Guidance Software | Whitepaper

Best Practices for Preservation & Collection of Electronically Stored Information for Litigation: Minimizing your e-discovery risk while reducing cost

John Blumenschein, Esq.
Patrick J. Burke, Esq.
Russell Gould

Guidance® SOFTWARE

I. Introduction

In the years since the amendments to the Federal Rules of Civil Procedure (FRCP) codified discovery obligations of electronically stored information (ESI), courts have interpreted the scope of those obligations in hundreds of cases around the U.S. These precedents have helped create the foundation for a set of e-discovery best practices, and in turn, these best practices have made e-discovery practitioners more confident in assessing legal risks.

This white paper addresses those best practices related to the preservation and collection of ESI and provides a summary of the overarching legal standards that place in-house and outside counsel under direct, personal legal obligations to ensure that relevant ESI is preserved as soon as litigation can reasonably be anticipated. It then discusses best practices during the various stages of the preservation and collection process and concludes with a discussion of an organization's economic considerations in implementing a defensible e-discovery process.

II. The Scope of the Legal Obligation to Preserve ESI

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 preserve all potentially relevant ESI, they will be able to execute all downstream processes; such as, identification, review, and production. However, if counsel do not preserve ESI in a timely manner, they risk losing evidence. Courts refer to this as "spoliation." When spoliation occurs, a court may issue sanctions depending on the egregiousness of the data loss.

a. Who Holds the Preservation Obligation?

The lawyers handling e-discovery matters bear more than just the preservation obligation; they also bear an ethical duty of competence and diligence.[1] Even when experts assist, the attorney retains an obligation to personally supervise the overall effort and its defensibility. It is strongly recommended that the legal department assemble an interdisciplinary e-discovery team headed by legal and including representatives from records management, compliance, audit and HR as well as IT (and/or IT Security) personnel who have the technical expertise and authority to conduct in-house ESI collection and preservation. Furthermore, the legal team should collaborate with the e-discovery team to draft written processes and procedures that apply to all ESI preservation exercises. This creates a repeatable, defensible process, which assures quality. The attorney then has the obligation to ensure all parties effectively follow the organization's e-discovery processes and procedures.

b. When Does ESI Need to Be Preserved?

Litigants must preserve potentially relevant ESI when they can "reasonably anticipate litigation."[2] This can be challenging. One rule of thumb is for counsel to determine if they feel justified marking a written memo on the matter as privileged "in anticipation of litigation." If so, then it is also time to begin preserving ESI. Realize that once memoranda begins being marked regarding a matter as privileged, the court will consider that the latest date to assert for launching preservation efforts. Because time is of the essence, there are strong advantages to having in-house capabilities to respond to the preservation obligation immediately and avoid the steps required to engage and coordinate with outside vendors.

c. Identification of Custodians and Systems that Store Relevant ESI

Once one can reasonably anticipate litigation, the legal team's initial focus must be to identify where relevant ESI resides and then take immediate steps to ensure effective preservation. Of course, targeting custodians' e-mail is a top priority, but keep in mind that many ESI

spoliation cases involve electronic documents other than e-mail.[3] In most cases employee laptops, workstations, group drives, or e-mail shares hold the bulk of relevant non-e-mail ESI. The legal team is responsible for identifying who those employees (referred to as "custodians" of their ESI) are. Once the legal team identifies the custodians, case law calls on the responsible attorneys to ensure that (1) each custodian receives appropriate legal hold notices and (2) each custodian's relevant ESI is found and preserved.[4]

d. What ESI Needs to Be Preserved?

When an event triggers the ESI preservation obligation, responding entities and their in-house and outside counsel share a primary duty to make reasonable assessments of appropriate ESI to preserve in good faith.[5] Courts do not require perfection; there is no duty to preserve every shred of paper, e-mail, electronic document, and backup tape.[6] Reasonableness is the standard, and a court will exercise its power 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.[7]

III. Best Practices for Identifying Relevant ESI

As noted above, courts have expressed their support for a reasonableness standard for e-discovery preservation and collection and have set out three practical requirements: first, identify sources of relevant ESI; second, notify the custodians of relevant ESI that they should not delete or change such ESI; and third, take affirmative steps to effectively preserve the relevant ESI in a way that is verifiable and does not degrade the properties of the document.

Best practices for the identification stage begin and end with smart lawyering, i.e., quickly learning enough about the substance of the matter and the organization's employees involved so that relevant ESI can be located and preserved as soon as possible. In this context, identification, hold and collection are a continuum of the same preservation workflow that results in the collection of targeted ESI across the network.

The task is to identify all employees, information repositories (e.g. group shares, SharePoint, document management systems, e-mail archives), and backup systems that may contain relevant ESI. Much of this phase involves investigation and interviews by the legal department. Lawyers simply need to dig into the matter on an initial basis, enough to effectively preserve potentially relevant ESI. Because the evidence lies on the organizations' networks, a network-enabled technology tool is a force-multiplier in these efforts.

