INSIDE THE MINDS

The Role of Technology in Evidence Collection

Leading Lawyers on Preserving Electronic Evidence, Developing New Collection Strategies, and Understanding the Implications of Social Media

ASPATORE

Understanding Counsel's Obligations and Challenges in the E-Discovery Process

Robert Friedman

Partner and Head, New York Business Trial Group

Sheppard Mullin Richter & Hampton LLP

ASPATORE

Introduction

There are two separate components to the topic of evidence collection in litigation. The first pertains to the lawyer's discovery duties and obligations under the Federal Rules of Civil Procedure and equivalent state rules. The other involves forensic and strategic evidence analysis aimed at helping an attorney win his or her case at trial, whether representing a civil litigant, a government entity, or a defendant in a criminal case.

With respect to discovery, the overarching goal is to meet the obligations established by federal and state rules. Judge Scheindlin famously established the scope of a producing party's e-discovery responsibilities under the Federal rules in *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 322 (S.D.N.Y. 2003). As she stated in her opinion, "... electronic documents are no less subject to disclosure than paper records. This is true not only of electronic documents that are currently in use, but also of documents that may have been deleted and now reside only on backup disks."

Most inside and outside counsel are mindful of electronic discovery obligations. Counsel may be less focused on the changes in evidence presentation spurred by greater accessibility to electronic evidence. This is the second part of the chapter—now that you have electronic discovery, how do you use it?

Rules and Trends Concerning Litigating Over Discovery

Greater accessibility to data is accompanied by greater accountability on the part of litigants. A litigating party must now be ready to defend any choice not to produce electronically stored information (ESI) with technological detail and sound legal basis. All litigators must be aware of certain Federal Rules, especially after the 2006 amendments.

First, Rule 26(a)(1)(B) makes clear that a party must disclose ESI at the outset of a case when those materials support the party's claims or defenses. Second, Rule 26(b)(2)(B) categorizes ESI into two classes: (1) ESI that is reasonably accessible, which a party must search and produce, and (2) ESI that is not reasonably accessible because of undue burden or cost. This second category is not required to be produced unless the requesting litigant

shows "good cause" that the electronic materials are relevant and valuable to the litigation. Third, Rules 16(b) and 26(f) direct parties to discuss issues relating to the preservation and production of ESI at their initial planning meeting. It is important to meet baseline obligations to avoid litigating over discovery, rather than the merits of the case, which has become an unfortunate reality. Electronic discovery has spawned a cottage industry of plaintiffs' lawyers and consultants eager to capitalize on discovery missteps.

Because of technological advances in this area, the needle has shifted, and courts are expecting more of litigants with respect to ESI production. For example, as discussed below, courts have largely abandoned an earlier presumption against the production of metadata. What was considered not "reasonably accessible" in the past may now be considered accessible. Consequently, inside and outside counsel must stay on top of technological advances and be aware that courts and opposing counsel are also up-to-date. Judges see cases involving e-discovery issues every day and expect litigants to meet the new standards when they are determining what is reasonable.

In addition, courts are increasingly familiar with motions to compel and motions to impose sanctions for spoliation related to e-discovery failures. One area of recent interest is social media status updates or feeds. Last year, for example, the Southern District of Indiana in *EEOC v. Simply Storage Management*, permitted an employer to obtain discovery of an employee's social networking activity that, through privacy settings, the employee had made unavailable to the general public. *EEOC v. Simply Storage Management,* 270 F.R.D. 430 (S.D. Ind. 2010). Last September, courts in New York and Pennsylvania, both hearing personal injury cases, compelled discovery of social media evidence that purportedly undercut the plaintiffs' claims of incapacitation. *Romano v. Steelcase*, 2010 NY Slip Op 20388, 30 Misc.3d 426 (Sup.Ct., Suffolk County 2010); *McMillen v. Hummingbird Speedway,* No. 113-2010 CD (C.P. Jefferson 2010). The court in *McMillen v. Hummingbird Speedway* ruled that "Where there is an indication that a person's social network sites contain information relevant to the prosecution or defense of a lawsuit ... access to those sites should be freely granted." *McMillen v. Hummingbird Speedway,* No. 113-2010 CD (C.P. Jefferson 2010). Accordingly, discovery targeted to social media has become a useful part of a litigator's discovery plan.

