Whitepaper

10 BEST PRACTICES FOR REDUCING E-DISCOVERY RISK AND COSTS

Million-dollar sanctions and public shaming by judges have led many corporations to seek a better way of performing the e-discovery process upon first notice of impending litigation. No longer patiently waiting for inside counsel teams to incorporate the discovery obligations in the Federal Rules of Civil Procedure (FRCP) or applicable state rules, courts expect corporations to apply intelligently and systematically the principles within an e-discovery process that are repeatable and defensible—no more foot-dragging, stone-walling, or excuses.

In addition to the pressures of the FRCP, the location and types of electronically stored information (ESI) continues to evolve. Organizations must not only search for information on premise in repositories, email, and on corporate owned computers, but now they must also incorporate discovery across employee owned devices, social media, and data stored in the cloud.

Certain proven best practices have evolved from corporate responses to the legal standards for discovery of electronically stored information (ESI). This paper presents those best practices and a summary of the overarching legal standards that place both in-house and outside counsel under direct, personal legal obligation to ensure that relevant ESI is preserved, reviewed, and produced in a compliant manner. It then discusses best practices during the litigation hold, identification, preservation, and collection processes, as well as those that apply through review and production.

BEST PRACTICE #1: INSTITUTE A SYSTEM FOR OVERSIGHT OF THE LITIGATION HOLD PROCESS

Technology is a force-multiplier in litigation hold, and organizations that use technology to manage legal hold notices have a reduced risk of failure. Many of the risks of spoliation exist in the multi-step hold notification process that can lead to faulty information-sharing between team members. Having oversight of the process, automating key steps, and being able to document compliance greatly reduce time and risk.

It is important to have a defensible process for giving notice of an ESI legal hold to potentially relevant witnesses. A process coupled with a technology solution that automates key steps can provide documentation of compliance and establish a repeatable process to be initiated immediately upon each successive notice of impending litigation.

A number of organizations rely on e-mails for their legal hold notices with “return-receipt requested” notices that are often ignored. The also try to track responses with spreadsheets. Software aids greatly in managing all the information, providing real-time feedback on whether
a hold has been viewed, seamlessly sharing of information among the team, and the production of complete and accurate records of communications with custodians of relevant ESI.

LITIGATION HOLD	TECHNOLOGY CAPABILITIES
Gaining oversight of the litigation-hold process is possible with an e-discovery solution that:	Automates the issuance of legal-hold notices
	Provides high-level reporting on the status of responses
	Simplifies the creation of custodian interviews
	Gives legal and IT teams the ability to work from the same list of potential witnesses/custodians
	Prompts custodians to identify where data may be found

Table 1: *Technology checklist for litigation hold*

BEST PRACTICE #2: PRESERVE RELEVANT ESI FROM ALL POTENTIAL DATA SOURCES ASAP

When an event triggers the ESI preservation obligation, responding entities and their counsel share a primary duty to make reasonable assessments of appropriate ESI to preserve in good faith. In fact, 80 to 90 percent of the legal risk in e-discovery occurs at the preservation stage. If you fail to preserve ESI properly at the beginning of a case, it is difficult and sometimes impossible to retrieve relevant ESI and metadata reliably months or years later, and the effort can be costly. Not only that, failing to preserve properly can mean that your time in court is spent defending your methodology rather than the merits of the case.

At the same time, courts do not require perfection: no legal duty exists to preserve every shred of paper, e-mail, electronic document, and backup tape for every case. ***Reasonableness is the standard.***

Many organizations have implemented e-mail archiving systems and rely on these systems to preserve e-mail for litigation. Because the duty to preserve ESI extends well beyond e-mail, this best practice involves enabling the rapid initiation of a process that preserves all relevant ESI, including:

- Word documents
- Excel files
- Acrobat files (.pdf)
- Archived e-mail
- Social-media and chat-system communications
- Cloud repositories
- Mobile devices such as smart phones and tablets
- All written communications stored locally on laptops, desktops, servers, and more

A court will exercise its authority to conduct a proportionality analysis to consider whether to relieve a party of its obligation to produce ESI from sources not reasonably accessible because of undue burden or cost. There are hundreds of cases where the critical evidence was ESI other than e-mail, such as ***Beard Research v. Kates***.[i] The amount of sanctions can be substantial.[ii]

Three practical requirements for meeting the reasonableness standard are:

1. Identify sources of relevant ESI
2. Notify the custodians of relevant ESI that they should not delete or change such ESI
3. Take affirmative steps to effectively preserve the relevant ESI in a way that is verifiable and does not degrade the properties of the document

Whenever you reasonably anticipate litigation over a particular matter, it's time to begin preserving ESI.