Experience teaches that—like legal hold and ESI collection— e-discovery professionals can accomplish identification faster, cheaper, and better with a unified technology solution. Guidance Software EnCase® eDiscovery is one such solution, and we will use it as an exemplar for what e-discovery professionals can and should achieve with enterprise-wide e-discovery software.

IV. Best Practices for Issuing Legal Hold Notices

Technology is also a force-multiplier when it comes to the legal hold process. The risks for spoliation lie in the multi-step hold notification process that invites faulty pass-offs of information among team members. Software aids greatly in managing all the information, seamless passing off of information among the team, and documenting compliance by keeping accurate and complete records of communications sent to and received from custodians of relevant ESI.

Organizations that have in-house technology to manage legal hold notices have a reduced risk of failure. That said, the only truly effective legal hold is one that results in collection and

preservation of the relevant ESI, rather than preserve in place holds that merely rely on others not to destroy it. When counsel can rely on in-house people, processes, and technology to collect relevant ESI in the first instance, they can worry less when it comes to the effectiveness of the legal hold notices sent to employees and to the various far-flung corners of the organization's information infrastructure. This is why organizations should have a unified e-discovery solution, like EnCase® eDiscovery, that seamlessly combines the legal hold notice and collection process.

V. Best Practices: Collection and Preservation of ESI

Best practices for collection and preservation of ESI revolve around these five concepts:

1. Perform a targeted collection.

Every additional 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, 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 IP theft.

2. Collect ESI based on search criteria appropriate to the case.

The scope of ESI collection from particular custodians depends on two things: the type of issues at stake in the underlying matter and 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 like Microsoft Word, Excel, PowerPoint, or e-mail. By collecting only "user-created data" only a fraction of the data will be collected compared to a full-disk image. 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, time-frame, and file-type filtering.

3. Preserve metadata

Metadata is a key component of every e-mail and electronic file and is often overlooked by novice e-discovery practitioners (only to find out that metadata was not preserved when it is too late during the analysis and review phase). It establishes, among other things, precisely when a document was created or modified.[8] Common metadata fields for electronic files include author, subject, file name, date and time created, and date and time last saved. For e-mail, common fields include author, recipient, CC, subject, BCC, date sent, and file name.[9] EnCase® eDiscovery automatically maintains all original metadata, including created and last-accessed dates, and stores that metadata in the EnCase Logical Evidence File container, which cannot be altered. Metadata is kept in its original state with the file rather than being stored separately. In this way, collected files are exact duplicates in every manner of the original source file, allowing for digital authentication and better searching and timeline creation in every case.

4. Custodian self-collection is unreliable and not defensible.

Relying upon individual custodians to conduct collections by themselves can result in

spoliation sanctions.[10] 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 legal hold notices to custodians in lieu of actual collection of the ESI. Custodians are not equipped to find responsive ESI; they usually are non-technical and do not have access to sophisticated search technology.

5. Perform a true early case assessment, before collection.

To best support the e-discovery process legal counsel should conduct early case assessment to see the relevant data as quickly as possible in order to analyze the case merits and develop a strategy. To achieve this objective analysis and first-pass review should be done early and often, at any point in the e-discovery process –including during collection and processing. 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 technology are able to conduct advanced searches for relevant ESI at the same time collection and processing occurs, which enables true early case assessment. 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 in hand 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 dataset prior to attorney review.

VI. Consider the economics of implementing a defensible ESI preservation and collection process versus outsourcing.

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 to 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. Guidance Software account managers can assist in the creation of a comprehensive ROI analysis geared to the implementation of the EnCase® eDiscovery solution.

VI. Conclusion

The authorities cited above underscore the importance of an effective and systemic e-discovery search and collection process. Best-practices technology can enable corporate counsel to establish such a defensible process that simultaneously minimizes risk and cost. Over collection 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 procedure, organizations can not only save money, but also greatly improve compliance.

This memorandum is provided as an informational resource only. The information contained in this document should not be considered or relied upon as legal counsel or advice.

For more information please visit www.guidancesoftware.com/eDiscovery

Notes

1 ABA Model Rules of Professional Conduct. Rule 1.1. A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. Rule 1.3. A lawyer shall act with reasonable diligence and promptness in representing a client. Rule 8.4(d). It is professional misconduct for a lawyer to engage in conduct that is prejudicial to the administration of justice.

2 *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. July 20, 2004) (*"Zubulake IV"*) (Defendant should have known documents were relevant to future litigation when former employee filed a complaint with the Equal Employment Opportunity Commission); *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities*, 2010 WL 184312 (S.D.N.Y.,2010) ("While litigants are not required to execute document productions with absolute precision, at a minimum they must act diligently and search thoroughly at the time they reasonably anticipate litigation").

