COUGHLIN DUFFY LLP

ATTORNEYS AT LAW

Preservation and E-Discovery from a Litigation and Risk Management Perspective

Kevin T. Coughlin, Esq.
Suzanne C. Midlige, Esq.
Robert J. Re, Esq.
Maida Perez, Esq.
Jason Pozner, Esq.

350 MOUNT KEMBLE AVENUE
P.O. BOX 1917
MORRISTOWN, NEW JERSEY 07962-1917
PHONE: (973) 267-0058
FACSIMILE: (973) 267-6442

WALL STREET PLAZA
88 PINE STREET, 5TH FLOOR
NEW YORK, NEW YORK 10005
PHONE: (212) 483-0105
FACSIMILE: (212) 480-3899

WWW.COUGHLINDUFFY.COM

COUGHLIN DUFFY LLP

TABLE OF CONTENTS

I. Introduction

The ubiquitous use of electronic media as a means of communications has had a powerful impact on all aspects of daily life. Corporations and organizations throughout the world have come to rely on electronic media in all facets of their operations. With the globalization of industry, the ability to instantly communicate is a tool that organizations worldwide find indispensable. Notwithstanding its ease of use, electronic communication is not without controversy, particularly where litigation is involved. Indeed, in recent years, we have seen an increasing number of cases wherein courts in the United States have addressed the vast use of electronic data and its impact on litigation in the United States.

United States Courts are continuously carving out and redefining the boundaries of electronic document preservation and production requirements. As a result of the drastic consequences now being sought from and often granted by courts in electronic discovery, organizations and its lawyers must keep a watchful eye on this evolving landscape. In perhaps the most infamous e-discovery sanctions case to date, a Florida jury awarded financier Ronald Perelman $1.45 billion in damages after the trial judge entered a default judgment against Morgan Stanley as a sanction for various e-discovery missteps.[1] The trial judge found that Morgan Stanley initially certified that all relevant electronic records had been produced, but then repeatedly uncovered new backup tapes months after the discovery deadline had passed. The trial judge ruled that Morgan Stanley had deliberately failed to comply with discovery and instructed the jury to assume that Morgan Stanley had helped to defraud Mr. Perelman. As a result of this instruction, Mr. Perelman had to prove only that he relied on Morgan Stanley's

[1] CPH (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., 2005 WL 679071 (Fla. Cir.Ct., Mar. 1, 2005), rev'd on other grounds, 955 So. 2d 1124 (Fla. Dist. Ct. App., 2007).

`

representations to his financial detriment. While the judgment, including the award of punitive damages, was later reversed on grounds unrelated to the electronic discovery issues (which were not discussed by the appellate court), the trial court's rulings and the jury's findings are a cautionary tale of the potential impact of electronic discovery abuses.

The rulings surrounding e-discovery can also be a trap for the unwary or uniformed — severe sanctions are not confined to egregious or intentional conduct but can also be assessed for mere ordinary negligence in complying with electronic discovery obligations. The standard for the award of such sanctions was most prominently articulated in the seminal case of Zubulake v. UBS Warburg LLC. [2] In this employment discrimination case, defendant UBS had taken steps to impose a "litigation hold" to ensure the retention of e-mails and other documents relevant to the litigation. Despite these steps, UBS employees deleted potentially relevant e-mails from their computers. In addition, UBS failed to produce many potentially relevant e-mails that had been retained, and delayed the production of the e-mails that it did produce. The Zubulake court held that the defendant had willfully destroyed potentially relevant e-mails and deserved the sanction of an adverse spoliation inference — an instruction to the jury that the lost e-mails were presumably relevant and damaging to defendant's case — which ultimately led to a $29.3 million judgment against UBS.

Other recent cases illustrate how courts do not hesitate to impose a variety of sanctions against litigants who fail to abide by their discovery obligations. In 2006, the Federal District Court for the Southern District of California imposed sanctions against a defendant, an investor in Napster, Inc., in a copyright infringement action regarding musical compositions.[3] After learning that the defendant's employees routinely deleted e-mails pursuant to its "long-standing"

[2] Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004).
[3] UMG Recordings, Inc. v. Hummer Winblad Venture Partners (In re Napster, Inc. Copyright Litig.), 462 F. Supp. 2d 1060 (D. Cal. 2006)

document policy, without regard to whether the deleted e-mails were relevant to the litigation, the court issued a preclusion of evidence order, an adverse inference instruction, and an award of attorneys' fees. The court found these sanctions appropriate despite the fact that the defendant's conduct did not constitute a "pattern of deliberately deceptive litigation practices," and notwithstanding evidence that the number of e-mails actually lost was small.

A New Jersey federal court imposed significant sanctions against an ERISA class action defendant for repeated e-discovery abuses, including failing to search e-mails and permanently losing others due to standard e-mail retention practices.[4] While reserving its decision as to the propriety of a default judgment until certain class action issues had been resolved, the court, notwithstanding its proclaimed reluctance to sanction parties, issued a variety of sanctions, including: (1) deeming certain facts admitted by defendant for all purposes; (2) precluding evidence that was not produced by the defendant in discovery; (3) striking various privilege assertions by the defendant; (4) directing the payment of substantial costs and attorneys' fees related to defendant's misconduct; (5) imposing fines in an amount to be determined after the court considered defendant's financial condition; and (6) appointing a discovery monitor at the defendant's expense to review defendant's compliance with the court's discovery orders.

Notwithstanding the imposition of severe civil and judicial sanctions, organizations should also be aware of the criminal liability which may be imposed upon an organization for failure to preserve documents in light of a pending litigation. The most notorious case emerged out of the fall of Enron. In Arthur Andersen LLP v. United States, the United States Supreme Court addressed the document retention practices of Arthur Andersen during the Enron investigation.[5] The accounting firm's policy, even after the recognition of an impending

[4] Wachtel v. Health Net, Inc., 239 F.R.D. 81, 90-91 (D.N.J. 2006).
[5] Arthur Andersen LLP v. United States, 544 U.S. at 696, 699-700 (2005).

investigation and litigation, allowed for the destruction of documents which could be relevant.[6] In that case, the continued destruction of documents in the face of knowledge of an impending investigation and litigation led to the criminal indictment of Arthur Andersen.[7]

These cases provide examples of how electronic discovery issues can lead to extraordinary and unforeseen adverse results to litigants. Lawyers have long struggled in the paper world with the question of whether they preserved and produced everything in discovery. In the era of electronic discovery this struggle is much more challenging. Electronically stored information is easily created, however, it is also easily destroyed and/or misplaced. Locating and accounting for all your electronic data is no easy task and a source of common mistakes. Preservation orders and common law preservation obligations can be difficult to comply with when dealing with electronic data and emerging technologies.

In response to the increasing number of cases, and escalating number of sanctions and judgments involving the exchange of electronic data during litigation, the Federal Rules of Civil Procedure ("Rules") were amended to specifically address litigant's rights and responsibilities with regard to electronically stored information ("ESI").[8] Although litigants were previously obligated to preserve and produce electronic documents, the Rules now explicitly outline concerns and issues that are specific to ESI, which were necessarily not at issue when individuals were strictly confined to paper documents. The task of ESI preservation, and its impact on the litigation process, is daunting in that it includes a wide-range of information which previously did not exist or was unavailable.

---

[6] Id. at 700-01.
[7] Id. at 702.
[8] The Rules were amended on December 1, 2006, and will be amended again effective December 1, 2007. Though the 2007 amendments make no substantive changes to the Rules, the organization and format of the Rules will change. Any citations to the Rules in this paper will be first to those currently in effect, and then to the form of the Rule in effect as of December 1, 2007.

This paper provides an overview of the recent amendments to the Rules with regard to the discoverability of ESI and the impact the changes have on litigants and potential litigants. The paper addresses when the obligations to preserve ESI arises in the context of litigation or potential litigation, the obligations that a party has with regard to preserving ESI and the legal consequences of non-compliance. Finally, we present a guide for organizations to consider in response to the newly revised Rules with regard to their individual corporate document retention policies.

