessment is made, on the one hand of he value of any documents and, on the other, of the cost of extracting them. There are, as Judge Brown noted in Earles, as Master Whitaker observed in Goodale and as Lord Justice Jackson noted in his Report, suppliers of technology solutions whose advice can be sought and whose solutions are available to supplement the legal input of the lawyers.

It is often asserted that US discovery has nothing to teach the UK about the proper approach to handling large volumes of documents. There are indeed differences in the rules, the scale and number of the cases, and the approaches taken by the court. There are, however, many similarities including (which comes as a surprise to many in the UK) an almost wilful failure by many US lawyers to

1117 *http://www.bailii.org/ew/cases/EWCA/Civ/2008/905.html*

understand even the most basic principles of the expectations of the rules nd the courts. Although some of the UK cases summarised above show failures of competence which would be punishable in any jurisdiction, some of them show a hardening judicial line in a way which is familiar to any student of US discovery cases. It is to that which we turn in the next section of this paper.

5. SUMMARY OF RECENT DEVELOPMENTS IN US eDISCOVERY LAW

This summary will focus on:

- The May 10-11, 2010 conference on potential amendments to the US Federal Rules of Civil Procedure featuring panels of US judges, practitioners and academics, held at Duke Law School in Durham, North Carolina; and
- A summary of two of the most significant recent US eDiscovery decisions of potential interest to UK judges and practitioners.

5.1 The Duke Conference

The singular event in US eDiscovery in 2010 to date was a conference held May 10 and 11 at Duke Law School, Durham, NC entitled "2010 Conference on Civil Litigation." Organized by the Standing Committee on Civil Rules, at the request of the Standing Committee on Rules and Procedure, which oversees amendments to the US Federal Rules of Civil Procedure ("FRCP"), its purpose is to explore the current costs of civil litigation, particularly discovery, and to discuss possible solutions.

The conference marks the beginning of a process to consider amending the FRCP – a process that will take years. It came as the federal courts are assessing the degree of satisfaction with the performance of the present system, and considered new empirical research done by the Federal Judicial Center and other data and papers prepared by various bar associations and others. eDiscovery was a central topic of the conference. Other topics to be considered include judicial management and the tools available to judges to expedite the process, the process of ettlement, and the experience of the states. It sought to solicit suggestions of lawyers, judges and academics as to how the system can be improved. A major portion of the Conference was devoted to an assessment and discussion of the empirical research.

Two of the US judges participating in the IQPC London conference – US Magistrate Judges Grimm and Facciola – were also key participants in the Duke conference. Judge Grimm was a presenter in the session on "Issues with the Current State of Discovery: Is There Really Excessive Discovery, and if so, What are the Possible Solutions?" He submitted a paper in advance of the conference entitled "The State of Discovery Practice in Civil Cases: Must the Rules be Changed to Reduce Costs and Burdens, or can Significant Improvements be Achieved Within the Existing Rules?" While some members of the defence bar argued that only rule changes can end the expense and alleged abuse of eDiscovery in US federal courts, Judge Grimm argued that the tools already exist the ensure that eDiscovery is cost-effective and proportional to what is at issue in the litigation, and affords both sides fair discovery

to ensure that essential facts needed to adjudicate or resolve the case. He urged that the real change required is in the inappropriate attitudes and behaviours that have stymied such efforts.

Judge Grimm's paper noted that a recent survey by the American Bar Association Section of Litigation reported that "25% of the lawyers who responded believed that the Rules 'should be reviewed in their entirety and rewritten to address today's needs.' More than 38% of the respondents believed that 'one set of rules cannot accommodate every type of case.'" He opined that:

While all of these studies increase awareness of deficiencies in the civil litigation system, it does not follow that a new round of comprehensive changes is the best or quickest way to achieve desired change. The old saying "[t]hose who cannot remember the past are condemned to repeat it" comes to mind regarding today's criticisms of the state of discovery practice in civil cases. One need only read the Advisory Committee Notes for Rules change decades ago to see that the same criticisms were raised then. While it is possible to envision some changes to the Rules of Civil Procedure, it is worth asking whether that is the best route to improvement, or whether the real problem is the failure to adhere to the Rules in their current form. In fact, the existing Rules provide all of the necessary tools to achieve the changes in practice that have eluded us for decades. Without behavioral change in the key participants in the civil justice system, however, even sweeping modifications to the Rules will not foster achievement of the desired goal. We might wish first to change the Rulers (judges) and the Ruled (lawyers) before reverting to yet another effort to change the Rules.

After all, there are three players in this drama whose actions cause the litigation system to succeed or fail: the parties themselves, the lawyers who represent them, and the judges who preside over their cases. Each is responsible for the status quo, and each must change if the system's shortcomings are to be improved. While it may be true that ours is a litigious society, in our litigation system the parties have choices, each of which bears a price tag. Moreover, where, as in the United States, the general rule is that each side bears the cost for its own litigation expenses (including counsel fees), absent any cost shifting statute, contractual agreement, or egregious conduct of an adversary that warrants shifting the costs as a sanction, the parties have the power to increase or decrease the cost of litigation.