Spoliation motions have also become a common litigation tactic. Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. *Gutman v. Klein,* No. 03 CV 1570(BMC)(RML), 2008 WL 4682208, (E.D.N.Y. Oct. 15, 2008) (citing *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999)). Federal Rule of Civil Procedure 37(f) states that "... absent exceptional circumstances, a court may not impose sanctions under these rules on any party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." However, parties must have the ability to suspend their deletion system when litigation is reasonably anticipated. *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 218 (S.D.N.Y. 2003) Failure to do so will likely lead to sanctions.

Attorneys should assist their clients in issuing "litigation holds" once a dispute arises. *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 218 (S.D.N.Y. 2003) ("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").

A litigation hold is a written notice that informs persons with the power to affect the continued existence of electronic information of the need to retain it. Judge Scheindlin's recent decision in *Pension Committee of the University of Montreal Pension Plan vs. Bank of America Securities* is instructive. There, plaintiffs failed to institute written litigation holds in a timely manner and engaged in careless and indifferent collection efforts after the duty to preserve arose. *Pension Committee of the University of Montreal Pension Plan vs. Bank of America Securities*, 685 F.Supp.2d 456, 463 (S.D.N.Y. 2010). The court issued a myriad of sanctions ranging from further discovery to monetary penalties and an adverse inference charge. Judge Sheindlin did not hide her displeasure with plaintiffs: "By 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." *Id.* at 462.

Counsel must not underestimate the effect of spoliation sanctions on the course of litigation. In *Gutman v. Klein,* the Eastern District of New York

imposed the sanction of a default judgment in favor of plaintiffs when it was discovered that a defendant had irretrievably deleted computer files that likely contained important information. *Gutman v. Klein,* No. 03 CV 1570(BMC)(RML), 2008 WL 4682208, (E.D.N.Y. Oct. 15 2008). More recently in *Victor Stanley Inc. v. Creative Pipe Inc.* defendant Mark T. Pappas failed to implement a litigation hold, failed to preserve ESI, deleted thousands of computer files, used programs to overwrite the files, and disobeyed numerous court orders regarding the production and preservation of ESI. Judge Grimm of the District of Maryland ordered that the spoliating defendant could avoid a two-year imprisonment sentence for contempt of court only by immediately paying all fees and costs awarded to plaintiff, calling Pappas' conduct "the single most egregious example of spoliation that [he had] encountered in any case." *Victor Stanley Inc. v. Creative Pipe Inc.* 2010 WL 3530097 (D. MD. Sept. 9, 2010).

Some litigants pursue spoliation issues just as resolutely as the underlying claims. As these cases make clear, any person or litigant who plans to bring or defend a lawsuit must have his ducks in a row as far as the preservation and production of ESI are concerned.

Metadata Preservation and Production Issues

Litigants should be particularly cognizant of the preservation of metadata. Metadata is information describing the history, tracking, or management of an electronic file—it is data about data. *See* Fed.R.Civ.P. 26(f), advisory committee's note (2006). Until recently, many courts took the position that unless metadata was material to resolving the dispute, there was no obligation to preserve and produce it, absent an agreement between the parties or order of the court. *See Kentucky Speedway LLC v. NASCAR Inc.*, 2006 U.S. Dist. (E.D. Ky. Dec. 18, 2006) ("… in most cases and for most documents, metadata does not provide relevant information"); *Wyeth v. Impax Laboratories Inc.*, 2006 U.S. Dist. (D.Del. Oct. 26, 2006) (ruling that most metadata was of limited value and a presumption against production of metadata had emerged in the Default Standard for Discovery of Electronic Documents in the U.S. District Court for the District of Delaware).

