

**MEETING YOUR COMPANY’S
ELECTRONIC DISCOVERY OBLIGATIONS**

Thomas A. French*
William C. Boak

TABLE OF CONTENTS

I. INTRODUCTION	2
II. LEGAL REQUIREMENTS FOR ELECTRONIC DISCOVERY	5
A. When is the Duty to Preserve Triggered and what is the Scope of the Duty?	5
B. The E-Discovery Process under the Rules.....	7
1. Rule 26(f) Conference of the Parties to Plan for Discovery	7
2. Rule 26(a) Initial Disclosures.....	8
3. Rule 16 Pretrial Conference and Scheduling Order	8
4. Discovery/Subpoenas	8
a. Rule 34 Requests for Production of ESI	8
b. Rule 33 Interrogatories	9
c. Rule 45 Subpoena	9
5. Inaccessible ESI: Shifting the Cost to Your Opponent.....	10
6. Motions to Compel or for Sanctions	11
7. Asserting claims of Privilege or Work Product Protection.....	12
C. The E-discovery Process in Pennsylvania	13
III. ESTABLISHING A SUCCESSFUL E-DISCOVERY PLAN	14
A. Creating an Electronic Records Management and Retention Policy.....	14
B. Legal Holds.....	15
C. Collection, Review, and Production of ESI	17
IV. RECOMMENDATIONS FOR GETTING STARTED.....	21
V. CONCLUSION.....	22

* Thomas A. French has litigated civil cases in federal and state courts for over 25 years. He has served on the adjunct faculty of Pennsylvania State University’s Dickinson School of Law and Widener University School of Law, and has lectured extensively on matters of civil litigation and trial practice. Mr. French is a founding member of the e-discovery practice group of Rhoads & Sinon, LLP.

William C. Boak is a 2006 magna cum laude graduate of Widener University School of Law where he was Executive Managing Editor of the Widener Law Journal. Prior to joining Rhoads & Sinon, Mr. Boak served as law clerk for the Honorable Thomas I. Vanaskie, United States District Judge for the Middle District of Pennsylvania.

For more information about Rhoads & Sinon LLP’s e-discovery services, visit www.rhoads-sinon.com.

I. INTRODUCTION

Companies large and small are finding themselves under the careful scrutiny of the federal courts. Some are being hit with expensive – sometimes multi-million dollar – sanctions and other adverse rulings.¹ Why? The answer would surprise many senior level executives and business owners. Courts are punishing companies for failing to comply with exacting requirements for disclosure of electronically stored information (“ESI”) when they become parties to civil litigation. In short, these companies are enhancing their risk of being found liable for damages, and are paying unnecessary attorneys fees and other financial sanctions, because they do not have plans and systems in place to enable them to comply with these discovery requirements.

According to a 2008 survey, 74% of all companies queried were sued at least once in the prior year, with 46% experiencing six or more new suits during the year.² Nearly one-third of corporate executives surveyed believed that litigation will continue to increase.³ Twenty percent of the billion dollar companies surveyed incurred over \$10 million in litigation expenses, during the prior year.⁴ Approximately sixty percent of all U.S. companies in the survey spent more than \$500,000 on litigation, in the year preceding the summary, with many spending between \$1 million and \$5 million.⁵

Significant within these litigation expenditures were the costs of complying with discovery obligations for ESI, placed upon all companies and other litigants by the Federal Rules