II. What is Electronically Stored Information ("ESI") and Where Do You Find It?

A. ESI Is Everywhere

The source of the trepidation from ESI preservation and the impact it has on the discovery process is the wide-range of information it encompasses which previously did not exist or was unavailable. Digital or electronic information can be stored in many different ways. When most people think about ESI, they generally look at it from the perspective of typical business documents such as e-mail, word processing documents, or spreadsheets. ESI that may be relevant to specific litigation, however, may be found in many different forms and places. Most organizations may not even be aware of where all its ESI is maintained. In recommending adoption of the revised Federal Rules the Report of the Judicial Conference Committee on Rules of Practice and Procedure said:

> The discovery of electronically stored information raises markedly different issues from conventional discovery of paper records. Electronically stored information is characterized by exponentially greater volume than hard-copy documents. Common cited current examples of such volume include the capacity of large organizations' computer networks to store information in terabytes, each of which represents the equivalent of 500 million typewritten pages of plain text, and to receive 250 to 300 million e-mail messages monthly. Computer information, unlike paper, is also dynamic; merely turning a computer on or off can change the

> information it stores. Computers operate by overwriting and deleting information, often without the operator's specific direction or knowledge. A third important difference is that electronically stored information, unlike words on paper, may be incomprehensible when separated from the system that created it. These and other differences are causing problems in discovery that rule amendments can helpfully address.

The most common form of ESI at issue in litigation is e-mail since it is used universally and is often not used carefully. The content of e-mail may be very informal and subject to differing interpretations. It also is not confined to a single source. In fact, e-mail can be located almost anywhere. It may be found on company e-mail servers, e-mail backup tapes, general server backup tapes, individual PCs used by company employees, personal PCs used by employees who do work at home, Blackberrys, Personal Digital Assistant (PDA) devices, servers of external e-mail or Internet Service Providers (ISP), ISP archive tapes, printed pages, or individual storage devices such as USB drives. In addition to the location of the sender's e-mail, businesses must consider where the recipient's e-mail is being stored. For example, e-mail that is forwarded, copied, or blind copied, can end up on the same list of devices noted above for many different individuals or entities. Importantly, even if deleted, e-mail may still be recoverable and, therefore, discoverable. [9]

In addition to e-mail, ESI covers the entire range of documents that can be produced with a personal computer. This includes but is not limited to, processing files, spreadsheet files, and presentation files. Digital files, including pictures, scanned images, and video or audio recordings, can be found on the same devices and storage media listed above for e-mail. As with

[9] Courts have ruled that Rule 34 requests seeking "deleted" electronic files are permissible. See, e.g. Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) (deleted computer records, including e-mail, are discoverable); Simon Property Group L.P. v. MySimon, Inc., 194 F.R.D. 639, 640 (S.D.N.Y. 2000) (court allowed the discovery of deleted files by ordering the appointment of an expert to make copies of the defendant's hard drives to extract the deleted files); Playboy Enterprises v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) (court permitted plaintiff's request for an expert to make a "mirror image" copy of the hard drive, which it would then use to locate the deleted files).

e-mail, the devices and media containing digital files may be controlled or owned by many different individuals or entities. Although digital files are easily copied, modified, and transferred, similar to e-mail, actual permanent deletion of these files is not easy and often will leave traces of the deletion activity.[10]

Other categories of ESI to be considered in planning discovery include company data repositories. These are typically databases containing business information, such as accounting records, personnel records, payroll records, manufacturing and sales records, mailing lists, customer lists, or any other large quantity of information that a company needs or wants to retain and use over time. Businesses should also consider fax server or fax machine logs, network system records (which maintain an extensive record of all activity performed on a computer network and on individual PCs connected to the network), company and individual voice mail systems and telephone answering devices (which may contain phone messages for long periods of time), and individual PC operating system logs (which maintain similar data as network system records although the level of detail is generally not as extensive). Also, instant messages ("IM's") are becoming as important and prevalent as e-mail. A party must be aware that IM's are discoverable ESI. Of course, company security systems will generally have a record of date, time, and the entry code or ID code used by the individual making an entry and a Global Positioning System in cell phones and automobiles will also track usage.

[10] See Thompson v. United States HUD, 219 F.R.D. 93 (D. Md. 2003) (stating that searching for deleted electronic records can be particularly time consuming and expensive given the number of storage locations that may have to be checked (e.g., desk-top computers, laptops, PDA's, employee home computers, back-up and archival data, and systems files, for instance), coupled with the possible need to use special search methods to locate deleted files).

B. Don't Forget the Metadata

Every document, whether electronic or not, also has a history. The history includes, but is not limited to the date of creation, the author(s), the revisions and modifications made, whether it has been copied or deleted and by whom. Prior to the advent of computers, the history of a document remained with the person(s) who created it. With technological advances and the pervasive exchange of electronic documents, however, this once private history may now be known and visible to all as metadata.

Metadata is ESI, typically not visible from the face of the document as printed out or as initially shown on the computer screen, but which is embedded in the software and retrievable by various means. It often provides information regarding the creation and modification of a document, and sometimes may include comments by persons participating in the creation or modification of the document. Under the amendments to the Rules, parties are required to consult at the onset of the litigation about the nature of pertinent electronic documents in their custody and the manner in which they are obtained.[11] During these initial discussions, an issue which will likely be raised is how the parties will handle the metadata contained in documents. This includes whether the parties wish to obtain the metadata, and if so, whether there will be any assertion or claim of privilege over some or all of the metadata.

Metadata raises unique issues concerning the waiver of privileges and whether it is ethical to remove metadata unbeknownst to other parties in litigation. One issue is whether metadata included in ESI can be scrubbed or deleted prior to producing the ESI. Another is whether a party can produce files by converting them to hard copy, scanning them, and then sending the image to the requesting party. Because metadata can provide important and critical information in certain instances and may also be considered probative evidence in litigation, it is

[11] F.R.C.P. 26(f)(2006), F.R.C.P. 26(f)(2007)

wise not to either scrub metadata or produce images of documents without the agreement of either the requesting party or the court.

In fact, the scrubbing or altering of the metadata, absent such consent, may expose a party to discovery sanctions.[12] In Williams v. Sprint United Management, the defendant produced requested spreadsheets but scrubbed the metadata. The court had ordered that the spreadsheets be produced in the form in which they are ordinarily kept. As a consequence, the court ordered the reproduction of the spreadsheets with the metadata. It also ordered that any assertion of privilege with regard to the metadata was deemed waived. In In re Seroquel Products Liability Litigation,[13] 2007 U.S. Dist. LEXIS 61287 (M.D. Fl. August 21, 2007), the defendant in a multi-district pharmaceutical products liability litigation was found by the court to have turned over ESI in unreadable formats. The plaintiffs had requested a large volume of ESI and the defendant produced over 10 million pages in electronic format. The scrubbing of metadata was a component of these issues. As a result, the court sanctioned the defendants, allowing the plaintiffs a further hearing to present evidence on their damages caused by defective production by the defendant.

C. Metadata and the Inadvertent Disclosure of Attorney-Client Communications and/or or Confidential or Proprietary Trade Secrets

The larger the amounts of electronic material that are produced in native format, the greater the odds that privileged content and/or metadata will get disclosed. Ethical obligations and case law exist to mitigate the ramifications of an inadvertent disclosure. As a practical matter, however, once privileged matter has been disclosed to an adversary or the public the

[12] Williams v. Sprint United Mgt., 230 F.R.D. 640 (D. Kan. 2005) (court required the production of metadata as probative evidence); but see Kentucky Speedway, L.L.C. v. NASCAR, Inc., 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. December 18, 2006)(court found there was a presumption against the production of metadata and that the requested metadata was not relevant).

[13] In re Seroquel Products Liability Litigation, 2007 U.S. Dist. LEXIS 61287 (M.D. Fl. August 21, 2007).

recipient will not be able to erase it from his/her memory. The inadvertent disclosure of metadata is one of the biggest risks facing lawyers today -- a risk made more acute by ethical and professional requirements to safeguard client confidences.

Generally speaking, the dangers of producing privileged or confidential information exist in two contexts. First, issues may arise in connection with an attorney's communications with a client's adversaries or third parties. Second, risks arise during the disclosure of a client's underlying documents and communications in the course of litigation. In either circumstance, inclusion of metadata in the document provided could accidentally expose confidential information to the detriment of the client and the attorney-client relationship. In recent years there has been a series of diverging ethics opinions among different jurisdictions in the United States regarding an attorney's ethical responsibilities with respect to the handling of metadata in electronic documents. For example, the August 2006 Formal Opinion 06-442 of the American Bar Association states that the "the Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer's reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of an adverse party." Similarly, the Maryland State Bar Association Committee on Ethics found that "there is no ethical violation if the recipient attorney (or those working under the attorney's direction) reviews or makes use of the metadata without first ascertaining whether the sender intended to include such metadata."