However, the tide has changed within the past few years, and a growing number of courts are ordering the production of ESI in the form in which the information is ordinarily maintained or in a reasonably usable form. As always, the court must balance the relevancy and burden in making its determination of reasonableness. As Magistrate Judge Frank Maas of the Southern District of New York explained:

> As a general rule of thumb, the more interactive the application, the more important the metadata is to the understanding the application's output. Thus, while metadata may add little to one's comprehension of a word processing document, it is often critical to understanding a database application. A spreadsheet application lies somewhere in the middle and the need for its metadata depends upon the complexity and purpose of the spreadsheet.

Aguilar v. Immigration and Customs Enforcement Division, 255 F.R.D. 350 (SDNY 2008).

In *National Day Laborer Organizing Network v. United States Immigration and Customs Enforcement Agency,* Judge Sheindlin recently held that certain metadata is an integral or intrinsic part of an electronic record and ruled that it should have been produced by the government in responding to a Freedom of Information Act (FOIA) request. She further admonished the parties to work together to deal with the production of metadata and other ESI, saying:

> Once again, this Court is required to rule on an e-discovery issue that could have been avoided had the parties had the good sense to meet and confer, cooperate, and generally make every effort to communicate as to the form in which ESI would be produced. … all lawyers … need to make greater efforts to comply with the expectations that courts now demand of counsel with respect to expensive and time-consuming document production.

Id.

Choosing Strategies and Cost-Shifting

The strategies that are chosen for evidence collection and submission will largely depend on the type of case a litigant is dealing with. A key practical consideration is how large the case is and how money much is at stake. With respect to evidence collection and discovery obligations, it is important to consider what is reasonable. For example, what would be considered reasonable discovery in a $1 billion or $50 million dispute may not be considered reasonable in a $1 million case. The Federal Rules specifically state that a court may limit the extent of discovery if it determines that the expense outweighs the likely benefit, taking into account the needs of the case, *the amount in controversy,* and the parties' resources." Fed.R.Civ.P. 26(b)(2)(C) (*emphasis added).*

A litigant will need to scale the scope of discovery to the costs that are involved. We have recently seen a greater acceptance on the part of many courts to entertain the concept of cost-shifting. Traditionally, there is a presumption that the responding party must bear the expense of complying with discovery requests. *Oppenheimer Fund Inc. v. Sanders,* 437 U.S. 340, 358 (1978). However, if the discovery of ESI imposes an "undue expense or burden on the responding party," cost-shifting may be considered. *Zubulake v. UBS Warburg,* 217 F.R.D. 309, 316-319 (S.D.N.Y. 2003). Assuming the requested discovery is inaccessible, *Zubulake* instructs that courts should engage in a cost-shifting analysis by sampling the data and applying the following seven-factor test:

1. The extent to which the request is specifically tailored to discover relevant information
2. The availability of such information from other sources
3. The total cost of production compared to the amount in controversy
4. The total cost of production compared to the resources available to each party
5. The relative ability of each party to control costs and its incentive to do so
6. The importance of the issues at stake in the litigation
7. The relative benefits to the parties of obtaining the information

Zubulake at 322.

Beyond on this seven-factor test, courts are more likely to shift costs when the producing party provides documented evidence that the discovery sought is not reasonably accessible. For example, in *Major Tours Inc. v. Colorel,* No. 05-3091(JBS/JS), 2009 WL 3446761 (D.N.J. Oct. 20, 2009), the producing party submitted affidavits that the retrieval of e-mails from de-duplicated backup tapes would cost between $81,425 and $114,000. The court therefore ordered the parties to share equally in these costs. In addition, courts are more likely to shift costs when the requesting party has thus far been in compliance with the rules and with court orders. In *Degeer v. Gillis,* No. 09 C 6974 (2010), 2010 WL 5096563 (N.D.Ill. Dec. 8, 2010), the producing party requested costs for any future searches and production, arguing that he had already searched and produced a huge volume of records at a cost in excess of $130,000. The court ultimately held that only some cost-shifting was warranted, essentially punishing both parties for their failure to approach the production of ESI with "a spirit of cooperation or efficiency." *Id.* The court was most troubled by the fact that the parties never discussed specific search terms or data custodians to be searched in advance of the document review process. *Id.*

Sophisticated Clients and Helpful Vendors: The Way Forward

Sophisticated litigants are increasingly perceptive with respect to early and effective ESI collection and preservation. Across the board, in-house and outside counsel are partnering early to identify the proper custodians of evidence, where relevant evidence is located, and how to preserve that evidence. Today, a major part of outside counsel's responsibility involves knowing a client's internal evidence collection protocol and preservation programs. An ancillary positive result is that both inside and outside counsel are evaluating and becoming familiar with the facts of their cases much earlier in the litigation process.