PRESERVATION	TECHNOLOGY CAPABILITIES
Working to preservation best practices is a straightforward matter with e-discovery technology that:	Searches and collects from all potentially relevant data sources, including : • Hard drives • Servers • Shared drives

	Enables processing of all potentially relevant file types:
	• Word
	• Excel
	• PowerPoint
	• Acrobat (.pdf)
	• E-mail
	  • *Archives*
	  • *Exchange*
	  • *Domino servers*
	  • *Locally stored .PST and .NSF files*

	Can collect content from various content management and e-mail archive systems as: • Microsoft SharePoint • EMC Documentation • Open Text • Symantec Enterprise Vault
	Are you able to collect from Cloud Repositories such as: • Box • Dropbox • Microsoft Office 365 • Google Drive • Amazon S3 • Google Drive

Table 2: *Technology checklist for preservation*

BEST PRACTICE #3: PERFORM A TRUE EARLY CASE ASSESSMENT—BEFORE COLLECTION

"Early Case Assessment" (ECA) has become a misnomer in the industry in that most e-discovery technologies only address ECA as a component of review, i.e., after data has been collected and processed. To best support the e-discovery process, legal counsel should conduct early case assessment prior to collection to see the relevant data as quickly as possible in order to analyze the case merits and develop a strategy. In addition, objective analysis and first-pass review should be performed early and often, at any point in the e-discovery process—including while collection and processing are taking place.

With full-disk image or outsourcing approaches, conducting an informed early case assessment is mainly not possible, because these approaches require collection to be completed and analyzed for relevant data before case assessment can be formed.

Organizations that have in-house e-discovery technology are equipped to conduct advanced searches for relevant ESI at the same time collection and processing occurs, which enables true early case analysis. EnCase® eDiscovery enables viewing of ESI as soon as it is collected from custodians, using its web-based interface that provides the ability to browse through and view documents and e-mails, providing relevant case information within hours. As a result, organizations have the ability to search, analyze, and review ESI content to understand case merits, identify responsive documents, and further cull down the data set prior to attorney review.

EARLY CASE ANALYSIS (ECA)	TECHNOLOGY CAPABILITIES
The ability to perform ECA is a significant advantage in formulating a case strategy. A robust e-discovery solution should help you:	Gain the earliest possible insight of potential costs, keywords, and custodians
	Uniquely test search criteria before ESI is collected, allowing you to adjust keywords, file types, or timeframes
	Identify custodians for litigation hold notification
	Identify relevant data sources
	Provide metrics on total data versus potentially relevant data

Table 3: *Technology checklist for ECA*

BEST PRACTICE #4: PERFORM A TARGETED SEARCH AND COLLECTION

Every gigabyte of unnecessarily collected ESI adds time, trouble, and cost to the downstream e-discovery workflow. Larger volumes of ESI also require greater storage and more computer power to search and cull, which ultimately slows all aspects of the workflow. For many years, vendors recommended the collection of "full disk images" from target computers, which resulted in increased fees for searching, processing, hosting, loading into attorney review platforms, and reviewing.

While full-disk imaging is not an e-discovery best practice for every case, the ideal solution is one that not only allows for efficient, targeted searches, but also for forensically sound full-disk imaging. Full-disk imaging can be a necessary tactic in certain circumstances, such as in internal investigations or the investigation of possible theft of intellectual property.

TARGETED SEARCH AND COLLECTION	TECHNOLOGY CAPABILITIES
You can greatly simplify the process of collection by targeting your searches with an e-discovery solution that:	Provides initial metrics on the amount and types of potentially relevant ESI
	Assesses collected data through advanced search, e-mail threading, and tagging capabilities
	Targets search and collection using filtering criteria on the front end, such as file types, keywords, and data ranges - this can reduce data-collection volumes by over 90 percent
	Analyzes ESI either pre- or post-collection for confidential or privileged data by searching for: • Keywords • File types • Metadata • Timestamps • Hashing • Other fields

Table 4: *Technology checklist for targeted search and collection*

BEST PRACTICE #5: COLLECT ESI BASED ON SEARCH CRITERIA OPTIMIZED FOR EACH CASE

The scope of ESI collection from particular custodians depends on two things:

1. The type of issues at stake in the underlying matter
2. The ability of counsel to formulate effective search criteria based on what they know about the case

In the vast majority of matters, it is a best practice to restrict collection to "user-created data"—those file types that hold nearly all the relevant evidence custodians create or receive, such as Microsoft Word, Excel, PowerPoint, or e-mail file types.