Rather than amend the FRCP, Judge Grimm urges federal courts to:

Encourage judges to develop a discovery budget, and involve the parties in the process;

- Adopt local rules or guidelines that stress the need for cooperation in the discovery process as an expectation of the court, and the willingness of the court to resolve discovery disputes promptly when they occur; and
- Be cognizant that seasoned practitioners have developed common-sense systems that can be adapted and adopted by courts for wider use.

US Magistrate Judge Facciola participated in a panel titled "Discussion of the Cost Benefit Analysis of eDiscovery, and the Degree to Which the New Rules are Working or Not." The panel – which in addition to Judge Facciola consisted of US District Court Judge Shira Scheindlin and a number of nationally prominent practitioners, endorsed a proposed new preservation rule for consideration, as to which there was: [A] consensus view that a rule addressing preservation (spoliation) would be a

valuable addition to the Federal Rules of Civil Procedure. All members of the Panel agree that such a rule should apply once an action has been commenced. (Panel members disagree as to whether such a rule can or should apply, along the lines of Rule 27, prior to the commencement of an action.) The Panel members also agree that the rules in general, and a preservation rule in particular, should treat differently huge cases, with enormous discovery, and all others.

The Duke conference organizers emphasized that an important part of the Conference is to encourage follow up on the subjects explored. It is hoped that the papers and discussion at the Conference will frame an agenda for possible amendments to the Federal Rules of Civil Procedure, and that they will be a basis for judicial education through the Federal Judicial Center and for further action by the Bar. Full information on the Duke conference, including the full roster of presenters and the papers submitted for consideration, can be found at: http://civilconference.uscourts.gov/LotusQuickr/dcc/Main.nsf/h_RoomHome/4df38292d748069d 0525670800167212/?OpenDocument.

5.2 Recent US eDiscovery Decisions

US eDiscovery case law has been dominated this year by contrasting decisions from two heavyweights of eDiscovery addressing the duty to preserve and the availability of sanctions for discovery misconduct leading to spoliation. The decisions highlight a split between the Federal Judicial Circuits regarding the level of culpability required for a finding of sanctionable spoliation and set the stage for further discussion regarding the propriety of imposing an adverse inference instruction in the absence of proof regarding the relevance of lost data.

The Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010)

In an amended order subheaded "*Zubulake* Revisited: Six Years Later" Judge Shira A. Scheindlin, author of the seminal *Zubulake* opinions, articulates something like a strict liability standard for spoliation and sets a high bar for the conduct expected of litigants and counsel engaged in discovery.

The underlying facts played out while the *Zubulake* opinions were being issued. Plaintiffs, sophisticated investors who sought to recover $550 million from liquidated offshore hedge funds, collectively retained lead counsel who asked them to provide records (including emails and electronic documents) to assist with preparing the complaint. Counsel did not issue a formal written hold or instructions to retain all relevant information, and investors were left unsupervised to find responsive records. When discovery went forward after a three-year stay, a group of defendants uncovered substantial gaps in certain investors' productions. With court ordered discovery regarding the investors' preservation, collection and production efforts, defendants identified over 300 emails missing from the productions of thirteen investors and moved against them for dismissal, alleging that they failed to preserve and produce records and then submitted false and misleading declarations concerning their discovery efforts.

Noting that this was not a case of purposeful destruction, Judge Scheindlin analyzed whether the conduct that led to the loss of records – specifically, failure to instigate timely, written litigation holds and "careless and indifferent collection efforts after the duty to preserve arose" – merited sanctions. This analysis involves four concepts: the level of culpability; the interplay etween the duty to preserve and the spoliation of evidence; who should bear the burden of proving that the conduct led to the loss of evidence; and the appropriate remedy.

Judge Scheindlin noted that negligence, gross negligence and willfulness form a continuum: "Conduct is either acceptable or unacceptable. Once it is unacceptable the only question is how bad is the conduct." Although the assessment is subjective, the standard of acceptable discovery conduct has emerged from years of judicial determinations; failure to meet these standards "may be negligent even if it results from a pure heart and an empty hand."

A chronological tour through the phases of discovery begins with the duty to preserve relevant information once litigation is reasonably anticipated: "A failure to preserve evidence resulting in the loss or destruction of relevant information is surely negligent, and depending on the circumstances, may be grossly negligent or willful."

In the collection and review phases, "depending on the extent of the failure to collect evidence, or the sloppiness of the review, the resulting loss or destruction of evidence is surely negligent, and, depending on the circumstances may be grossly negligent or willful." Noting that each assessment is fact-bound and that the variety of efforts and failures is infinite, Scheindlin provides a non-exhaustive list of examples:

> [T]he failure to collect records – either paper or electronic – from key players constitutes gross negligence or willfulness as does the destruction of email or certain backup tapes after the duty to preserve has attached. By contrast, the failure to obtain records from *all* employees (some of whom may have had only a passing encounter with the issues in the litigation), as opposed to key players, likely constitutes negligence as opposed to a higher degree of culpability. Similarly, the failure to take all appropriate measure to preserve ESI likely falls in the negligence category.