¹ See *Qualcomm, Inc. v. Broadcom, Inc.*, Case No. 05cv1958-B (BLM), 2008 U.S. Dist. LEXIS 911 (S.D. Cal. Jan. 7, 2008). In *Qualcomm*, U.S. Magistrate Judge Barbara L. Major ordered Qualcomm to pay \$8,568,633.24 as a sanction for “its monumental and intentional discovery violation.” *Id.* at *63. At trial, one of Qualcomm’s employees admitted to having received emails from a “standards-setting body,” a group Qualcomm had consistently denied any involvement with. *Id.* at *12, 18. Only days earlier Qualcomm’s trial team discovered the emails on the employee’s computer, but declined to produce the emails on the ground they were nonresponsive to Broadcom’s discovery requests, even though the emails undercut Qualcomm’s theory. *Id.* at *16-17. Furthermore, Qualcomm conducted no investigation, in the wake of this discovery, to determine if emails existed on other employees’ computers. *Id.* at *17. After trial, Qualcomm eventually searched the email archives of twenty-one employees and found over 46,000 documents that had been requested but never produced. *Id.* at *23. In concluding Qualcomm violated its discovery obligations, Judge Major rejected Qualcomm’s contention that its failure to produce was inadvertent. Qualcomm presented no evidence that it actually searched for these emails, and inexplicably, it was able to locate all emails helpful, or at least not harmful, to its case, yet could not find any emails prejudicial to its theory. *Id.* at *33-35. The number of employees receiving the emails also suggested it was incredible Qualcomm was unaware that the emails existed. *Id.* at *36. Finally, even if Qualcomm was unaware of the emails, there were enough warning signs to alert Qualcomm that its document search and production were deficient. *Id.* at *36-40. Because the evidence established Qualcomm intentionally withheld over 46,000 emails, which prolonged the litigation and increased its complexity, Judge Major concluded such conduct “justifie[d] a significant monetary award.” *Id.* at *60-62.

² FULBRIGHT & JAWORSKI, L.L.P., FIFTH ANNUAL LITIGATION TRENDS SURVEY FINDINGS 14 (2008) [hereinafter LITIGATION TRENDS SURVEY], available at <http://www.fulbright.com/litigationtrends41>. Fulbright & Jaworski commissioned an independent research firm to survey senior corporate counsel on their views and experience on litigation related matters. *Id.* at 2. A statistically significant sample of 358 respondents participated, including public and private companies ranging in revenues from under \$100 million to over \$1 billion. *Id.* at 6-7.

³ *Id.* at 9.

⁴ *Id.* at 22.

⁵ *Id.*

of Civil Procedure and the rules of some state courts. These requirements impose upon companies a duty to preserve ESI once the threat of litigation becomes reasonably known, a duty to make voluntary disclosures of relevant ESI at early stages of litigation, and an obligation to respond with reasonable completeness to discovery requests for ESI from litigation opponents.

Electronic discovery is more complex than traditional paper discovery, making it potentially much more expensive. According to one study, 92% of all new data is stored electronically, and 60% of all business critical information is stored within corporate email systems.⁶ In 2007, 92 billion emails were sent each day, worldwide.⁷ ESI is changeable and, unlike paper which can be destroyed, remains in existence even after it has been “deleted” from email systems or computer hard drives.⁸ A single email can be found on many computer hard drives and can have multiple recipients and secondary recipients. ESI can be found on many types of media, from cell phones and portable email devices such as a Blackberry™, to network servers and internet shared spaces. Each ESI communication also has non-obvious metadata attached to it. This metadata, not part of the communication usually seen by the sender or recipient, can show when a document was first created, whether and when it was altered, to whom it was sent and resent, what was attached to it, whether it was part of an email conversation thread, and other information.⁹ In some cases, not only must the actual ESI communication be retrieved and produced in discovery, all versions of the document, in its “native” or original format, with its unaltered metadata, may be requested.¹⁰

The consequences of failing to fulfill these discovery obligations can be devastating. Courts have imposed costly sanctions on litigation parties and their counsel for non-compliance. These sanctions have taken many forms, including orders to pay the opponent’s counsel fees,¹¹ prohibiting the introduction of favorable evidence,¹² instructing the jury to make an adverse inference or finding on an issue,¹³ and entering judgment against the non-complying party.¹⁴ In any significant litigation, the cost of e-discovery compliance, and the potential risk of loss associated with sanctions for non-compliance, is more than enough to justify the most careful attention to developing an effective e-discovery compliance program.¹⁵

⁶ COURTNEY INGRAFFIA BARTON, *THE DISCOVERY BOOK* 4 (2d ed. 2008) (citing SCHOOL OF INFORMATION MANAGEMENT AND SYSTEMS, UNIVERSITY OF CALIFORNIA, BERKELEY, *HOW MUCH INFORMATION?* 2003, <http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm>).

⁷ *Id.*

⁸ *Id.*

⁹ *Id.* at 5, 32.

¹⁰ *See, e.g., id.* at 33 (quoting *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 652 (D. Kan. 2005)).