3 *Richard Green (Fine Paintings) v. McClendon*, 262 F.R.D. 284 (S.D.N.Y. Aug. 13, 2009) (Plaintiff's motion for sanctions granted based on a handful of Excel files created on a home computer); *Innis Arden Golf Club v. Pitney Bowes, Inc.*, 257 F.R.D. 334 (D. Conn. May 21, 2009) (Plaintiff precluded from offering evidence of contaminants in its soil for failing to preserve electronic records of soil analysis and the soil samples themselves); *Arteria Property Pty Ltd. v. Universal Funding V.T.O., Inc., et al.*, 2008 U.S. Dist. LEXIS 77199 (D.N.J. Oct. 1, 2008) (Court found Defendants had a duty to preserve its web site at the time the suit was filed even though a nonparty hosted it); *Beard Research v. Kates*, CA No. 1316, (Del. Chanc. May 29, 2009) (PowerPoint presentations); *Digene Corp. v. Third Wave Technologies, Inc.*, 2008 WL 483752 (W.D. Wisc. Feb. 8, 2008) (PowerPoint presentations); *Williams v. Sprint/United Management Co.*, 2007 WL 196890 (D. Kan. Jan. 23, 2007) (spreadsheets); *Sklar v. Clough*, 2007 WL 2049698 (N.D. Ga. Jul. 6, 2007) (article from online newspaper, PowerPoint presentation); *W.E. Aubuchon Co., Inc. v. BeneFirst, LLC*, 245 F.R.D. 38 (D.Mass.,2007) (electronic images of claim forms).

4 *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 2007 WL 684001 at *17 (D.Colo., Mar. 2, 2007) ("While instituting a 'litigation hold' may be an important first step, the obligation to conduct a reasonable search for responsive documents continues… "); *In re NTL Securities Litig.*, 2007 WL 241 344 at *15 (S.D.N.Y. Jan. 30, 2007) ("Although NTL sent out [litigation] hold memos . . . those hold memos were not sufficient, since they subsequently were ignored"); *Samsung Electronics Co., Ltd. v. Rambus Inc.*, 2006 U.S. Dist. LEXIS 50007 (E.D. Va. Jul. 18, 2006) ("It is not sufficient, however, for a company merely to tell employees to 'save relevant documents,' ... this sort of token effort will hardly ever suffice"); *Exact Software North America, Inc. v. Infocon, Inc.*, 479 F.Supp.2d 702 (N.D. Ohio Dec. 5, 2006) (Court demands company outline steps taken to preserve, search and collect ESI in response to discovery request); *Wachtel v. HealthNet*, 2006 WL 3538935 (D.N.J. Dec. 6, 2006) (Court criticizes Healthnet's "utterly inadequate" eDiscovery process where paralegal merely e-mails preservation notifications).

5 *Texas v. City of Frisco*, 2007 WL 828055 (E.D. Tex. March 27, 2008)("[W]hile they do not specifically address pre-suite litigation hold requests, the Rules of Civil Procedure contemplate that the parties will act in good faith in the preservation and production of documents. See Fed. R. Civ. P. 37."); see Sedona Commentary on Preservation at 2 & n.3.

6 *Zubulake* at 212, 217.

7 FRCP 26(b)(2)(B) Specific Limitations on Electronically Stored Information. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made,

the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C).

8 See *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D.Md. May 4, 2007) (Presumption is that metadata is not hearsay and is prima facie evidence of authenticity).

9 See *National Day Laborer Organizing Network v. United States Immigration and Customs Enforcement Agency*, 2011 WL 381625 (S.D.N.Y. Feb. 7, 2011) (opinion withdrawn); *O'Neill v. City of Shoreline*, 2010 WL 3911347 (Wash. Oct. 7, 2010)(Embedded metadata in an electronic document should be disclosed as part of the Washington State Public Records Act); *Lake v. City of Phoenix*, 222 Ariz. 547 (Ariz. Oct. 29, 2009) (Metadata contained in public records maintained in an electronic format should be disclosed per the Arizona public records act).

10 *Qualcomm v. Broadcom*, 2010 WL 1336937 (S.D.Cal. April 2, 2010) ("… 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 supported the important legal arguments, claims, and defenses being presented to the court. These fundamental failures led to the discovery violations").

Our Customers

Guidance Software's customers are corporations and government agencies in a wide variety of industries, such as financial and insurance services, technology, defense contracting, pharmaceutical, manufacturing and retail. Representative customers include Allstate, Chevron, FBI, Ford, General Electric, Honeywell, NATO, Northrop Grumman, Pfizer, SEC, UnitedHealth Group and Viacom.

About Guidance Software (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations 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 30,000 licensed users of the EnCase technology worldwide, the EnCase® Enterprise platform is used by over half of the Fortune 100, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from Law Technology News, KMWorld, Government Security News, and Law Enforcement Technology.

For more information about Guidance Software, visit www.guidancesoftware.com.

Guidance® SOFTWARE
The World Leader in Digital Investigations™