On the interplay between the duty to preserve and spoliation, Scheindlin reiterates that the duty arises when a party reasonably anticipates litigation and that case law makes it "crystal clear" that breaching this duty may be sanctionable. Because plaintiffs largely control the timing of litigation, their duty is usually triggered before litigation commences.

The burden of proving the loss of evidence and its consequences differs depending on the severity of the sanction. From least to most harsh, sanctions include: "further discovery, cost shifting, fines, special jury instructions, preclusion, and the entry of default judgment or dismissal (terminating sanctions)." For less severe sanctions "the inquiry focuses more on the conduct of the spoliating party than on whether documents were lost, and if so, whether those documents were relevant and resulted in prejudice to the innocent party." For more severe sanctions the court considers the spoliating party's

conduct, whether the lost evidence was relevant and whether the innocent party suffered prejudice as a result of the loss.

An innocent party must prove that the spoliator "(1) had control over the evidence and an obligation to preserve it at the time of destruction or loss; (2) acted with a culpable state of mind upon destroying or losing the evidence; and that (3) the missing evidence is relevant to the innocent party's claim or defense." To ensure that the burden is appropriate: "When the spoliating party's conduct is sufficiently egregious to justify a court's *imposition* of a presumption of relevance and prejudice, or when the spoliating party's conduct warrants *permitting* the jury to make such a presumption, the burden then shifts to the spoliating party to rebut that presumption." Jury instructions vary in degree: "the more egregious the conduct, the more harsh the instruction." Where a spoliating party acted willfully or in bad faith, "a jury can be instructed that certain facts are deemed admitted and must be accepted as true." For willful or reckless conduct, the court may impose a mandatory but rebuttable presumption.

Once spoliation is established, the court determines what if any sanction is appropriate, imposing the least harsh sanction that acts as a deterrent, places the risk of an erroneous judgment on the party that wrongfully created the risk, and restores the prejudiced party to the position it would have been in absent the wrongful destruction of evidence.

Applying this analysis to the investors' discovery efforts, the court found that their duty to preserve arose months before they retained lead counsel and clearly encompassed electronic records. Counsel's instructions did not meet the standard for a litigation hold because did not direct recipients "to preserve all relevant records – both paper and electronic" nor was there "a mechanism for *collecting* the preserved records" for searching and monitoring by someone other than the employee.

The burden then fell to the defendants to show that documents were destroyed after the duty to preserve arose. In addition to identifying specific documents missing from productions, defendants asked the court to assume that investors received and generated additional documents that should be presumed missing. The court rejected the investors' argument that this was "absurd" and required "rank speculation; the paucity of some productions and the "admitted failure to preserve some records or search at all for others . . . leads inexorably to the conclusion that relevant records have been lost or destroyed."

Without evidence of egregious conduct such as perjury or intentional destruction (for example, "burning, shredding, or wiping out computer hard drives"), the court declined to grant dismissal The court found that some investors were grossly negligent and others negligent. For those who were grossly negligent, because the defendants sufficiently proved failure to produce and resulting prejudice, "a jury will be permitted to presume, if it so chooses, both the relevance of the missing documents and resulting prejudice", subject to the investors' rebuttal. Monetary sanctions were imposed on all investors to compensate defendants for costs associated with their motion.

Judge Scheindlin concluded with three notes. First, the judgment call of whether to award sanctions is inherently subjective. "A court has a 'gut reaction' based on years of experience as to whether a litigant has complied with its discovery obligations and how hard it worked to comply." Second, these inquiries are inherently fact intensive and must be reviewed case by case. Nevertheless, Scheindlin offers the following guidance:

After a discovery duty is well established, the failure to adhere to contemporary standards can be considered gross negligence. Thus, after the final relevant *Zubulake* opinion in July, 2004, the following failures support a finding of gross negligence, when the duty to preserve has attached: to issue a written litigation hold, to identify the key players and to ensure that their electronic and paper records are preserved, to cease the deletion of email or to preserve the records of former employees that are in a party's possession, custody, or control, and to preserve backup tapes when they are the sole source of relevant information or relate to key players.

And third, because of the increasing risk that litigants will seek sanctions, courts should give "most careful consideration" before finding that a party has violated its discovery duties. Parties should "anticipate and undertake document preservation with the most serious and thorough care, if for no other reason than to avoid the detour of sanctions."

Rimkus Consulting Group, Inc. v. Cammerata Civil Action No. H-07-0405. (S.D. Tex. Feb. 19, 2010)

A month later, Judge Lee Rosenthal, current Chair of the Federal Rules Advisory Committee's Committee on Rules of Practice, also reviewed the standards for sanctions in cases of spoliation. Analyzing the *Pension Committee* decision, Judge Rosenthal identified important differences between the circuits.