¹¹ *See, e.g., De Espana v. Am. Bureau of Shipping, Inc.*, No. 03 Civ. 3573 (LTS)(RLE), 2008 U.S. Dist. LEXIS 62865, at *13-15 (S.D.N.Y. Aug. 18, 2008).

¹² *See, e.g., R&R Sails, Inc. v. Ins. Co. of the State of Penn.*, Civ. No. 07-cv-0998-H (POR), 251 F.R.D. 520, 2008 U.S. Dist. LEXIS 44552, at *24-25 (S.D. Cal. Apr. 18, 2008).

¹³ *See, e.g., Connor v. Sun Trust Bank*, 546 F. Supp. 2d 1360, 1376-77 (N.D. Ga. 2008).

¹⁴ *See, e.g., Columbia Pictures, Inc., v. Bunnell*, No 2:06-cv-01093 FMC-JCx, 2007 U.S. Dist. LEXIS 96360, at *24-25 (C.D. Cal. Dec. 13, 2007).

¹⁵ Trial attorneys are well aware of the costs and complexities of corporate e-discovery compliance. Unless the e-discovery process is carefully managed, the costs of meeting these obligations could exceed the defendant’s

How can companies reasonably comply with these discovery obligations? How can they consistently preserve documents when their email systems and other electronic devices on which ESI is stored are in constant use within their businesses? How can they reasonably search their systems in order to reliably find documents they are required to preserve and produce? How can a company's proprietary and privileged information be kept confidential? How can all of this be done while avoiding excessive cost?

Responsible company executive managements take these obligations and risks seriously and implement an e-discovery compliance program.¹⁶ Fortunately, there are a number of effective options available to meet this need. Software providers have developed and refined programs that allow companies to effectively place "legal holds" on their ESI and track the retrieval process. Other software assists companies in reliably conducting searches for responsive, discoverable documents. Industry standards for document management and search protocols have been developed and refined.¹⁷

Forward-leaning companies retain special outside counsel to assist in implementing an e-discovery program. These attorneys work with in-house counsel, IT directors, software vendors, and technology consultants to help companies develop document management and retention/destruction policies, and other policies, procedures, and training programs in order to prepare to meet their discovery obligations. Then, because they have become intimately familiar with their client's document management systems and e-discovery compliance programs, these counsel represent their clients in court whenever e-discovery issues arise.

Such attorneys will know from the developing body of case law how to fashion a discovery plan that can be shown to be reasonably reliable, will preserve non-discoverable

potential liability, leading some to conclude that aggressive e-discovery practice is a form of legal "blackmail" in some cases, LITIGATION TRENDS SURVEY, *supra* note 2, at 51 (quoting respondents' views on pretrial disclosures in light of e-discovery rules), and in other cases dissuades plaintiffs from bringing otherwise meritorious claims. On September 9, 2008, the Institute for the Advancement of the American Legal System and the American College of Trial Lawyers Task Force on Discovery released an Interim Report of the key findings of a survey they conducted of trial lawyers entitled the *2008 Litigation Survey of Fellows of the American College of Trial Lawyers*. According to the organizations' press release, the survey led to the following conclusions, among others:

- The broad legal system – while not broken – is in need of substantial repair; deserving cases are not brought because they fail a rational cost-benefit test (85% believe litigation in general and discovery in particular are too expensive);
- Litigation costs drive some cases to settle that should not settle on the merits (83% of respondents).

Press Release, Institute for the Advancement of the American Legal System and American College of Trial Lawyers, Institute for the Advancement of the American Legal System and American College of Trial Lawyers Release Major Survey that Finds Serious Cracks in U.S. Civil Justice System (Sept. 9, 2008), *available at* http://abajournal.com/files/Survey_Press_Release_Final.pdf.

¹⁶ Some company executives and in-house counsel may feel the threat of sanctions is overstated and does not justify the allocation of significant company assets to address e-discovery compliance. Although there are numerous cases in which substantial sanctions have been imposed, many lawsuits do not see e-discovery disputes at all. It is predicted that e-discovery compliance issues will become increasingly frequent as the trial attorney bar becomes more knowledgeable and proficient about employing the various e-discovery strategies available under the Rules.