In contrast, the New York State Bar Association Committee on Professional Ethics issued an opinion finding that lawyers had an ethical duty to try to limit improper disclosure of metadata pursuant to DR 4-101(B), which states that a lawyer shall not "knowingly" reveal a

client's confidences or secrets.[14] The opinion noted that metadata may, among other things, include editorial comments, strategy considerations, legal issues raised by the client or lawyer, and legal advice provided by the lawyer. Although not all metadata is necessarily confidential or secret, the committee noted that it may, in many circumstances, reveal information that is either privileged or the disclosure of which would be detrimental or embarrassing to the client. Therefore, the committee explained, when a lawyer sends a document by e-mail, as with any other type of communication, the lawyer must exercise reasonable care to ensure that she does not inadvertently disclose her client's confidential information. The committee stated that what constitutes reasonable care will vary with the circumstances, including the subject matter of the document, whether the document was based on a "template" used in another matter for another client, whether there have been multiple drafts of the document with comments from multiple sources, whether the client has commented on the document and the identity of the intended recipients of the document. Significantly, the committee found that reasonable care may, in some circumstances, call for lawyers to stay abreast of technological advances.

Similar to the approach taken by the New York Bar Association, in August 2007, the Legal Ethics Committee of the District of Columbia Bar issued Ethics Opinion 341. The DC Bar's opinion conduced that "when a receiving lawyer has actual knowledge that an adversary has inadvertently provided metadata in an electronic document, the lawyer should not review the metadata without first consulting with the sender and abiding by the sender's instructions. In all other circumstances, a receiving lawyer is free to review the metadata contained within the electronic files provided by an adversary."

In a recent case involving inadvertent disclosure of information embedded in the metadata, the United States Federal Trade Commission ("FTC") released dozens of trade secrets

[14] New York Bar Association Opinion Number 782 (Dec. 8, 2004)

in public court documents involved in an antitrust litigation to block Whole Foods Market's $565 million purchase of Wild Oats. [15] The FTC documents revealed that Whole Foods planned to close 30 or more Wild Oats stores in competitive markets, a move that the company believed would nearly double revenue for some Whole Foods stores. In addition, the FTC documents disclosed how Whole Foods negotiates with suppliers to drive up costs for stores. In the documents, the FTC regulators also discussed the company's closely held marketing strategies. Many of the details in the documents, which FTC lawyers filed electronically, were not intended to be released publicly, but words which were believed to be redacted were actually just electronically shaded black. In fact, the words could be searched, copied, pasted and read in versions downloaded from court computer servers. Court officials did realize the mistake and replaced the filing with a version using scanned pages of the redacted documents. However, the Associated Press downloaded the document from the public server before it was replaced by a properly redacted version. As a result, confidential and proprietary trade secrets of Whole Foods were disclosed to the public.

Given the undeveloped nature of the law, continually evolving technology, the exponential dependence on electronic communications, and the potentially catastrophic impact of inadvertent disclosure of a client's secrets or confidence, it is clear that the issue of metadata protection is likely to continue to plague unwary lawyers and their clients and inflate the cost of transaction and litigation representation. Therefore, it is vital for corporations and their counsel to be aware of metadata and of how their software stores it in order to properly safeguard their clients' confidences. In addition, there must be a continuing dialogue among lawyers, their clients and the client's IT departments to ensure that the disclosure of metadata that is potentially

[15] Christopher S. Rugaber, *Error by FTC Reveals Whole Foods' Trade Secrets*; Associated Press, August 15, 2007 at http://www.washingtonpost.com/wp-dyn/content/article/2007/08/14/AR2007081401784.html

privileged and/or confidential is protected. As the Williams and Seroquel cases illustrate above, parties are not free to determine on their own whether to keep or scrub metadata. While metadata may not be probative or relevant in all cases, it is difficult to determine if this is so at the outset of, or prior to, litigation. Therefore, it is prudent for companies to avoid scrubbing metadata included in litigation holds to avoid the possible consequence of sanctions. Instead, parties should determine whether they might want to scrub metadata, and then, when conferencing with their adversaries after the inception of litigation, attempt to agree on what metadata will or will not be produced. In the event that the parties cannot come to a mutual agreement as to the treatment of the metadata, they can always resort to the assistance of the court to resolve the matter.

III. The Impact of the Changes to the Federal Rules of Civil Procedure on Your Organization

Contrary to the suggestions in the legal media, the amendments to the Federal Rules do not alter or change any previous obligations of litigants in connection with anticipated or pending litigation. Instead, the amendments are intended to clarify and outline a litigant's obligations regarding ESI. While reasonably clear prior to 2006, the revised Rules make it resoundingly clear that ESI is not only discoverable in all of its forms, but that potential parties to litigation have a responsibility to preserve that information. In conjunction with the amendments to the Rules, individual states within the United States have also begun updating their discovery rules. For example, California has authorized its courts to order parties to produce discovery electronically.[16] Illinois, Mississippi, New Jersey and Texas courts allow parties to request ESI

[16] CAL. CIV. PROC. CODE §§ 2017.710-2017.740 (2007).

in specific forms.[17] In addition, Kansas and Wyoming now require attorneys to be familiar with their client's computer systems.[18]

Businesses, therefore, must be concerned with three crucial questions regarding the discovery of ESI:

> (1) What events may trigger an obligation to preserve ESI? This entails determining the likelihood of potential court action, and whether, and when, the party in question should have known of the likelihood of court action;
>
> (2) What types of documents should be preserved? Is the data "relevant"? This is not a straightforward question because it depends on the facts of every individual case, and is an inherently subjective question. If the data is relevant, then a potential party has the duty to preserve that data; and
>
> (3) Once the litigation has begun, and data is requested, does the requesting party have a right to the data? Should the requesting party pay for the expense of getting the data?

A. The Duty to Preserve Information: Litigation Hold Letters

With the wide-range and volume of data currently being stored electronically, organizations may face a daunting challenge when a legal obligation arises to preserve documents. Absent reasonable notice of impending litigation, the Rules impose no sanctions or other penalties on litigants who destroy documents in the normal course of business.[19] Once litigation can be reasonably anticipated, however, any automatic deletion programs must be terminated.[20] Though not a new requirement,[21] in light of the amendments to the Rules and recent court opinions imposing sanctions on parties for their failure to preserve and/or produce electronic documents, an effective internal litigation hold letter is critical for an organization

[17] See Douglas W. Kim, *E-discovery: A Practical Approach*, The SciTech Lawyer, Fall 2007, at 7.
[18] Id.
[19] F.R.C.P. 37(f)(2006); F.R.C.P. 37(e)(2007).
[20] Peskoff v. Faber, 2007 U.S. Dist. LEXIS 62595 at *20 (D.D.C. Aug. 27, 2007).
[21] Lewy v. Remington Arms Co. Inc., 836 F.2d 1104 (8th Cir. 1987).

threatened with litigation. The recent revisions to the Rules and the increasing number of e-discovery judicial opinions may lead some to believe that preservation obligations with regard to electronic discovery are a new concern. However, courts, as well as advisory and regulatory bodies, have long required that parties and their employees, agents and/or representatives in possession of relevant evidence in any form should safeguard the preservation of that evidence.[22]

One of the earliest cases to discuss the obligation to preserve documents in light of the emergence of electronic media was the seminal case of In re Prudential Ins. Co. of Am. Sales Practices Litigation.[23] The Prudential case brought to the forefront the inherent problem facing companies in connection with ensuring that its relevant electronic documents are preserved in connection with anticipated or pending litigation. This policyholder class action lawsuit stemmed from allegations that Prudential employed deceptive sales practices in its sale of life insurance policies.[24] The federal district court entered a discovery order early in the case requiring all parties to preserve all documents and "other records" relevant to the litigation. Despite this order, documents were destroyed at four Prudential offices. Although Prudential management had distributed document retention instructions to its agents and employees via its e-mail system, some employees did not have access to e-mail, while others routinely ignored it. Furthermore, senior management never distributed the court's directive to all of its employees. As a result, outdated sales practice records – key records pertinent to the lawsuit – were destroyed by Prudential. In light of the foregoing, the court held that Prudential lacked a "clear

[22] See The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery I (Sedona Working Group Series 2004); Sedona Conference, the Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, available at www.thesedonaconference.org.

[23] In re Prudential Ins. Co. of Am. Sales Practices Litigation, 169 F.R.D. 598 (D.N.J. 1997).