By collecting only user-created data, only a fraction of the data will be collected, compared to what is collected with a full-disk image, which is everything. When counsel has sufficient information to reasonably determine effective search criteria, it is reasonable to collect ESI by culling at the point of collection, applying keyword, timeframe, and file-type filtering.

BEST PRACTICE #6: PRESERVE METADATA IN A FORENSICALLY SOUND MANNER AT THE POINT OF COLLECTION

Metadata is a key component of every e-mail and electronic file and is often overlooked by novice e-discovery practitioners during the preservation phase, only to find out during the analysis phase that it is important, and then it is too late. It establishes, among other things, precisely when a document was created or modified.

Employing this best practice assists in the document-review stage of litigation, in creating timelines, and in establishing authorship of ESI. Failure to preserve metadata can have significant adverse consequences.[iii]

The volatile nature of metadata makes preserving it at the point of collection critical to future requirements and to avoid adverse inferences or sanctions. Production of ESI should be made in a form in which information is ordinarily maintained or reasonably usable, taking into account the need to produce reasonably accessible metadata that gives the receiving party the same ability to access, search, and display information as the producing party (Sedona Conference Principle 12).

PRESERVING METADATA	TECHNOLOGY CAPABILITIES
An enterprise-grade e-discovery software system should:	Automatically maintain all original metadata, including "created" and "last accessed" timestamps
	Preserve the source file and metadata in an unalterable container, such as the Logical Evidence File container file type in EnCase eDiscovery, accepted in courts around the world
	Save the data and metadata together in their original state, not separately
	Produce an exact duplicate of the original source file
	Maintain that original state throughout processing and load-file creation

Table 5: *Technology checklist for Preserving Metadata*

Preserving these basic fields in a forensically sound manner is important for authentication of ESI at trial as well as giving context to files and searchability for review. Courts generally order production of metadata, when requested, in the initial discovery phase.[iv]

The challenge with metadata is that, at the time of preservation and collection of ESI, it is unknown if the metadata is, or will become, relevant. If the metadata is altered at the outset, it can be impossible to reset it to its original state. Thus, best practice is to lock down the metadata in a forensically sound manner for every case.

Some e-discovery software programs automatically maintain all original metadata, including created and last-accessed dates. This metadata should be stored in an unalterable evidence file container that cannot be altered and can be used to prove chain of custody.

METADATA FIELDS	ELECTRONIC FILES	E-MAIL
Author	X	X
Recipient		X
Subject	X	X
File Name	X	X
CC Recipient(s)		X
BCC Recipient(s)		X
Date/Time Created	X	
Date/Time Saved	X	
Date Sent		X

Table 6: *Common metadata fields for electronic files and e-mail*

BEST PRACTICE #7: AVOID CUSTODIAN SELF-COLLECTION

Custodian self-collection is unreliable and not defensible. Relying upon individual custodians to conduct collections without oversight can result in spoliation sanctions. The preservation obligation attaches to the responding party as well as in-house and outside counsel involved in e-discovery decision-making.

Thus, when organizations task custodians with carrying out counsel's preservation obligation—without counsel's close supervision—it is viewed as an unlawful "outsourcing" of the preservation obligation. More typically, the practical problem is that custodians are not very good at identifying and preserving responsive ESI. This is the primary reason why it is not a best practice to simply send litigation-hold notices to custodians in lieu of actual collection of the ESI.

Custodians are not equipped to find responsive ESI; they are often non-technical people without access to sophisticated search technology.

BEST PRACTICE #8: BRING PRESERVATION AND COLLECTION IN-HOUSE

The outsourcing of e-discovery preservation carries certain risks. Internal e-discovery teams develop proficiency in dealing with e-discovery collections and preservations both large and small, and can lose their edge when vendors handle these tasks without them. The ability to handle small collections as a significant advantage in smaller matters like employment cases should not be overlooked, because organizations' sanctions do not come infrequently from the smaller discovery matters.

In-sourcing e-discovery preservation can bring dramatic savings, even when considering the added workload for company personnel. Organizations implementing in-house e-discovery processes typically conduct a budget analysis that takes into account estimated costs for personnel, hardware, technology, and training for the e-discovery team. With respect to required technology, it is recommended to conduct a return on investment (ROI) analysis, which computes the cost of the software (license, annual maintenance, staffing, related services, and training) and then calculates how long it will take for the savings to pay for the technology compared to the cost of outsourcing.