The Rimkus case concerned several forensic engineers who left Rimkus to set up their own business, then sought to nullify their noncompete agreements. Rimkus filed suit, alleging breach of employment agreements and misuse of Rimkus's trade secrets and proprietary information.

Rimkus sought sanctions for spoliation, alleging that the former employees intentionally deleted emails and attachments while under a duty to preserve. The court agreed that there was a duty to preserve the materials but found conflicting evidence on the issue of intent.

Judge Rosenthal opened with a discussion *Pension Committee* sanctions framework. Unlike *Pension Committee, Rimkus* involved intentional rather than merely negligent spoliation. Judge Rosenthal identified key differences between Judge Scheindlin's circuit, the Second Circuit, and the Fifth Circuit. In the Fifth Circuit, unlike in the Second Circuit, simple negligence does not warrant the imposition of an adverse inference. Rather, the court must find evidence of bad faith. Further, the Fifth Circuit has not addressed "whether even bad-faith destruction of evidence allows a court to presume that the destroyed evidence was relevant or its loss prejudicial." Instead, precedent suggests that it is necessary to show relevance. Judge Rosenthal also noted that in her view, the US Supreme Court's *Chambers v. NASCO, Inc.,*[1118] decision may "require a degree of culpability greater than negligence" for a court to grant an adverse inference instruction based upon a court's inherent power.

Determining whether and what sanctions to impose "requires a court to consider both the spoliating party's culpability and the level of prejudice to the party seeking discovery." There is a continuum of culpability—from intentional conduct intended to make evidence unavailable in itigation to the negligent loss of information—as well as a continuum of prejudice—from the loss of

1118 *Chambers v. NASCO, Inc.,* 501 U.S. 32, 43–46 (1991).

a claim or a defense due to lost evidence to little or no impact when other evidence is available. These two sliding scales should be measured in tandem:

A court's response to the loss of evidence depends on both the degree of culpability and the extent of prejudice. Even if there is intentional destruction of potentially relevant evidence, if there is no prejudice to the opposing party, that influences the sanctions consequence. And even if there is an inadvertent loss of evidence but severe prejudice to the opposing party, that too will influence the appropriate response, recognizing that sanctions (as opposed to other remedial steps) require some degree of culpability.

The analysis is intensely fact driven. A high level of culpability with a low level of prejudice may not warrant a severe sanction, while a high degree of prejudice with a low level culpability may. Judge Rosenthal cited *Zubulake IV*[1119] regarding the elements of proof that a party seeking an adverse inference instruction must demonstrate: (1) [T]he party with control over the evidence had an obligation to preserve it at the time it was destroyed; (2) the evidence was destroyed with a culpable state of mind; and (3) the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

Judge Rosenthal concluded that presumptions of relevance or prejudice or culpability were not warranted her and determined that it was within the jury's purview to determine the level of culpability to be inferred and, if misconduct was found, whether or not to infer that the lost information would have been unfavorable to the defendants.

Going forward, the uncertainty surrounding the duty to preserve will be exacerbated by the different emerging standards for sanctions, the availability and severity of will likely turn on a fact-specific balancing of the level of culpability and the degree of prejudice, balanced differently depending on the Circuit in which in the case is litigated.

1119 *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 220 (S.D.N.Y. 2003).

Article Index

Backhouse, Denise. *Master European Data Privacy Law.* Fall 2010..... 349

Backhouse, Denise, Patrick Burke and Chris Dale. *eDisclosure after Jackson: Developments in Electronic Disclosure in England & Wales (With an Update on US eDiscovery Law).* 2010. 472

Backhouse, Denise, Patrick Burke and Morgan Lewis. *Seeking a Balance in the Discovery Equation: Pre-trial Disclosure/ Discovery in UK and US Civil Litigation of European-Based Data.* 2009. 459

Barsocchini, Albert. *eDiscovery and the Cloud: Judges Pushing Companies to Insource eDiscovery.* 2010. 378

Barsocchini, Albert. *It's Time to Bridge the Gap between eDiscovery, Internal Investigations, Audit and Compliance.* Winter 2010..... 383

Barsocchini, Albert. *The Keyword vs. Concept Search Debate.* 2009.....370

Barsocchini, Albert. *Voice of the Corporation: The 30(b)(6) Witness.* Spring 2009.....355

Blumenschein, John. *Victor Stanley II: New Landmark E-Discovery Sanction Decision.* Fall 2010. 353

Burke, Patrick. *Bringing eDiscovery Processing In-House.* 2009. 367

Burke, Patrick. *CISO Profiles Rise as their Reach Extends into Legal.* London City Security..... 320

Burke, Patrick. *Data Protection: Duty to Disclose.* July 7, 2010. 278

Burke, Patrick. *eDiscovery Spoliation Sanction Milestone: Monetary Sanction Imposed on an In-House Counsel.* 2010.37