[24] Id. at 600.

and unequivocal document preservation policy," that the lost materials were relevant and would have reflected negatively on Prudential, and imposed a $1 million sanction.[25]

1. What triggers an organization's obligation to issue a Litigation Hold Letter or Preservation Notice?

There are obvious events that trigger the issuance of a litigation hold letter, such as the filing of a complaint (on your own behalf or by another party), a form notice of claim, receipt of a subpoena or knowledge of a civil or criminal investigation by a regulatory or government agency.[26] Notwithstanding, there are many other events that can predate the filing of a complaint, or notice of an ensuing investigation, that may place an organization on "notice" of potential litigation, warranting the issuance of a litigation hold letter or preservation notice. In fact, courts have held that the "obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party *should have known that the evidence may be relevant to future litigation."* [27] In this regard, once a party reasonably anticipates litigation, including litigation it plans to initiate, courts have held that it is under an obligation to suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents.[28] Unfortunately, neither the Rules nor courts have set clear and exact guidelines describing precisely when, prior to the filing of a complaint,

[25] In the ten years following the Prudential decision, a large number of courts have held that senior management in organizations have an obligation to effectively distribute a litigation hold notice to its employees. See e,g, Danis v. USN Communications, Inc. No. 98 C 7482, 2000 WL 1694325, at 38-41 (N.D. Ill. October 20, 2002) (circumstances of the case indicated insufficient involvement of management in proper oversight and delegation of preservation responsibilities).

[26] Procter & Gamble Co. v. Haugen, 2003 WL 22080734, No. 1:95CV94 DAK (D. Utah August 19, 2003)

[27] Zubulake v. UBS Warburg, L.L.C., 220 F.R.D. 212 (S.D.N.Y. Oct. 22, 2003) ("Zubulake IV") (emphasis added); See also, The Sedona Conference, Commentary on Legal Holds, the Trigger & the Process, Sedona Conference Working Group on Electronic Document Retention & Production (WG1) (August 2007 Public Comment Version), Guideline 1 "Reasonable anticipation of litigation arises when an organization is on notice of a credible threat it will become involved in litigation or anticipates taking action to initiate litigation," available at www.thesedonaconference.org.

[28] Id.

the duty to preserve data begins.[29] Since a party can be sanctioned if it fails to preserve data when it should, it is of paramount importance that potential parties be aware when they must cease automatic deletion programs and begin retaining ESI.[30]

While there may be some mystery about when to impose a litigation hold, in many cases there is no need for potential parties to guess at whether litigation may ensue. If some employees think that a fellow employee, client, or other third party, may sue, this conjecture does not create an obligation to preserve data.[31] However, if a potential party begins internal discussions about how to handle future litigation, or begins creating new documents or data for the purpose of potential litigation, then a data preservation program must be created.[32] Unfortunately, this is not a precise science, as illustrated below.

In the leading case of Zubulake v. UBS Warburg, L.L.C., the defendant, one of Europe's largest financial services firm, was sued in a gender discrimination action in August of 2001. Yet the court determined that the defendant's obligation to preserve documents began in April of that year. The court based its determination on two facts. First, the defendant's employees began discussing the plaintiff in e-mails which were entitled "UBS Attorney Client Privilege." Second, the director of the firm's U.S. Asian Equities Sales Desk, who was the plaintiff's direct superior and one of the individuals who allegedly discriminated against the plaintiff because of her gender, testified that as early as April of 2001 he thought a potential lawsuit was possible. The Zubulake court found that because almost all the defendant's employees were circulating e-mails about potential litigation and the plaintiff's direct superior also thought litigation was possible, the defendant was on notice as early as April of 2001 of potential litigation. In fact, the

[29] Cache La Poudre Feeds, L.L.C. v. Land O'Lakes, Inc., 2007 U.S. Dist. LEXIS 15277 at *24 (D. Co. March 2, 2007) (stating that the time when the duty to preserve ESI arises is determined on a case by case basis).
[30] See *infra* Section IV.
[31] Zubulake IV, 220 F.R.D. at 217.
[32] Samsung Elecs. Co. v. Rambus Inc., 439 F. Supp. 2d 524, 542 (E.D. Va. 2006).

court determined that the idea that litigation was possible was "pervasive", and was held by a senior official in a decision making position. This combination of facts led the Zubulake court to conclude that the defendant should have reasonably anticipated litigation, and begun a document preservation program, i.e. litigation hold prior to the plaintiff's formal filing of a complaint.[33]

The two key concepts that emerged from Zubulake that potential parties should keep in mind when determining whether to impose a litigation hold are: 1) *probability* and 2) *reasonableness*.[34] Potential parties must conclude that litigation is likely, not a mere possibility, before a litigation hold becomes necessary. The conclusion that a party reaches as to probability must also be reasonable, i.e., the party must have evidence to which it can point that supports its conclusions about probability. Despite the fact that it is impossible to say where parties can draw the line on the imposition of litigation holds, what follows is a short list of events that should lead to the imposition of a litigation hold:

- A draft complaint, whether filed or not;
- Requests for production of documents;
- A subpoena from a third party;
- A request to preserve specific documents;
- A complaint filed with or by a regulatory agency;
- A written demand letter from a lawyer for a party that makes a claim and proposes a resolution, clearly threatening litigation if no resolution is reached.

If litigation is threatened or a party receives a demand letter, that party should ask the following questions:

- How specifically do the communications with the other party describe the circumstances which led to the demand? Are the specifics correct?
- How credible is the demand?
- Who authored the demand letter, and what is his/her role?

[33] Zubulake IV, 220 F.R.D. at 216-17.
[34] TODD L. NUNN, ET AL., UNDERSTANDING THE NEW E-DISCOVERY RULES 20 (DRI 2006).

- Who is the communicator for the other party and to whom are they writing? Is the communication to or from attorneys?
- How explicit and credible is the threat of litigation?

The duty to impose a litigation hold can also come from a third party source, such as a news media report. To determine if a litigation hold should be imposed based on such sources, parties should ask:

- How reliable and accurate is the source?
- How widespread are such reports?

On the other hand, if you are the party contemplating litigation, you should ask yourself the following questions:

- Who within your organization knows anything about the proposed litigation? Does that individual have authority to sue? If not, have they told any decision-maker(s) about the facts which form the basis of the suit?
- Does legal counsel, whether in-house or outside counsel, know the facts and been asked for an opinion?
- Have any steps been taken towards filing suit, or communicating with other parties about the potential suit?
- Has there been any research on a demand letter or has one been sent?[35]

The determination of the timing of pre-litigation preservation decisions requires a fact-sensitive analysis. Indeed, an organization may have to make a decision to preserve documents years before an actual lawsuit is instituted.[36] Therefore, if after considering the facts at issue, the parties involved, the relationship between the parties and the potential for the dispute to rise to the level of a formal complaint, an organization is seriously considering whether documents may

[35] Id. at 21.

[36] Zubulake IV, 220 F.R.D. at 216-17 (S.D.N.Y. 2003) (UBS reasonably anticipated litigation five months before the filing of the EEOC charge (and a few years prior to the filing of a civil complaint) based on the e-mail of several employees revealing that plaintiff intended to sue); Stevenson v. Union Pac. Ry. 354 F.3d 739 (8th Cir. 2004) (railroad reasonably knew that fatal crashes usually lead to litigation).

require preservation in connection with anticipated litigation, then chances are a litigation hold letter or preservation notice is warranted.

2. **The Essential Elements of an Effective Litigation Hold Letter**

Once an organization makes a determination that it is under a duty to preserve documents, it must notify its employees in writing, detailing what types, and for what time period, documents must be preserved. A litigation hold letter or preservation notice, serves the purpose of directing a party to protect from destruction certain documents and data that are, or could possibly be, relevant to a threatened or pending litigation, regulatory investigation or audit. One commentator has defined the litigation hold letter as:

> …a written directive to all potentially relevant personnel of a company advising them that there is a specific subject matter which has resulted or is likely to result in litigation, to describe that subject matter, and the people involved in it, in sufficient degree to inform the recipients of the communication of the true nature of the actual or anticipated dispute, and then to specifically advise them to both locate and save all relevant paper documents, e-mails, and any other items that may be contained in the company's computer system. [37]

In drafting an effective litigation hold letter, organizations must be aware that this letter must be read and understood not only by employees or third parties but perhaps by adversaries and the court should the matter evolve into litigation. In fact, the letter must be understood by a broad corporate audience, from the mailroom to the board room while at the same time contain the necessary elements required by courts to ensure that organizations have taken all necessary steps to comply with any discovery obligations. Therefore, the key is to craft a letter that is straightforward and simple yet maximizes compliance and thereby reduces the risk of evidence

[37] Timothy J. Hagan, *The International and Domestic Implications of Electronic Discovery on Litigation and Business Practices*, International Legal News, vol. 2 at 7 (June 10, 2005).

destruction. In order for the letter to be effective the following guidelines should be followed in drafting an internal litigation hold letter:

1. **The letter should be sent by high level corporate officers such as the company Chairman, Chief Operating Officer or General Counsel**. This emphasizes that the obligation to preserve documents is recognized as important by the highest levels of the company and that company management is aware of and endorses the process. As the Prudential case made clear this obligation cannot be delegated in any event.