In addition, since the 2003 *Zubalake* decision, an entire industry of vendors has risen from the electronic discovery morass. In many cases, in-house attorneys will work with regular outside vendors and will institute programs and protocols for electronic evidence collection and preservation. This may occur even before outside counsel becomes involved. Outside vendors routinely assist with discovery planning, data gathering, computer forensics, and the searching of computers and e-mail. Obviously there is a benefit to

using the same vendor because the vendor can customize the program, and the parties gain efficiencies through familiarity. In addition, the vendor will usually offer the client a better price.

The use of e-discovery vendors has also spawned a number of advancements with respect to the evidence collection, preservation, and analysis process. Some of these advancements include analytics, predictive coding, and more advanced algorithms for data searching. New technology is even being used to analyze and investigate the tone of e-mails. Evidence collection is now a highly competitive field, and the competition has bred many of these new technological advances. Vendors also offer metrics to evaluate cost and efficiencies. Another ancillary result is that clients are able to evaluate e-discovery costs in a more predictable fashion and to negotiate flat-fee or capped rates with outside counsel.

The challenge for both in-house and outside counsel is to determine which processes and vendor programs are appropriate for the particular case at issue and how these processes will assist in meeting obligations established by the discovery rules and in ultimately winning the case. It is important to ensure that the discovery program and protocol chosen by a corporation or litigant have been tested, and that the corporation or litigant is comfortable that it will withstand scrutiny against an adversary who, one must assume, will litigate your document preservation and production procedures.

Winning the Case: Determining Strategies for Obtaining, Admitting, and Analyzing Electronic Evidence

Many of the same technological advances that are used to preserve and produce documents can be used to obtain evidence and win the case. For example, once presented with a plaintiff's production, a defending party can use predictive coding to shed irrelevant documents. Algorithms and search terms can be used to pick out correspondences between key players in the litigation. Forensic computer analysis may also be employed as part of a strategic case analysis plan. If a litigant can access or obtain discovery of laptops, mobile devices, and/or personal computers, a forensic analysis can be helpful in determining the history of key documents and of communication between and among the parties in the litigation.

However, the bounty of electronic evidence that can be mined through new technologies will be of little help if it is ultimately excluded at trial. Evidentiary rules must be considered when ESI is proffered.

Authentication Guidelines for Electronic Records

Under Federal Rule of Evidence 901(a), a party seeking to admit an electronic exhibit must make a prima facie case showing that the exhibit is what he or she claims it to be. *Lorraine v. Markel American Ins. Co.,* 241 F.R.D. 534, 542 (D.Md. 2007). Authentication of an electronic exhibit presents unique challenges, as changes to the exhibit may sometimes be difficult or impossible to detect and uncover.

One of the easiest ways to authenticate an electronic record is to have a witness testify that the item is what it claims to be, a method permitted by Federal Rule of Evidence 901(b)(1). In *U.S. v. Kassimu,* 188 Fed. Appx. 254, 2006 WL 1880335 (5th Cir. 2006), for example, the Fifth Circuit held that computer records were properly authenticated by an employee who demonstrated "familiarity with the procedure by which the records were generated." Many corporate litigants use the 30(b)(6) witness to authenticate ESI. Federal Rule of Civil Procedure 30(b)(6) allows a party to compel an organization, such as a corporation, to designate an agent to testify on its behalf regarding pre-designated topics. In the e-discovery realm, 30(b)(6) witnesses can be called upon to testify as to a company's document preservation procedures and chain of custody issues. Federal Rule of Evidence 901(b)(3) also allows for authentication by an expert witness through a comparison with specimens that have already been authenticated. *Lorraine v. Markel American Ins.,* 241 F.R.D. 534 (D.Md. 2007). Importantly in the ESI area, an expert in computer forensics may be called upon to prove that evidence has not been altered or changed from the time it was collected through its production in court. *Id.*