PRESERVATION AND COLLECTION	TECHNOLOGY CAPABILITIES
Legal departments can reduce spoliation risks and e-discovery costs with a technology solution that:	Delivers the most comprehensive results possible
	Collects and preserves relevant data in a repeatable and defensible manner that ensures a strict chain of custody
	Performs collection and preservation of ESI in a manner that is non-disruptive to day-to-day business operations

Table 7: *Technology checklist for preservation and collection*

BEST PRACTICE #9: STREAMLINE REVIEW BETWEEN IN-HOUSE AND OUTSIDE COUNSEL

In-house counsel is in a better position to control the identification, location, and preservation of relevant ESI, but outsourcing the review process has been a common corporate practice. Often, in-house counsel conducts an initial review of documents to isolate key documents, then relies on outside counsel for a more comprehensive review and production of document. Maintaining a consistent process of review between in-house and outside counsel is challenging, particularly when different methods are being used to review ESI.

In order to streamline the review between in-house and outside counsel, legal teams need a collaborative platform that enables a seamless integration between in-house review capabilities and full review. This type of environment can also greatly simplify the process of producing ESI to opposing counsel in a consistent manner. Also, time and money is saved by avoiding costly upload charges from an in-house review platform to one utilized for full review by outside counsel.

STREAMLINING REVIEW AND PRODUCTION	TECHNOLOGY CAPABILITIES
Inside counsel can lower the risk of errors as well as time and costs for review and production with a central legal repository that:	Collects only new data for each case
	Offers cross-case perspectives when working on multiple matters
	Establishes consistent, defensible processes across all matters
	Eliminates redundant data through de-duplication
	Enables you to analyze sooner and more easily through the use of metrics and cross-case trend reports

Table 8: *Technology checklist for streamlining review and production*

BEST PRACTICE #10: IMPROVE ABILITY TO MANAGE ESI PRODUCED ACROSS ALL MATTERS

With many corporate counsel expecting an increase in litigation in the coming year, it no longer makes sense to reinvent the wheel with each notice of impending litigation. Many legal teams still find it extremely complicated to compare ESI from prior matters with that collected, reviewed, and produced for a current case.

Processes must be evolved to the point of defensibility, incorporate new data sources, and then made repeatable across all cases while still containing costs. This is only possible with a collaborative technology environment that retains all work product, compares current cases to previous ones, and ensures that documents withheld in one matter are never produced in another, such as attorney-client privileged or confidential information. Keeping all matters in a single repository enables instant comparison and analysis of production across all pending matters for an organization, rather than relying on a myriad of review platforms used by different law firms handling cases for the organization.

CONCLUSION

The best practices outlined above as well as the authorities cited underscore the importance of an effective and systematic e-discovery process. Best-practices technology can enable corporate counsel to establish such a defensible process in order to simultaneously minimize risk and cost while also increasing the likelihood that they will be able to try each case based on its merits and not on the shortcomings of the e-discovery process employed. Overcollection, sanctions, and high e-discovery costs are symptoms of the absence of a defendable, repeatable, in-house process. By establishing a scalable and system-wide e-discovery process, organizations can not only save money, but also greatly improve compliance.

LEARN MORE ABOUT ENCASE EDISCOVERY

For more information on EnCase eDiscovery, please visit: guidancesoftware.com/ediscovery

CITATIONS

[i] See Beard Research v. Kates, CA No. 1316, (Del. Chanc. May 29, 2009); Digene Corp. v. Third Wave Technologies, Inc., 2008 U.S. Dist. LEXIS 10816 (W.D. Wisc. Feb. 8, 2008) (PowerPoint presentations); and Sprint v. United Management Co., 2007 U.S. Dist. LEXIS 5477 (D. Kan. Jan. 23, 2007) (spreadsheets).

[ii] See Qualcomm, Inc. v. Broadcom Corp., 2008 WL 66932 (S.D.Cal. 2008) ($8.5 million in sanctions); United States v. Philip Morris USA, 327 F. Supp.2d 21 (D.D.C. 2004) ($2.75 million in sanctions); MOSAID Techs, Inc. v. Samsung Elec. Co., 348 F. Supp. 2d 334 (D.N.Y. 2004) ($500 million in sanctions).

[iii] See Bray & Gillespie Management LLC v. Lexington Ins. Co., 2009 WL 546429 (M.D. Fla. Mar. 4, 2009).

[iv] See Aguilar v. ICE | DHS, 2008 WL 5062700 (S.D.N.Y. Nov. 21, 2008).

GUIDANCE SOFTWARE

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.