Burke, Patrick. *EU Data Protection versus U.S. eDiscovery.* Fall 2009.....337

Burke, Patrick. *New Decision Holds Attorneys to Reasonable Inquires.* 2009.....371

Burke, Patrick, Patrick E. Zeller. *Legal Issues Raised by the Collection of Electronically Stored Information in Russia and China.* Summer 2010. 267

Burke, Patrick. *Standoff between EU Data Protection and U.S. eDiscovery Requires Difficult Compromises for Both Sides.* Fall 2009. 335

Carlson, Scott and Patrick E. Zeller. *E-Discovery and Trade Secrets Law: Limitations on Discovery.* 2010. 312

Dale, Chris. *Recent eDiscovery Developments in Australia and the U.K.* Spring 2009. 359

Dale, Chris. *The Place for EnCase® eDiscovery in Electronic Disclosure for Major Corporations in UK Courts.* 2009....417

Dale, Chris. *UK e-Disclosure Turning Point: The Corporate Focus on Cost-Effective Collection and Processing of E-Mail and Electronic Documents for Litigation and Regulatory Purposes.* 2009..... 397

Guidance Software. *At Liberty Mutual, E-Discovery is a Team Effort.* 2010. 347

Guidance Software. Interview. *Judge Andrew Peck on Keywords, Privacy and What Sherlock Holmes Teaches about eDiscovery.* Winter 2010. 385

Guidance Software. Interview. *Seyfarth Shaw's Scott Carlson Provides Insight into How Clients are Handling eDiscovery.* 2009. 362

Guidance Software. *Judge Simon Brown Discusses Growing Impact of Electronic Disclosure in the U.K.* 2009. 340

Guidance Software. *Recent Court Ruling Underscores Importance of File Metadata Preservation.* 2009. 366

Guidance Software. *What's New in EnCase eDiscovery Version 5*.* 2013. 414

Jaar, Dominic, and Patrick Zeller. *Canadian Privacy Law: The Personal Information Protection and Electronic Documents Act (PIPEDA).* *286*

Jaar, Dominic. *A Primer on International eDiscovery in Canada*. 2010. 299

Jaar, Dominic. *Is Preservation an Obligation?* *309*

Lim, Daniel. *Best Practices for Public Sector eDiscovery Collection.* 2008 387

Lim, Daniel. *Judge Scheindlin States Litigants, Including the Government, Must Demonstrate Ability to Search and Assess ESI.* Fall 2009. 342

Lim, Daniel. *Legal Must Stay Actively Involved in Selecting eDiscovery Solutions*. Spring 2009. 361

McManamy, Chad. *The E-Discovery Toolbox: What You Should Look for in a Unified E-Discovery Solution.* 2010. 344

Miller, Matthew. *Understanding Legal Hold Technology: Email Archiving for eDiscovery.* 2009. 364

Oot, Patrick and John J. Rosenthal. *Protecting Privilege with FRE 502.* 2010. 380

Oot, Patrick. *Verizon Continues its Goal of Using Technology to Become Self-Reliant in the eDiscovery Process.* 2009. 373

Rhoden, Michael. *Selecting the Right eDiscovery Solution: Preserve in Place vs. Collect to Preserve.* 2009. 375

Zeller, Patrick. *Reduce Your Risk of E-Discovery Sanctions by 80 Percent.* Fall 2010. 351

Case Index

AccessData Corp. v. Alste Tech. GMBH....261
Acorn v. County of Nassau....171
ADD Beard Research, Inc. v. Kates....220
ADD Ex parte Cooper Tire & Rubber Co....220
AdvantaCare Health Partners, L.P. v. Access IV....161
Aguilar v. Immigrations and Customs Enforcement Div. of the US Dep't of Homeland Sec....158
Airtrans, Inc. v. Mead....123
Al-Sweady & Ors, R (on the application of) v. Secretary of State for Defence....257
Ameriwood Industries, Inc. v. Liberman....193, 393
Am. Nat'l Prop. & Cas. Co. v. Campbell Ins., Inc....165
Antioch Co. v. Scrapbook Borders, Inc....155
Apple, Inc. v. Samsung Elecs. Co. Ltd....167, 174
Armstrong v. Executive Office of the President....49
Autotech Techs, Ltd. P'ship v. AutomationDirect.com, Inc....187
Baker Hughes Inc. v. Homa....157, 187
Balboa Threadworks, Inc. v. Stucky....192
Barnes v. CUS Nashville....211
Barrow v. Miner....219
Bd. of Regents of the Univ. of Nebraska v. BASF Corp....151
Beck v. Test Masters Educ. Servs., Inc....146
Bellinger v. Astrue....208
Blakey v. Continental Airlines....225
Bohach v. City of Reno....223, 224
Bone v. State....5
Bray & Gillespie Mgmt., LLC v. Lexington Ins. Co....143
Broccoli v. Echostar Communications Corp....164
Broderick v. State....49
Brown v. Aud....89
Burleson v. State....23, 24, 26
Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc....178, 329
Cannata v. Wyndham Worldwide Corp....176
Cartel Asset Management v. Ocwen Financial Corp....159
Carter v. State (Texas)....83
Chin v. Port Authority of New York & New Jersey....172, 176
Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc....27, 153
Columbia Pictures v. Bunnell....160
Commonwealth v. Piasecki....32
Community Bank vs. Progressive Casualty Insurance Company....204
Covad Comm. Co. v. Revonet, Inc....158
Crispin v. Audigier....211