Authentication may be also derived from circumstantial evidence pursuant to Federal Rule of Evidence 901(b)(4). This rule permits exhibits to be authenticated by "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances. Fed. R. Evid. 901(b)(4). One method by which electronic evidence may be authenticated under Rule 901(b)(4) is by examining its

metadata. *See Lorraine v. Markel American Ins.,* 241 F.R.D. 534, 548 (D.Md. 2007) ("Because metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Rule 901(b)(4)").

Authentication issues inevitably arise in the context of archived websites, which can be extremely useful in litigation. Web archive destinations, such as Internet archive, allow users to retrieve copies of web pages as they existed at various times in the past. *See* James V. Masella, *The Use and Admissibility of Evidence from the Internet,* INSIDE THE MINDS: NEW DEVELOPMENTS IN EVIDENTIARY LAW IN NEW YORK, 2011 Ed., 55. However, the vast majority of courts will admit archived screen shots from the Internet Archive and similar companies only after a litigant has procured a "statement or affidavit from an Internet Archive representative with personal knowledge of the contents of the Internet Archive website." *St. Luke's Cataract and Laser Institute P.A. v. Sanderson,* 2006 WL 1320242 (M.D. Fla. May 12, 2006); *see also Specht v. Google,* 2010 WL 5288154 (Dec. 17, 2010 N.D.Ill) (refusing to consider Internet Archive printouts not authenticated by an officer or employee of the Internet Archive); *Audi AG v. Shokan Coachwork Inc.,* 592 F.Supp.2d 246, 279 (N.D.N.Y. 2008) ("Plaintiffs also submit copies of Defendants' website [into evidence]. However, Plaintiffs use the www.archive.org website to generate the submitted images without authentication from a representative of that website. Accordingly, the court will not consider same in support of Plaintiffs' motion for summary judgment"). Litigants seeking to introduce such evidence should make sure to procure the requisite employee statement.

Hearsay Concerns and Policies

Hearsay issues are pervasive in the ESI arena. As is the case with conventional paper evidence, the contents of an electronic document will be deemed hearsay if they contain an out-of-court statement that is offered in evidence to prove the truth of the matter asserted. Fed.R.Evid. 801(c). A "statement" is defined as an "oral or written assertion" or "nonverbal conduct of a person." Fed.R.Evid. 801(a).

One interesting hearsay consideration that is especially relevant in the ESI context is the question of whether the evidence at issue constitutes an out-of-court "statement." For example, in *People v. Nazary,* 91 Cal. App. 4th 727, 754 (2010), a California Court of Appeals found that because computer printouts were machine-generated, they could not constitute hearsay and should be admitted. As the court explained, "The essence of the hearsay rule is a requirement that testimonial assertions shall be subjected to the test of cross-examination. … Under no possible scenario could the PIC machines have been cross-examined." *Id.; see also Lorraine v. Markel American Ins.,* 241 F.R.D. 534, 564 (Where the [electronic] writings are non-assertive, or not made by a "person," courts have held that they do not constitute hearsay, as they are not "statements").

This problem is especially germane when it comes to metadata. Metadata can be divided into two categories: system metadata and application metadata. *The Sedona Conference Commentary on ESI Evidence & Admissibility,* March 2008. System metadata consists of information generated by a computer without human input. *Id.* Examples include a file's name, location, format, and the dates on which a file was created, modified, and accessed. *Id.* Courts have held that system metadata cannot constitute "hearsay" under the Federal Rules of Evidence, as it is generated by a computer and not a human. For example, in *United States v. Hamilton,* 413 F.3d 1138 (10th Cir. 2005), a criminal case involving Internet pornography, the government introduced and the district court admitted copies of approximately forty-four images at issue. Each of the images featured computer-generated "header" information, including the screen name of the poster, subject of the posting, date that the images were posted, and the poster's Internet protocol (IP) address. *Id.* at 1142. The court noted, in ruling that the header information was not hearsay, "Of primary importance … is the uncontroverted fact that the header information was automatically generated by the computer … this uncontroverted fact clearly places the header information outside of Rule 801(c)'s definition of 'hearsay.'" *Id.; see also U.S. v. Khorozian,* 333 F.3d 498, 506 (3d Cir. 2003) (concluding that header information automatically generated by a fax machine was not hearsay, as nothing "said" by a machine is hearsay).

