eDiscovery Collection Best Practices for the Enterprise

Guidance® Software
The World Leader in Digital Investigations™

I. Introduction

The vast majority of risk associated with electronic discovery centers around the effectiveness of a litigant's preservation and collection efforts. Since 2004, dozens of companies involved in high-stakes litigation have incurred hundreds of millions of dollars in collective losses because of failure to demonstrate a defensible eDiscovery preservation and collection process. This trend has increased as several post-December 2006 court decisions invoke the newly-enacted amendments to the Federal Rules of Civil Procedure (FRCP) to apply a heightened degree of scrutiny to this critical aspect of the eDiscovery equation.

In addition to substantially increased risk, much of the high cost of eDiscovery stems from poor collection practices that result in over-collection and other inefficiencies. Companies routinely pay millions of dollars per case to eDiscovery service providers due to lack of an efficient internal process. However, utilizing best-practices processes and technology during the preservation, collection and culling stages enables considerable cost savings that flow through the entire eDiscovery cycle.

To help organizations understand how to mitigate these staggering risks and costs, this paper presents a legal overview of the best practices for collecting and preserving Electronically Stored Data (ESI). Addressed in this paper are (1) why maintaining an established and systemic eDiscovery process is essential; (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 an organization's eDiscovery process should be outsourced or brought in-house.

This paper should not to be construed as legal advice or be relied upon as such. Rather, the goal of this paper is to serve as a reference for organizations that seek or are weighing the importance of establishing a proper eDiscovery collection and preservation capability.

II. The Critical Importance of an Established Process and the Perils of Custodian Self-Collection

One of the most important aspects of the new eDiscovery FRCP amendments is that they direct attention to electronic discovery issues in the early stages of litigation. For instance, the new rules require that relevant electronic evidence be identified, preserved and disclosed at the outset of the litigation, thus necessitating — among other requirements — an effective process to meet these preservation obligations. 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 capability to preserve 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, 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."[1]

Under these new rules, litigants face a greater likelihood of court sanctions with failure to properly preserve relevant ESI at the outset of the litigation. It is no surprise then that recent cases applying amendments to the Federal Rules underscore the need for a defensible eDiscovery preservation and collection capability. In these important decisions, courts are carefully scrutinizing efforts undertaken to execute litigation holds and collection in the context of motions to compel and for sanctions.

For instance, *In re NTL, Inc. Securities Litigation*, 2007 WL 241344 (S.D.N.Y. Jan. 30 2007), 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 . . ."[2] 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 *Peskoff v. Ferber* — F.R.D. —, 2007 WL 530096 (D.D.C.), the Court heavily scrutinized the defendant's ESI preservation, search and collection efforts employed 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:

> "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."

Similarly, in *Wachtel v. Health Net, Inc.*, 2006 WL 3538935, (D.N.J . Dec. 6, 2006), 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." The Court made clear that having a paralegal merely email preservation notifications is insufficient, noting that "Despite the document hold, thousands of employees' emails failed to be searched."[3] The Court found that "even when [defendant's] employees could search their emails, their searches were *sporadic* rather than *systemic*."[4] The Court, concluding that these failings constituted bad faith, imposed harsh evidentiary and monetary sanctions.

Samsung Electronics v. Rambus, 439 F.Supp.2d 524 (E.D. Va. 2006) echoes the 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."[5] The Court determined that the defendants' lack of consistent systematic and effective processes to collect and preserve relevant ESI demonstrated spoliation of evidence.

The unmistakable message from these cases is diligent and effective ESI preservation and collection efforts are required under the new FRCP amendments and will be expected as a matter of course going forward. Companies 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.

Law firms and corporations 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 dangerous 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 thus defend the specific search, retrieval and collection efforts of each custodian. Manual efforts, by definition, are non-systemized and do not allow for documented and consistent application of objective criteria for the collection of ESI 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 its 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 or accuracy of the data collection. Several recent cases provide that file metadata must be preserved and produced.[6]
- **Authentication Challenges**: Custodian self-collection does not generate an automated chain of custody and thus will likely (and unfortunately) require the employees' personal testimonies to explain their efforts.
- **Scalability**: Custodian self-collection beyond a few individuals is highly disruptive and involves a substantial logistical challenge, requiring extensive coordination and project management.
- **Expense**: The notion that custodian self-collection is less expensive is a myth. Inefficient collection efforts result in high back-end processing and review costs; larger cases require hundreds of hours of additional project management fees by outside counsel or consultants.