Crown Castle USA, Inc. v. Fred A. Nudd Corp. 173
Da Silva Moore v. Publicis Group 200, 201
Daubert v. Merrell Dow 17, 21, 29
Davis v. Gracey 107
Diepenhorst v. City of Battle Creek 192, 323, 393
Digicel (St. Lucia) Ltd & Ors v. Cable & Wireless Plc & Ors 249
Doe v. Norwalk Community College 136
D'Onofrio v. Sfx Sports Group, Inc. 187
Eagle Investment Systems Corporation v. Tamm 224
Earles v. Barclays Bank Plc 254
EEOC v. JP Morgan Chase Bank, N.A. 146
EEOC v. Simply Storage Mgmt., LLC 210
EEOC v. Ventura Corp. Ltd. 146
E.I. Du Pont De Nemours & Co. v. Kolon Indus., Inc. 166
Electrolux Home Prods., Inc. v. Whitesell Corp. 153
Enquip Tech. Group, Inc. v. Tycon Technoglass 262
Eon-Net LP v. Flagstar Bancorp 174
Equity Analytics, LLC v. Lundin 194
Eurand, Inc. v. Mylan Pharmaceuticals, Inc. 193
Flagg Bros., Inc. v. Brooks 221
Flagg v. City of Detroit 213, 378
Flexsys Americas LP v. Kumho Tire U.S.A., Inc. 191, 392
Fraser v. Nationwide Mutual Insurance Co. 224
Frasier v. State 115
Fridell v. State (Texas) 86
Frye v. United States 17, 74
Furmanite America, Inc. v. T.D. Williamson, Inc. 31
Gabriel Technologies v. Qualcomm 203
Galaxy Computer Services, Inc. v. Baker 30
Gates Rubber co. v. Bando Chem. Indus 5
Global Aerospace Inc. v. Landow Aviation, L.P 201
Goodale v. The Ministry of Justice 255
Goodman v. Praxair Services, Inc. 175, 408
Google Inc. v. Am. Blind & Wallpaper Factory Inc. 324
Grant v. Marchall (Australia) 62
Grant v. Marshall 93
Green v. Beer 203
Green v. Blitz 144
Green v. McClendon 140, 352
Griffin v. State 211
Haraburda v. Arcelor Mittal USA, Inc 174
Harkabi v. Sandisk Corp. 138
Harry Weiss, Inc. v. Moskowitz 184
Hernandez v. Hillsides, Inc. 226
Hernandez v State 63
Holmes v. Petrovich Dev. Co., LLC 206
Indep. Mktg. Group, Inc. v. Keen 184
In re Air Cargo Shipping Services Antitrust Litig 261

In re A&M Fla. Props. II, LLC 142
In re Biomet M2a Magnum Hip Implant Products Liability Litigation 201
In re Fontainebleau Las Vegas Contract Litig. 206
In re Hawaiian Airlines, Inc. 178, 329
In re Honeywell Int'l, Inc. 135
In re Krause 136
In re NTL, Inc. Securities Litigation 134, 140, 329
In re Pinnacle Eng'g, Inc. 192
In re Search of: 3817 W. West End 154, 155
In re Seroquel 151
In re Verisign Inc. 135
In re Vioxx Prods. Liab. Litig. 181
In re Weekley Homes, L.P. 220
Jennings v. Orange Reg'l Med. Ctr. 177
Jones v. Bremen High School Dist. 228 175
Kay Beer Distributors, Inc. v. Energy Brands, Inc. 193
Keesoondoyal 14
Keithley v. Homestore.com, Inc. 160
Kelly v. Montgomery Lynch & Assoc. 134
Kelly v. State 22, 66
Kingsway Financial Services, Inc. v. Pricewaterhouse-Coopers, LLP 183
Kleen Products LLC v. Packaging Corp of America 201
Kronisch v. United States 170, 391
Krumwiede v. Brighton Associates 69, 185
Kucala Enterprises, Ltd. v. Auto Wax Co., Inc. 77, 78, 161
Kumho Tire Company, Ltd. v. Carmichael 23
Laughner v. State 1
Ledbetter v. Wal-Mart Stores, Inc. 212
Ler Wee Teang Anthony v. Public Prosecutor 92
Liebert Corp. v. Mazur 85
Logan v. State 27, 90
Lorraine v. Markel American Insurance Company 3
Magana v. Hyundai Motor America 220
Mailhoit v. Home Depot U.S.A., Inc. 212
Mancia v. Mayflower Textile Services Company 158
MasterCard International, Inc. v. Moulton 162
Mathew Dickey v. Steris Corporation 17
McCann v. Harleysville Insurance Company of New York 212
Merck Eprova AG v. Gnosis S.p.A. et al. 175
Metropolitan Opera Association v. Local 100, Hotel Employees & Restaurant Employees International Union 155
Micron Tech., Inc. v. Rambus, Inc. 146
Mikron Industries, Inc. v. Hurd Windows & Doors, Inc. 159
Miller v. Holzmann 216, 217
Moreno v. Hanford Sentinel, Inc. 212
Mosaid Technologies Inc. v. Samsung Electronics Co. Ltd. 163
Mudron v. Brown & Brown, Inc. 153
Muick v. Glenayre Electronics 226
National Day Laborer Organizing Network et al. v. United States Immigration and Customs Enforcement Agency 177