2. **It should be sent to the appropriate corporate audience.** It is not necessary, especially in larger corporations, for the litigation hold letter to be directed to all employees. However, it is vital that the letter be disseminated to those employees and departments that could potentially have access to relevant information. When the issues in dispute have not been clearly defined or the company is unaware of all the potential issues that may arise, it is advisable to err on the side of broader dissemination.

3. **It should be simple and straightforward.** In order to ensure that employees will read and understand the mandate to preserve documents, an internal hold letter should not exceed five or six brief, plainly worded, and easily understood paragraphs. The first or second paragraph of the letter should simply and clearly tell the employee what the subject matter at issue is, the nature of the litigation or investigation and that all documents and data, electronic or otherwise, relating to that issue, should be carefully preserved.

4. **It must define what needs to be preserved and where it might be located.** This is likely one of the most important elements to the letter. The hold letter should define the term "documents and data" and the potential "sources" of where the data may be stored, in order for the employee to understand the broad scope of the obligation. More importantly, this reminds the employee that documents are not relegated merely to paper documents but include a wide-range of electronic documents and sources, including back-up tapes.

5. **It must give clear direction to the audience.** Employees must be made aware of exactly what steps need to immediately take place in order to ensure the proper preservation of documents.

6. **Inform and identify for the audience the risks of non-compliance.** Employees must also be made aware of the importance of preserving documents and the risks or serious consequences to the company if the data is intentionally or unintentionally, lost, destroyed or compromised.

7. **Advise the audience of the continuing duty to preserve documents and the company's continued follow-up.** The litigation hold letter is only effective if employees understand that this is a continuing obligation. Moreover, they must be made aware that management and its legal counsel (in-house and/or outside) will be following up on the employee's preservation efforts. There must be an established follow-up protocol. A litigation hold will only be effective if there is continuous follow-up by management and its counsel.

As evidenced by the Prudential case, having a preservation notice or litigation hold in place is not enough, it must be disseminated to all employees who could potentially have access to relevant information in connection with the pending or anticipated litigation. Because of the globalization of business, special attention should be paid to information that may be held in locations outside of the United States, where other countries may have laws that conflict with U.S. discovery requirements. For example, the European Directive 95/46/eC (the "Directive"), effective October, 1998, governs the processing and use of personal data for all EU Member States, and identifies eight data protection principles. This includes the principle that personal data shall not be kept for longer than is necessary for the purposes for which it is processed. It also states that personal data shall not be transferred to a country or territory outside of the EU, unless that country or territory ensures an "adequate" level of protection for the rights and

freedom of data subjects in relations to the processing of personal data.[38] Whenever the laws of the EU or individual members thereof conflict with obligations in the U.S., those questions should be put to the U.S. court to determine the proper course of action. Otherwise, if a party makes its own choice, and a U.S. court disagrees with that course of action, a party may potentially be exposed to sanctions.

An even bigger hurdle may be the underlying differences in the judicial systems. Most of Europe has adopted rules of disclosure under which parties are not typically required to produce a large volumes of documents, while in the United States, parties can request that their adversaries turn over any "relevant" documents.[39] There are differences among the individual nations of the EU as well. For example, it is illegal in Germany to examine e-mails an employee marks private without the permission of the employee.[40] Yet in the United States, e-mails are considered the property of the employer. When faced with litigation in the United States every party must remember that there may be different rules with which it must become familiar, some of which may conflict with the laws of the home forum. As the cases in this area demonstrate, a party's decision whether to issue a litigation hold letter and the proper steps to affect a hold will be highly scrutinized if any evidence is alleged to have been lost during the course of a litigation.

B. The Scope of the Duty to Preserve: What Data is Potentially Relevant?

Once a potential party imposes a litigation hold, or has been served with a complaint or a demand to preserve documents, it must determine what data to retain. United States courts do not expect businesses, especially large organizations, to save every bit of data that passes through

[38] The Sedona Conference, Commentary on Legal Holds, the Trigger & the Process, Sedona Conference Working Group on Electronic Document Retention & Production (WG1) (August 2007 Public Comment Version), Guideline 6 "When a duty to preserve arises, reasonable steps should be taken to identify and preserve relevant information as soon as practicable. Depending on the circumstances, a written legal hold (including a preservation notice to persons likely to have relevant information) may be issued," available at www.thesedonaconference.org.

[39] Matthew Blake, The Perilous Journey of Overseas E-Discovery, available at www.discoveryresources.org/pdfFiles/blake_022006.pdf.

[40] Id.

its operations, recognizing that such a requirement would cripple the business.[41] Courts do require that businesses identify *what* documents are relevant, and *who* are the relevant persons. Thus, for example, in an employment discrimination case, while quarterly profit forecasts would not be relevant, e-mails most likely will be. And while e-mails may be relevant, only e-mails sent to and from relevant persons need to be preserved, rather than all company-wide e-mails.

The Rules guide the exchange of ESI after litigation has begun, requiring litigants to give the other parties any ESI that it plans to use to support its position.[42] The Rules do allow parties to withhold from production any document which may be subject to an evidentiary privilege, such as attorney-client privilege.[43] Even if information subject to a privilege is turned over, the party that inadvertently released the information can demand that the party that received the information destroy any copies made and return the ESI.[44] Parties can also withhold ESI that is difficult to access, either in terms of effort or expense.[45] This ground for withholding ESI is explored more thoroughly in the next section.

Before producing ESI to another party, litigants must review what data should be released. The first step is determining where potentially relevant data may be located. ESI can be divided into five different categories:

- Active, online data, such as hard drives, which are easily accessible.
- Near-line data, usually meaning a robotic storage device which houses removable media, and uses robotic arms to access the data.

[41] Zubulake IV, 220 F.R.D. at 217.
[42] F.R.C.P. 26(a)(1)(B)(2006); F.R.C.P. 26(a)(1)(A)(ii)(2007).
[43] F.R.C.P. 26(b)(5)(A)(2006); F.R.C.P. 26(b)(5)(A)(2007).
[44] F.R.C.P. 26(b)(5)(B)(2006); F.R.C.P. 26(b)(5)(B)(2007).
[45] F.R.C.P. 26(b)(2)(B)(2006); F.R.C.P. 26(b)(2)(B)(2007).

- Offline storage or archived data, which is typically stored on a removable optical disk or magnetic tape media.
- Backup tapes.
- Erased, fragmented or damaged data.[46]

Each of these categories of data must be considered when a party is investigating where potentially relevant data is located. The next step should be determining who are the "key players" in the impending or current litigation. "Key players" are those employees who are likely to have relevant information.[47] This is a critical step in the process. Determining who is a "key player" is obviously situation dependent, but should be relatively clear with each situation. For example, in Zubulake, the "key players" were Zubulake's co-workers at the Asian Equities Sales Desk, including the head of the Desk.[48] Potential parties should err on the side of caution when making this determination as it is not worth risking possible sanctions down the road.[49] Potential parties must be proactive in this area, and "key players" who are known should be interviewed so that other "key players" can be identified.

Once the "key players" have been identified, a potential party should determine what data to preserve. Parties must preserve anything that was created by or on behalf of any of the "key players," and any other data which refers in any way to the subject of the current or impending litigation. Further, while a party need not search inaccessible data for potentially relevant ESI, if it does know or becomes aware that potentially relevant ESI exists on inaccessible data, that data must be preserved.[50] Again, it is best to err on the side of caution when determining what data to

[46] Zubulake v. UBS Warburg, L.L.C., 217 F.R.D. 309, 318-19 (S.D.N.Y. 2003) ("Zubulake I").
[47] Zubulake IV, 220 F.R.D. at 218.
[48] See generally, Zubulake III, supra.
[49] See *infra* Section IV.
[50] Zubulake IV, 220 F.R.D. at 218.

preserve. As a rule of thumb, anything that can contain any potential relevance to an impending or current lawsuit must be preserved.