¹⁷ See, e.g., THE SEDONA CONFERENCE, THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE (2d ed. 2007), <http://www.thesedonaconference.org/dltForm?did=Guidelines.pdf>.

confidential and privileged information, and avoid unnecessary cost. E-discovery counsel will know how to prove that the company's efforts were in compliance with the court's requirements. Finally, utilization of special e-discovery counsel will allow for greater efficiencies in navigating through this difficult and often costly process.

This paper will detail the legal requirements applicable to discovery in the federal courts and in the Commonwealth of Pennsylvania. It will describe how proactive companies prepare for compliance with their discovery obligations, and will provide a series of "best practices" successful companies employ to limit risk and cost throughout this process.

II. LEGAL REQUIREMENTS FOR ELECTRONIC DISCOVERY

The Federal Rules of Civil Procedure ("Rules") were amended in 2006 to provide expressly for disclosure, discovery, and production of ESI. Prior to the amendments, courts and attorneys interpreted the term "document" in Rule 34(a) and other Rules as covering ESI.¹⁸ The emergence of new and dynamic technology, however, made it difficult to "fit [ESI] within the traditional concept of a 'document.'"¹⁹ "Rule 34(a) [was] amended to confirm that discovery of [ESI] stands on equal footing with discovery of paper documents."²⁰

The drafters of the 2006 amendments declined to define ESI because of the myriad computer systems in use and because of rapid technological change. Instead, ESI should be understood expansively as "any type of information that is stored electronically."²¹ The drafters intended Rule 34(a) "to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments."²² This expansive approach applies wherever the Rules refer to ESI.²³

These Rules are mandatory for all parties to lawsuits filed in the federal courts.

A. When is the Duty to Preserve Triggered and what is the Scope of the Duty?

The duty to preserve evidence is generally triggered by the filing of a lawsuit, but may arise earlier if a party has notice that litigation is reasonably foreseeable.²⁴ Indeed, "knowledge of a potential claim is deemed sufficient to impose a duty to preserve evidence."²⁵

¹⁸ FED. R. CIV. P. 34 advisory committee's note (2006 Amendment). *See also, e.g.*, *Thompson v. U.S. Dep't of Housing and Urban Dev.*, 219 F.R.D. 93, 96 (D. Md. 2003) (observing that courts have held email and other ESI are "documents" subject to initial disclosure under Rule 26(a) and discovery under Rule 34(a)).

¹⁹ FED. R. CIV. P. 34 advisory committee's note (2006 Amendment).

²⁰ *Id.* In this regard, the advisory committee observed that unless the requesting party clearly distinguishes between ESI and traditional paper documents, a discovery request for production of "documents" should be understood to encompass ESI. *Id.* Furthermore, Rules referencing only "documents" "should be interpreted to include [ESI] as circumstances warrant." *Id.*

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ *Cache La Poudre Feeds, LLC v. Land O'Lakes Farmland Feed, LLC*, 244 F.R.D. 614, 621 (D. Colo. 2007); *Mosaid Techs., Inc. v. Samsung Elecs. Co.*, 348 F. Supp. 2d 332, 335 (D.N.J. 2004) (quoting *Zubulake v. UBS*

A duty to preserve evidence, independent from a court order to preserve evidence, arises when there is (1) pending or probable litigation involving the defendant; (2) knowledge of the existence or likelihood of litigation; (3) foreseeable prejudice to the other party if the evidence were to be discarded; and (4) evidence relevant to the litigation.²⁶

For example, the receipt of a demand letter makes litigation reasonably foreseeable.²⁷ As soon as litigation is anticipated, the party must suspend its document retention/destruction policy and issue a litigation hold to preserve relevant documents.²⁸

A party must preserve evidence that it knows or should know is relevant to pending or reasonably foreseeable litigation.²⁹ That duty is not discharged, however, by selectively preserving evidence helpful to its theory while destroying evidence adverse to the party and/or helpful to its adversary.³⁰ At the same time, the party is not expected to preserve every single document or email in its possession. Rather, the party must preserve all documents and tangible things “made by individuals ‘likely to have discoverable information that the disclosing party may use to support its claims or defenses.’”³¹ This duty extends to documents prepared for such individuals, as well as “to information that is relevant to the claims and defenses of any party, or which is ‘relevant to the subject matter involved in the action.’”³² In short, a party must preserve “‘what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.’”³³