Neustar, Inc. v. F5 Networks, Inc. 197
Nichia Corp v. Argos Ltd 252
Northington v. H&M Int'l 147
Nova Measuring Instruments Ltd. v. Nanometrics, Inc. 135, 390
Nursing Home Pension Fund v. Oracle Corp. 163
O'Connor v Ortega 228
Offenback v. L.M. Bowman, Inc. 212
Ohio v. Huffman 7
Oklahoma ex. rel. Edmondson 136
O'Neill v. City of Shoreline 219
Pacific Coast Steel, Inc. v. Leany 206
Peach v Bird [2006] NTSC 14 (Australia) 93
Peal v. Lee 220
Pension Committee of University of Montreal v. Banc of America Securities 165
People v. Bovio 26
People v. Carratu 114
People v. Donath 83
People v. Lugashi 6, 8, 22
People v. Pacifico B. 116
People v. Rodriguez 19, 62, 75
People v. Scolaro 84
People v. Shinohara 62, 67
Peskoff v. Farber 150
PIC Group, Inc. v. LandCoast Insulation, Inc 166
Pillay v. Millard Refrigerated Services, Inc. 147
Pippins v. KPMG LLP 209
Porath v. State (Texas) 86
Positive Software Solutions Inc. v. New Century Mortgage 11
Potts v. Dollar Tree Stores, Inc. 197
QK Healthcare, Inc. v. Forest Laboratories, Inc. 170
Qualcomm Inc. v. Broadcom Corp. 140, 155, 156
Quon v. City of Ontario 229
Rattray v. Woodbury County 166
Regina v. Cox 91
Regina v. D.E.W.B. 91
Regina v. J.M.H. 92
Residential Funding Corp. v. DeGeorge Financial 216
Rimkus Consulting Group, Inc. v. Cammarata 165, 173, 206
Robert Bosch LLC v. Snap-on Inc. 197
Roffe v. Eagle Rock Energy GP, L.P. 179
Romano v. Steelcase Inc. 219
Rosa v. Commonwealth 102, 104
Rowe Entm't, Inc. v. The William Morris Agency 131
R & R Sails v. Insurance Co. of State of PA 209
Russo v. State 103, 104
S2 Automation LLC v. Micron 184
Samsung Electronics v. Rambus 178, 324
Sanders v. State 21, 22, 62, 66, 137, 322, 396

Scotts Co. LLC v. Liberty Mut. Ins. Co. 187
Sekisui American Corp. v. Hart. 176
Semsroth v. City of Wichita 190
Shoesmith, R (on the application of) v. OFSTED & Ors 256
Siani v. State Univ. of New York at Farmingdale 166
Simon Property Group v. mySimon, Inc. 129
Smyth v. Pillsbury Co. 222, 225, 232
Societe Nationale Industrielle Aerospatiale v. United States District Court for the Southern District of Iowa 468
So. New England Telephone Co. v. Global NAPs, Inc. 160
Sony Music Entertainment (Australia) Ltd. v. Univ. of Tasmania, et al. 94
Star Direct Telecom, Inc. v. Global Crossing Bandwidth, Inc 134
State (Minnesota) v. Levie 84
State (N.C.T. of Delhi) v. Sandhu 92
State of Minnesota v. Kandel 128
State of Nebraska v. Nhouthakith 62, 77
State of Washington v. Leavell 22, 62, 74
State (Ohio) v. Anderson 80
State (Ohio) v. Cook 3, 24, 70
State (Ohio) v. Heilman 68
State (Ohio) v. Morris 14, 70, 123
States of America (District Court) v. Royal American Shows, Inc. 260, 300
State v. Bizewski 122
State v. Bolsinger 118
State v. Butler 129
State v. Hayden 74
State v. Kaminski 123
Stengart v. Loving Care Agency, Inc. 204, 226
Steve Jackson Games, Inc. v. United States Secret Service 224
Storer v. Hayes Microcomputer Products 51
Tantivy Communications, Inc. v. Lucent Technologies Inc. 164
Taylor v. Mitre Corp. 167
Taylor v. State 71
Tener v. Cremer 167
Thorncreek Apartments III, LLC v. Village of Park Forest 205
Tomlinson v. El Paso Corp. 133
Toussie v. County of Suffolk 171
Tracy v. NVR, Inc 176
Treppel v. Biovail Corporation 191, 391
TR Investors v. Genger 220
Trulock v. Freech 82
Tulip Computers Int'l B.V. v. Dell Computer 155
Two-Way Media, LLC v. AT&T, Inc. 89
Unigard Sec. Ins. Co. v. Lakewood Engineering & Mfg. Corp. 170
United Cent. Bank v. Kanan Fashions, Inc. 166
United Medical Supply Company v. United States 215
United States v. Alexander 129
United States v. Andreozzi 155
United States v. Andrus 81, 101