When searching for potentially relevant data, parties must look not only at the ESI within its possession, but also within its control. Thus, if a party contracts with a third party to store its data, or uses a third party to run its web servers, the information held by those third parties is under its control, and must be searched for potentially relevant data.[51] In Columbia Pictures Industries v. Bunnell et al., the defendant was alleged to have infringed on the copyrights of the plaintiff by running a file sharing service over the internet, allowing users to download movies.[52] The defendant used the servers of a third party that stored information, including movie files, that were downloaded by users.[53] The defendant argued that the files on those servers were not discoverable because they were not within the defendant's possession. The court rejected this argument, holding that, because the defendant had control and access to those files, it was required to preserve and produce them on request.[54] As Bunnell illustrates, the rule in this area is to leave no stone unturned. Wherever a party may store data, so long as it is accessible, and under the control or possession of that party, it must be identified, located, and searched.

Once a party has determined the "key players" and what data it must preserve, it must determine how to preserve it. Parties can choose how to preserve data identified as potentially relevant. There are some general guidelines that parties should follow when determining how to preserve the data. Making mirror image copies of the data will always be acceptable. Simply retaining the data in its present form is also acceptable. Parties should not alter data in any way,

[51] See Columbia Pictures Indust. v. Bunnell et al., 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. June 19, 2007).
[52] Id. at *8-16.
[53] Id.
[54] Id. at *55.

as this will likely lead to sanctions and penalties being imposed once the data is disseminated in litigation.[55] Therefore, retaining the integrity of the original document is vital.

C. Who bears the costs of producing the ESI?

Once a party is aware of how the data must be released, parties often become concerned over the cost of such productions. In fact, the cost of discovery is often the most important consideration by parties when considering entering into, and settling lawsuits. For many productions of ESI, the cost will be similar to, if not less than, the cost of a production of paper discovery. ESI is more easily searched than paper documents, and can, in many cases, be collated and stored more quickly with less man power. This is only true, however, when the data is easily accessed and searched.[56] When the data is stored on backup tapes, or on other medium which must be restored in order to be fully searched, the time and expense of producing data located on such medium can grow exponentially.

The Federal Rules allow for a party to object to producing ESI if it can demonstrate "undue burden or cost." [57] For the most part, even if a party can show that producing the requested ESI will impose too great of a burden or cost, courts will still order the production, although they may shift the cost of that production to the party requesting the data. Parties must remember that courts will not shift the cost of production in every case.[58] Courts first apply a seven part test to determine whether the request imposes an undue burden or cost, making cost shifting appropriate:

1. How specifically does the request ask for ESI that will likely be important in the litigation?

[55] See *infra* Section IV.
[56] See *supra* text accompanying note 46.
[57] F.R.C.P. 26(b)(2)(C)(2006), F.R.C.P. 26(b)(2)(B)(2007).
[58] Zubulake I, 217 F.R.D. at 318.

2. Can the ESI being sought can be obtained from other sources?
3. How much will the production cost, compared to the amount of damages the plaintiff claims?
4. How much will the production cost, compared to the cost of production with the resources available to each party?
5. What is each party's ability to produce the data as cheaply as possible, and what is their incentive to do so?
6. What issues will the data go to, and how important are those issues in the litigation?
7. What are the relative benefits to each party of getting the information?[59]

The most important factors a court will look at are the specificity of the request and whether the information can be obtained from any other source. What courts are looking for is the likelihood that the requested discovery contains the data sought. The more likely it is that the ESI has the information desired, the more likely it is that courts will require the responding party to pay the cost of the production.[60] If a court determines that there is a low probability that the requested ESI does not contain the information sought, then it will look at the next three factors, which seek to answer the questions of how expensive the production will be and which party is in the best position to handle the cost.[61] The remaining factors are of relatively little importance and rarely come into play.[62]

[59] Id. at 322, see also Notes of the Advisory Committee on 2006 Amendments ("Advisory Committee Notes"), F.R.C.P. 26.
[60] McPeek v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001).
[61] Zubulake I, 217 F.R.D. at 323.
[62] Id.

Following this analysis, courts have come to different conclusions about when to order a requesting party to bear the cost of production. Some courts will order a limited production, or "sampling", to determine what, if anything, will be found. Only if, after the "sampling", it appears that a further search is of any utility, will a complete production be ordered.[63] Other courts will order the production, but shift only a portion of the cost to the requesting party.[64] Some courts will shift the entire burden to the requesting party, when the disparity between the resources of the two parties is great, and the chances that the sought after data exists in the requested ESI. While the seven factor test has no presumption either for or against cost shifting, in practice, there must be quite a low likelihood that the requested ESI contains the sought after data, and a large disparity between the resources of the parties, for a court to order a total shifting of cost. Responding parties must be aware that they will likely still shoulder quite a bit of the cost for any requested production. Notwithstanding, they should also be aware that the cost of the production is less than that of any sanctions that may be imposed for not producing, or altering, the requested ESI.

D. Post-Litigation Procedures

While the Rules explain in what form ESI can be produced, parties are encouraged to come to their own agreements about how ESI may be produced.[65] When a request for the production of ESI is made, the requesting party can ask that the ESI be turned over in a specific form.[66] The party receiving the request can object to the requested form of the ESI, but must give reasons why it is objecting and what form it intends to use.[67] If no specific form of ESI is

[63] Hagemeyer N. Am., Inc. v. Gateway Data Scis. Corp., 222 F.R.D. 594, 603 (E.D. Wisc. 2004).
[64] Zubulake v. UBS Warburg, L.L.C., 216 F.R.D. 280, 289 (S.D.N.Y. 2003) ("Zubulake III"); see also Wiginton v. C.B. Richard Ellis, Inc., 229 F.R.D. 568, 577 (N.D. Ill. 2004).
[65] Parties are encouraged to discuss discovery of ESI during the discovery-planning conference and reach agreement on the forms of production. Advisory Committee Notes, F.R.C.P. 26(f).
[66] F.R.C.P. 34(b)(2006); F.R.C.P. 34(b)(1)(C)(2007).
[67] F.R.C.P. 34(b)(2006); F.R.C.P. 34(b)(2)(D)(2007).

requested, and there is no agreement between the parties governing the form of ESI to be produced, then a party which is producing ESI must produce it in the form in which it is usually maintained, or a form that can be used by the requesting party with relative ease.[68]

Pitfalls, however, abound when producing ESI absent an agreement on the form of the production. Courts will not hesitate to penalize parties who attempt to gain an advantage by producing ESI in a manner which is difficult for the other parties to use. Even production of ESI in paper form is not always appropriate. In In re Bristol-Myers Squibb Securities Litigation,[69] the parties agreed on a ten cents per page charge for copies during discovery.[70] The court vacated the agreement, however, upon the revelation that the defendant was producing electronic documents in paper form.[71]

While the Rules mandate a pre-trial conference between the parties and a judge to arrange for a schedule of discovery, the parties are encouraged to make their own arrangements prior to this meeting. The best way to prepare for such meetings is to meet with a representative from the Information Technologies department in order to become more familiar with the terminology and technology at issue. It is also a good idea to plan on deposing a representative of the other party's Information Technology department, so that the ESI received from that party can be used in the most efficient and productive way.

IV. Consequences of Non-Compliance

Failure of a party to abide by the discovery obligations, may give rise to legal and economic sanctions. Potential sanctions for non-preservation or spoliation include: dismissal of claim or granting judgment in favor of a prejudiced party, suppression of evidence; and adverse

[68] F.R.C.P. 34(b)(2006); F.R.C.P. 34(b)(2)(E)(2007)
[69] 205 F.R.D. 437 (D.N.J. 2002).
[70] Id. at 439.
[71] Id. at 440-41.

inference or spoliation inference; fines, and attorneys' fees and costs. In addition, courts may order the re-production of ESI if the initial production is not in the proper form. While not a sanction per se, the cost of production can be staggering. By one estimate, a typical hard drive storing up to 9,000,000 pages cost more than $1,000,000 to produce.[72]

There are many examples of the consequences to companies who fail to comply with the obligations arising from the preservation of electronically stored information. For example, in Coleman Holdings v. Morgan Stanley & Co., a $1.45 billion verdict was entered against Morgan Stanley arising from its inability to recognize substantial shortfalls in e-mail production when it represented that all responsive e-mails were produced. [73] In response to the plaintiff's initial request for discovery, Morgan Stanley produced only 8,000 pages of documents, including only a handful of e-mails.[74] The court ordered Morgan Stanley to preserve ESI and do a more thorough search of its records.[75] After certifying that it had complied with the order, Morgan Stanley revealed that it had discovered about 1,000 backup tapes which had not previously been disclosed.[76] As a consequence, the court ordered that the burden of proof at trial would be shifted from the plaintiff to the defendant, and a statement to the jury of Morgan Stanley's efforts to hide its e-mails.[77] The court entered default judgment against Morgan Stanley, leaving only the question of damages for a jury, which awarded Coleman Holdings $1.45 billion.[78] While the judgment, including the award of punitive damages, was later reversed on grounds unrelated to

---

[72] Sarah Michaels Montgomery, *E-discovery: Aligning Practice with Principles*, THE SCITECH LAWYER, Fall 2007, at 12.