So to address these concerns, large companies are establishing a highly operational and systemized process to address ESI requirements as a standard litigation practice instead of a more reactive and *ad hoc* approach. The traditional "wait-and-see" approach to eDiscovery — where companies and counsel often defer addressing ESI until its production is demanded by opponents — results in a disjointed approach to ESI typified by 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 organizations 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, the question turns to the scope of required preservation and collection efforts. Are full-disk images of every custodian's hard drive necessary? What are the benefits and proper role of computer forensics in the eDiscovery collection equation? Must the entire email system of a company be searched? Can search and collection be narrowly tailored to specific custodians, specified timeframes and keywords?

A. 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 new 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."[7] Similarly, in *Zubulake v. UBS 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 corporate entity. Accordingly, the Court agreed to limit the defined searches to certain individuals "most likely to have information relevant to the arbitration issues."[8] See also *U.S. v. Greathouse,* 297 F.Supp.2d 1264 (D. Or. Oct. 20, 2003) [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…[9]

B. Full-disk Images Not a Routine Requirement for eDiscovery Preservation

Collection and preservation of ESI must incorporate a defensible process that accomplishes the objective 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 eDiscovery vendors and consultants as a routine eDiscovery practice. While such deep-dive analysis is required in some circumstances, full-disk imaging is unwarranted as a standard eDiscovery 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 eDiscovery processing and hosting fees are usually calculated on a per-gigabyte basis, costs are increased exponentially.

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.

In sum, 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 eDiscovery collection process is one that will both facilitate compliance while mitigating costs.

IV. The Benefits and Defensibility of an In-House Process

A key decision for corporate counsel is whether the organization's eDiscovery search and collection process should be internalized and run by trained IT personnel equipped with the proper technology and training, or to rely on hired service providers. With a 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. As much of the expense and shortcomings associated with a non-systemized eDiscovery process occur in the collection phase, an internal and systemized capability enables both cost savings and improved ability to comply with the amended FRCP.

In addition to considerable cost savings, establishing a systemized and consistent process reduces business disruption and mitigates risk by enhancing compliance. As noted above, the "early attention" requirements of the amended FCRP 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 and run by a well-trained internal team that is very familiar with the organization's IT infrastructure and that works alongside corporate legal is well-suited to meet these requirements.

In fact, recent case law fully supports the defensibility of large organizations handling eDiscovery internally. 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.[10] 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 defendable process and defeat the plaintiff's highly charged 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 clients data storage systems. Residential's eDiscovery provider professed 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 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 to design efficient and systemized processes that are largely executed 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 is proving to be the most effective for large organizations.

V. Effective Enterprise Technology: The Foundation of a Defendable Process

Establishing a defendable process is a critical element of compliance as opposing counsel are now routinely seeking to capitalize on the eDiscovery 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 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 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 FRCP amendments, these tactics will only increase.

An established enterprise investigation capability can be a powerful shield against these tactics. For instance, EnCase® Enterprise is based on the core 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 an effective chain of custody. Such a solid foundation of credibility and reliability provides 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 organizations can not afford to forgo such a scalable, systemized — and thus defendable — process in place.

The identification and preservation of ESI is a technical process that requires a technical solution, especially if a company hopes to establish such capabilities on a global, integrated and 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[11] and can qualify as an exception to the hearsay rule.[12] These tasks are achieved simultaneously in an automated fashion all without disrupting operations.

VI. Conclusion

The authorities citied above underscore the importance of an effective and systemic eDiscovery search and collection process. Best-practices technology can enable corporate counsel to establish such a defensible process that simultaneously minimizes cost. Routine full-disk imaging, over collection and high eDiscovery costs are symptoms of the absence of a systemized process. By establishing a scalable and system-wide eDiscovery procedure, large organizations can save millions while greatly improving 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.

FOOTNOTES:

1 *Managing Discovery of Electronic Information*: *A Pocket Guide for Judges*; Federal Judicial Center, 2007 Barbara J. Rothstein, Ronald J. Hedges and Elizabeth C. Wiggins

2 *Id.* at *20

3 *Wachtel*, 2006 WL 3538935 at *8 (emphasis added)

4 Id. at *18 (emphasis added).

5 Id. at 565.

6 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).

7 The Sedona Principles; *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, Principle 11 (2003)

8 *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

9 Manual for Complex Litigation § 40.25(2). (emphasis added)

10 *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 at *8 (S.D.N.Y. July 20, 2004)

11 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.

12 Fed. R. Evid. 803(6)

ABOUT GUIDANCE SOFTWARE (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.

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.