United States v. Bailey 226
United States v. Balon 113
United States v. Bass 87
United States v. Bhownath 72, 104
United States v. Bonallo 8
United States v. Briscoe 8
United States v. Brooks 120
United States v. Calimlim 91, 120, 121
United States v. Campos 10
United States v. Carey 108, 111, 113
United States v. Crume 49
United States v. Davis 87
United States v. Dean 39, 50
United States v. Downing 23
United States v. Farlow 122
United States v. Frabizio 128
United States v. Ganier 31
United States v. Glasser 8
United States v. Gray 110, 111, 112, 113, 121
United States v. Greathouse 11, 78, 191
United States v. Habershaw 62, 76
United States v. Hill 117, 118, 127
United States v. Hilton 30
United States v. Houston 88
United States v. Kuntz 89
United States v. Lacy 107
United States v. Liebert 18, 26
United States v. Long 88, 101, 231, 232
United States v. Maali 15, 81, 117
United States v. Maxxam, Inc. 172
United States v. Moore 8
United States v. Naparst 52
United States v. O'Keefe 130, 194, 195, 389
United States v. Philip Morris USA, Inc. 162
United States v. Quinn 23
United States v. Riccardi 91, 119
United States v. Roberts 105
United States v. Rossby 113
United States v. Saelee 20
United States v. Salcido 65
United States v. Scott 3, 29, 74, 112, 121
United States v. Scott-Emuakpor 29, 74
United States v. Sedaghaty 217
United States v. Seifert 51
United States v. Shirazi 73
United States v. Siddiqui 1
United States v. Simpson 106
United States v. Soto 90

United States v. Stanley 90
United States v. Strum 72
United States v. Tank 2, 8, 39
United States v. Turner 105, 116
United States v. Upham 10, 13, 76, 80, 106
United States v. Weatherspoon 18, 26
United States v. Whitaker 3, 5, 8, 23
Universal City Studios v. Reimerdes 52
Upton v. Knowles 17
U.S. v. Comprehensive Drug Testing Case 107
U.S. v. Siciliano 63
Vasudevan Software, Inc. v. Microstrategy Inc. 192
Vector Investments v. Williams 256
Victor Stanley Inc. v. Creative Pipe, Inc. 194
Victor Stanley Inc. v. Creative Pipe, Inc. II 173, 208, 353, 354
Voom Holdings LLC v. EchoStar Satellite LLC 176
Wachtel v. Health Net, Inc. 151
Weisman v. Hopf-Himsel, Inc. 26
Whelan Associates, Inc. v. Jaslow Dental Laboratories, Inc. 59
Whitmore v. Cate 90
Wiginton v. CB Richard Ellis, Inc. 220
William A. Gross Construction Associates, Inc. 158, 159, 194
Williams v. Massachusetts Mutual Life Insurance Company 67, 148, 152, 395
Williams v. Sprint/United Mgmt. Co. 181
Williams v. Taser International, Inc. 136
Williford v. State 22, 62, 65, 66
Wilson v. Thorn Energy, LLC 169
Wisconsin v. Schroeder 112
Wm. T. Thompson Co. v. General Nutrition Corp. 159
Xpel Technologies Corp v. American Filter Film Distributors 62
Yelton v. PHI, Inc. 15
Z4 Technologies, Inc. v. Microsoft Corp. 134
Zenith Elecs. Corp. v. WH-TV Broad. Corp. 181
Zubulake IV 170, 173, 190, 391, 409, 493
Zubulake V 13, 14, 148, 150, 161, 171, 176, 189, 190, 191, 216, 323, 351, 391, 392, 395, 493
Zubulake v. UBS Warburg, LLC 13

Guidance Software is the leader in digital investigation solutions. EnCase® Enterprise is used by numerous government agencies and 65 of the Fortune 100. Market-leading solutions EnCase® eDiscovery, EnCase® Cybersecurity, and EnCase® Analytics help organizations respond to e-discovery requests, security incidents, and emerging internal and external threats.

Guidance® SOFTWARE | EnCase®

www.encase.com