[73] Coleman Holdings v. Morgan Stanley & Co, 2005 Extra LEXIS 94 (Fla. Cir. Ct. Mar. 23, 2005). The court found that Morgan Stanley made misrepresentations in a court-ordered "Certificate of Compliance," failed to properly account for "newly discovered" network backup tapes, failed to produce attachments to e-mails, and failed to properly perform electronic text searches when looking for responsive documents.

[74] Id. at *4.

[75] Id. at *8

[76] Id. at *14-15.

[77] Id. at *15.

[78] Id. at *33-34.

the electronic discovery issues (which were not discussed by the appellate court), the trial court's rulings and the jury's findings serve as a good example of the potential impact of electronic discovery abuses.

In the leading case of Zubulake v. UBS Warburg,[79] the court imposed sanctions against UBS Warburg and admonished counsel and client by quoting the classic line from the movie Cool Hand Luke, "What we've got here is a failure to communicate." The court spoke at length on the need for counsel to interface extensively with IT personnel to "become fully familiar with her client's . . . data retention architecture," and emphasized that counsel and client's failure to do so played a large role in the sanctions that ultimately led to the $29 million verdict against the investment firm.

In a more recent case between Qualcomm and Broadcom, communications companies involved in a patent infringement litigation, a judge ordered Qualcomm to pay Broadcom's attorney's fees of $8.5 million. At trial, a witness revealed the existence of 21 e-mails that had not been produced by Qualcomm. The revelation led to the discovery of hundreds of thousands of relevant documents that had not been produced. Significantly, an attorney for Qualcomm falsely gave the judge the impression that he was unaware of the 21 e-mails. After Broadcom prevailed at trial, the judge ordered that Qualcom should also pay Broadcom's attorney's fees.[80] A decision has not been made on what, if any, sanctions will be imposed on the attorneys for Qualcomm.[81]

The most severe sanctions are imposed when there has been spoliation of evidence. Spoliation of evidence is the destruction or significant alternation of evidence, or the failure to

[79] Zubulake v. UBS Warburg, 229 F.R.D. 422 (S.D.N.Y. 2004) ("Zubulake V").
[80] Jessie Seyfer, *Judge: Qualcomm Firms Can Disclose Work Product*, THE RECORDER, October 1, 2007, available at www.law.com.
[81] Jessie Seyfer, *Day Casebeer Partner Is Central to Qualcomm Discovery Mess*, THE RECORDER, October 4, 2007, available at www.law.com.

preserve property for another's use as evidence in pending or reasonably foreseeable litigation.[82] The consequences of spoliation are seen in the Morgan Stanley and Zubulake cases. In Thompson v. United States Department of Housing and Urban Development,[83] a class action suit alleging racial discrimination in urban housing, the court noted that the Rules allow for such "draconian" sanctions that are often "case determinative."[84] In that case, the plaintiffs sought to bar the calling of witnesses whose e-mails had not been produced by the defendant.[85] The court noted that, after finding that spoliation had occurred, it is left to the court's discretion what sanctions to impose.[86]

Where spoliation is egregious, courts will impose an adverse inference that can be used against the wrongdoer at trial. A party seeking an adverse inference based on spoliation must establish: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed 'with a culpable state of mind'; and (3) that the destroyed evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense."[87]

In Jane Doe v. Norwalk Community College,[88] a Connecticut community school was sanctioned for discovery misconduct and spoliation of evidence for its destruction of electronic data. The plaintiff in this gender discrimination case sought an adverse inference against the defendant for completely erasing the hard drives of key witnesses.[89] The court allowed an adverse inference against the school at trial, specifically, the presumption that the destroyed

[82] Mosaid Technologies, Inc. v. Samsung Elecs. Co., Ltd., 348 F. Supp. 2d 332, 335 (D.N.J. 2004) (citing Zubulake V, 229 F.R.D. at 430).
[83] 219 F.R.D. 93 (D. Md., December 12, 2003).
[84] Id. at 102.
[85] Id. at 96.
[86] Id. at 100.
[87] Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 107 (2d Cir. 2002).
[88] 2007 U.S. Dist. LEXIS 51804 (D.Conn., July 16, 2007),
[89] Id. at *5.

evidence was unfavorable to the school's defense, and awarded the costs of the motion to the plaintiff.[90]

Other options are also available to courts. Recently, a district court in the District of Columbia ordered the solicitation of bids from forensic computer technicians to assess whether the search and restoration of additional data from defendant's company computer was justified under F.R.C.P. 26(b)(2)(c).[91] In Peskoff v. Faber, the plaintiff sought e-mails received or authored by him, which the defendant claimed no longer existed.[92] Despite the fact that there was an archive of all electronic documents on the plaintiff's hard drive at the time he left the defendant's company, the defendant claimed that no e-mails existed for a two year period.[93] Because this time period pre-dated the litigation, the court found that the defendant was not obliged to preserve those documents.[94] There was no doubt that the information sought was relevant, and the court determined that a forensic search of the defendant's computers was in order, to ascertain what, if anything, remained.[95]

Court's have imposed an expansive net over a party's obligation to preserve responsive ESI and an adversary's access to same. This does not mean that a party has unfettered access to his adversary's electronic databases. In fact, courts have held that the Rules generally do not give the requesting party the right to search the responding party's records. [96] Notwithstanding, the above examples illustrate the importance of developing reliable resources to navigate the corporate infrastructure, as well as the risks associated with "going it alone" or, even worse,

---

[90] Id. at *30.
[91] Peskoff v. Faber, 2007 U.S. Dist. LEXIS 62595 (D.D.C. August 27, 2007).
[92] Id. at *1-2.
[93] Id. at *2.
[94] Id. at *21.
[95] Id. at *25.
[96] In Re Ford Motor Co, 345 F.3d 1314, 1317 (11th Cir. 2003); see also Butler v. Kmart Corporation, 2007 WL 240682 (N.D. Miss., Aug. 20, 2007) (stating that the 2006 amendments to the Federal Rules of Civil Procedure concerning electronically stored information do not disturb the validity of In Re Ford Motor Co.).

going with the wrong person. The same lesson is imparted by the changing rules, as federal and state rules of procedure require the identification of a contact person with extensive knowledge of IT systems to assist in coordinating discovery.

V. Best Practices Guidelines for E-Discovery

A. The Role of the Document Retention and E-mail Retention Policy

Now that the Rules explicitly include ESI, the distinction, or lack thereof, between "document" and "data" must likewise be addressed in corporate document retention policies. In the past, some organizations may have found such policies unnecessary. However, considering the sheer volume of data passing through most worldwide organizations, it is prudent to address data retention practices and formalize a written policy. In fact, in making a determination whether there has been "spoliation" or a "good-faith operation of an electronic information system," a court may examine the document/data retention policy in effect at the time.[97] For example, in Arthur Andersen LLP v. United States, the United States Supreme Court addressed the document retention practices of Arthur Andersen during the Enron investigation.[98] The accounting firm's policy, even after the recognition of an impending investigation and litigation, allowed for the destruction of documents that could be relevant.[99] In that case, the continued destruction of documents in the face of knowledge of an impending investigation and litigation led to the criminal indictment of Arthur Andersen.[100]

While most cases will not lead to criminal liability, Arthur Andersen, LLP illustrates the dangers that abound when companies do not give the proper attention to their document retention

---

[97] Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005); see also Samsung Elecs. Co. v. Rambus Inc., 439 F. Supp. 2d 524 (E.D. Va. 2006); Hynix Semiconductor, Inc. v. Rambus, Inc., 2006 U.S. Dist. LEXIS 30690, 2006 WL 565893, *20 (N.D. Cal. 2006).
[98] Arthur Andersen LLP, 544 U.S. at 699-700.
[99] Id. at 700-01.
[100] Id. at 702.

programs. Rule 37(f) explicitly requires courts to analyze whether the loss or alteration of ESI occurred as the result of "routine, good-faith operation" of the system. While this language allows a company to continue using its normal procedures, absent notice of impending litigation, it does not absolve companies from being watchful for signs that they may become embroiled in litigation. Significantly, this safe-harbor provision under Rule 37(f) does not relieve a party from sanctions for the loss or alteration of evidence which occurred pursuant to a retention policy.