Application metadata, on the other hand, includes spreadsheet formulas and comments or redline changes in word processing documents and is the

product of human input. *Id.* Accordingly, litigants will generally have to find a hearsay exception or other argument to admit it. For example, application metadata might be admitted using the business records exception under Federal Rule of Evidence 803(6), or a litigant could argue that the metadata constitutes a party admission and thus is not hearsay under the Federal Rules. Fed.R.Evid. 801(d)(2).

Conclusion

While technology can aid in case preparation and provide efficiencies, there is no substitute for rolling up your sleeves and reviewing documents. No matter how advanced the technology, there may be nuanced issues in these cases, and important documents simply may not fit into any algorithm or search term. In my view, once they have the tools, good trial lawyers cannot take shortcuts.

Key Takeaways

- Ensure that your client has a clear document retention policy in the ordinary course of business.
- Make sure your client also can suspend or alter that retention policy to preserve discoverable data when litigation is reasonably anticipated.
- Stay abreast of technological advancements in electronic discovery.
- Ensure that the discovery program and protocol your client has in place has been tested and that you are comfortable that it will withstand scrutiny against an adversary who may very well attempt to litigate your document preservation and production protocol.
- Address document preservation early and often in discovery.
- Meet with your adversary as early as possible to discuss electronic discovery issues and cost-saving tactics.
- *Be offensive:* Do not lose sight that you are also an advocate and need to analyze how to obtain, admit, and use electronic evidence.

Robert Friedman is a partner in Sheppard Mullin Richter & Hampton LLP's Business Trial and White Collar practice groups in the firm's New York office. He heads the Business Trial practice group in New York.

Mr. Friedman focuses his practice on business and corporate litigation matters. He has particular experience in securities litigation, internal investigations, corporate trust litigation, real estate litigation, director and officer liability, bankruptcy litigation, restrictive covenants, and intellectual property. He has tried cases involving trade secrets, computer software theft allegations, false advertising, and alleged securities law violations. He has also handled maritime disputes on behalf of shipping companies and creditors' committees.

Mr. Friedman has tried more than sixty cases and regularly represents financial institutions, technology companies, Internet marketers, and litigation trustees in significant business disputes. He speaks and writes extensively on various litigation topics and is widely quoted in the legal and mainstream press. He was named a 2010 New York Super Lawyer.

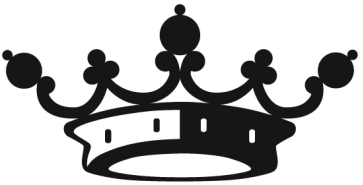
Prior to entering private practice, Mr. Friedman was a senior trial attorney in the Homicide Bureau of the Kings County District Attorney's Office.

Acknowledgment: *Kathryn Hines, an associate at Sheppard Mullin Richter & Hampton LLP, assisted in the preparation of this chapter.*

ASPATORE

Aspatore Books, a Thomson Reuters business, exclusively publishes C-Level executives and partners from the world's most respected companies and law firms. Each publication provides professionals of all levels with proven business and legal intelligence from industry insiders—direct and unfiltered insight from those who know it best. Aspatore Books is committed to publishing an innovative line of business and legal titles that lay forth principles and offer insights that can have a direct financial impact on the reader's business objectives.

Each chapter in the *Inside the Minds* series offers thought leadership and expert analysis on an industry, profession, or topic, providing a future-oriented perspective and proven strategies for success. Each author has been selected based on their experience and C-Level standing within the business and legal communities. *Inside the Minds* was conceived to give a first-hand look into the leading minds of top business executives and lawyers worldwide, presenting an unprecedented collection of views on various industries and professions.



ASPATORE