Therefore, it is of critical importance for companies to understand how each of their systems manages and ultimately deletes data. Without an understanding of the infrastructure and internal operating system, a party may find itself unable to create, update and implement an effective policy. Competing interests between the IT and legal professionals can be expected. Therefore, an organization's legal team and IT professionals must work together in the creation or updating of a policy and, more importantly, in its ultimate implementation. IT staff responsible for implementing document retention policies with respect to ESI may not even be aware that there is an obligation to preserve ESI that they destroy on a routine periodic basis. Failure to notify responsible IT staff of what ESI must be preserved so that ESI is not destroyed could subject a company to sanctions.[101]

For example, it is common for network and server accounts to be disabled; e-mail accounts to be disabled; and voice mail accounts to be deactivated when an employee leaves an organization. Sometimes the disabling of these accounts will result in, or be accompanied by, destruction of ESI associated with those accounts. Individual PCs may be "recycled" and reissued to another employee or even disposed of and all the ESI on the PC may be destroyed as a result. Importantly, ESI, unlike physical records, is also subject to automatic destruction without any explicit action. Network and computer log files are usually limited by time or size

[101] Kier v. UnumProvident Corp., 2003 U.S. Dist. LEXIS 14522 (S.D.N.Y. Aug. 22, 2003).

so that new activity overwrites old activity. There may be a need to suspend the automatic destruction of ESI so that discoverable ESI that is subject to preservation obligations is not inadvertently destroyed.

Remember that a document retention policy tells a story that may be subject to the scrutiny of hindsight in the event that information that once existed is unavailable during litigation or other legal proceedings. Therefore, the policy should accomplish at least four goals: (1) identify subject documents; (2) embody legal objectives; (3) identify specific time periods for retention; and (4) explain processes and lines of responsibility in clear unambiguous terms. More importantly, the policy must be realistic and enforced. However, merely having a policy in place will not provide a safe-harbor to an organization that may be faced with discovery sanctions. In this context, an organization will have to demonstrate its good-faith operation of an electronic information system, that a well-reasoned document retention policy is in place and that all persons relevant to its enforcement are properly trained.

The document retention policy is a double-edged sword in that its proper creation and implementation can protect a party from sanctions; but an ill-advised policy or one not properly followed can, in fact, create the record to support a claim of failure to act "in good faith." In this regard, the most important aspect of the policy is the section that provides for suspension of that very policy, the litigation hold or preservation notice. Although at first glance companies may not want to expend the effort and resources on amending or adopting a document retention policy that anticipates a litigation hold, it is undoubtedly worth the effort when compared to the ramifications of not doing so.

B. E-Discovery Liaison

Soon after litigation has begun, parties will begin exchanging discovery, including ESI.[102] Federal courts expect parties to work amongst themselves and agree about what ESI will be turned over, and in what form. As stated above, the Rules now requires parties to identify and resolve differences related to disclosure or discovery of ESI (including format of production) in advance of the initial conference with a judge that results in a discovery scheduling order. Each party should appoint an e-discovery liaison, through whom all e-discovery requests and responses are channeled.[103]

An "e-discovery liaison" is an individual through whom all e-discovery requests and responses are channeled.[104] The liaison can be an employee, an attorney or a third party consultant, and should know the systems a party uses, as well as the mechanics of e-discovery.[105] Besides organizing a party's e-discovery, the liaison should also be able to participate in e-discovery dispute resolutions.[106] Many states have codified similar procedures within their rules, and some courts, such as the U.S. District Court for the District of New Jersey, go further by requiring parties to identify an "e-discovery liaison" to assist counsel in the preliminary stages leading up to the initial conference with the court.[107] Although not mandated by the federal rules, companies should seriously consider the implementation of this role before the next lawsuit arises.

One of the biggest issues with which a liaison is a benefit is determining precisely what must be turned over. Besides concerns over whether various evidentiary privileges may apply to

---

[102] F.R.C.P. 26(a)(2006), F.R.C.P. 26(a)(2007).
[103] Model Order Governing the Exchange of Electronic Discovery, District Court for the Eastern District of Pennsylvania, available at www.paed.uscourts.gov/documents/procedures/savpol6.pdf.
[104] Id.
[105] Id.
[106] Id.
[107] District of New Jersey Local Rule 26.1(d)(1).

prevent the disclosure of some information, in the digital age, parties are also concerned about the form of ESI to be turned over. For example, a party may wish to turn over a hard copy (print out) of ESI, but doing so obscures some of the data contained in the digital form, such as a spreadsheet. Can a party turn over the hard copy, or must it turn over the digital file? And if it must turn over the digital file, can it make any alterations to the data before turning it over? Must it obtain permission from the court before doing so?

The selection of the individual for this role should be thought out and not merely a "front person." First, the liaison should be knowledgeable enough to present an inventory of the active corporate systems that store and manage all information, as well as obsolete (legacy) systems, backup and archive media for the time period that counsel deems relevant. In addition, there should be a discussion of network or system "settings" that affect storage and deletion of data, such as dated e-mails and attachments. The extent to which settings are changed, even if such changes increase costs, should be a dialogue with consideration of legal and other business concerns.

Some consideration should be given to the liaison's effectiveness as a witness. As discovery focuses more on technology, a subject alien to many attorneys and judges, the quality and quantitative depth of the individual explaining such issues will influence the success rate of the litigation. It is worth noting here that a trend is developing where courts are suggesting that counsel be accompanied by IT professionals when meeting with adversaries and/or the court to resolve discovery disputes, even if the input from the professional is provided off the record, confidentially or *in camera*.

Finally, it is important to recognize that the creation of a reliable contact or network of contacts within the IT ranks is neither a distraction nor an added expense. If properly prepared

and engaged, the e-discovery liaison is an investment in an enduring resource that is likely to yield substantial economic returns by reducing litigation costs and exposure. Even better, the institutionalization of electronic discovery resources and a litigation response plan will reap greater benefit with cases, as storage and processes are streamlined and data are reused (and already authenticated) when overlapping facts arise in separate suits. Perhaps the best benefit of all is that the company will be prepared, and its processes will be defensible.

VI. Conclusion

While modern companies face daunting challenges when managing their ESI, successful administration of electronic systems can be achieved with proper preparation. The examples of sanctions and large judgments in this paper are reminders of what happens to companies that do not properly consider potential litigation when designing their document retention systems. Corporations must form a working group made up of executives, attorneys and representatives of the IT department. This working group should create a document retention policy to disseminate to all employees. The policy must outline situations and events which could lead to potential litigation. It should inform all employees that they should report such events to a member of the working group. The policy should include procedures for putting a litigation hold on ESI which may be relevant in any possible litigation, including what computer systems will be used to store information which would otherwise be deleted in the normal course of business. The policy should also provide guidance on how to proceed once a complaint has been filed, including the identification of "key players" and relevant documents. The policy should indicate what procedures will be used for the production of ESI, the formation of any agreements about production with other parties in litigation, and what forms of ESI should be requested from other parties.

It goes without saying that litigation is an expensive prospect for any organization, small or large. However, with the right policies and procedures in place, companies can greatly reduce the likelihood of large sanctions or judgments. Accordingly, we strongly recommend that you carefully review your policies, procedures and practices regarding electronic data. E-discovery issues arise in every case. The difficulty and daunting challenges emerge in determining how to deal with the issues in cases that have varying fact patterns and varying amounts in controversy. Importantly, organizations need to overcome the "language barrier" between IT and legal that occurs from the discussion of technical issues. There must be a proper understanding of the obligation of preserving electronic data in anticipated or pending litigation or regulatory investigation. An important factor for organizations is to learn to manage the rising costs of electronic discovery including the design of an electronic data strategy for responding to discovery requests which include narrowing the scope to relevant data; avoiding undue burden or expense; and seeking cost shifting as appropriate. Finally, and most importantly, businesses must develop best practices in dealing with the emerging and changing issues of electronic discovery.