Warburg LLC (*Zubulake V*), 229 F.R.D. 422, 430 (S.D.N.Y. 2004). *Zubulake V* was one of several seminal and influential decisions on electronic discovery issued by U.S. District Judge Shira A. Sheindlin before the 2006 Amendment. *See also* *Zubulake v. UBS Warburg LLC (Zubulake IV)*, 220 F.R.D. 212 (S.D.N.Y. 2003) (ordering sanctions for failing to preserve backup tapes); *Zubulake v. UBS Warburg LLC (Zubulake III)*, 216 F.R.D. 280 (S.D.N.Y. 2003) (allocating between plaintiff and defendant the cost of restoring and producing backup tapes); *Zubulake v. UBS Warburg LLC (Zubulake I)*, 217 F.R.D. 309 (S.D.N.Y. 2003) (articulating standards for resolving disputes regarding scope and cost of e-discovery).

²⁵ *Winters v. Textron, Inc.*, 187 F.R.D. 518, 520 (M.D. Pa. 1999).

²⁶ *Id.* (quoting *Balotis v. McNeil*, 870 F. Supp. 1285, 1290 (M.D. Pa. 1994)).

²⁷ *See, e.g., Consol. Aluminum Corp. v. Alcoa, Inc.*, 244 F.R.D. 335, 340 & n.8 (M.D. La. 2006).

²⁸ *Zubulake IV*, 220 F.R.D. at 218.

²⁹ *Benton v. Dlorah, Inc.*, Case No. 06-CV-2488-KHV, 2007 U.S. Dist. LEXIS 80503, at *10 (D. Kan. Oct. 30, 2007).

³⁰ *Id.*

³¹ *Id.* at *11 (quoting *Zubulake IV*, 220 F.R.D. at 218).

³² *Zubulake IV*, 220 F.R.D. at 218 (quoting FED. R. CIV. P. 26(b)(1)); *see also id.* (“duty to preserve extends to those employees likely to have relevant information – the ‘key players’ in the case”).

³³ *Id.* at 217 (quoting *William T. Thompson Co. v. Gen. Nutrition Corp.*, 593 F. Supp. 1443, 1455 (N.D. Cal. 1984)). According to one jurist, the “threshold issue in all production is, of course, relevance. . . . The problem is really in its application. The best example of that is metadata.” James C. Francis IV, U.S. Magistrate Judge, U.S. District Court for the Southern District of New York, *Preservation, Production & Cost-shifting in E-discovery*, Presentation Before Fordham University School of Law (Apr. 17, 2007), in PRACTICING LAW INSTITUTE, ELECTRONIC DISCOVERY GUIDANCE 2008: WHAT CORPORATE AND OUTSIDE COUNSEL NEED TO KNOW 16 (2008) [hereinafter ELECTRONIC DISCOVERY GUIDANCE 2008] (edited version of presentation). The judge concludes that metadata often has

The party must retain all relevant ESI in existence at the time the preservation duty attaches and all relevant ESI created thereafter. Because there are multiple ways to manage and preserve ESI, parties have discretion to select the means appropriate to accomplish this task.³⁴

Finally, it bears mentioning that the issuance of a litigation hold is just the beginning of a party's preservation and discovery obligations. Working with counsel, who is charged with monitoring the party's compliance with its preservation and production obligations, the party (and counsel) must ensure "(1) that all relevant information (or at least all sources of relevant information) is discovered[;] (2) that relevant information is retained on a continuing basis; and (3) that relevant non-privileged material is produced to the opposing party."³⁵

B. The E-Discovery Process under the Rules

1. Rule 26(f) Conference of the Parties to Plan for Discovery

Almost immediately after a suit is filed, Rule 26(f) requires parties to confer and discuss the disclosure and any issues regarding preservation of ESI and attempt to agree on a proposed discovery plan.³⁶ In that plan, the parties must state their views and proposals on, *inter alia*, (1) any issues concerning disclosure or discovery of ESI, as well as form or forms in which ESI should be produced; and (2) any issues about claims of privilege or work-product protection.³⁷ With respect to claims of privilege or work-product protection, parties are encouraged to agree on a procedure for the assertion of privilege or protection after production, and, if there is such agreement, the discovery plan should indicate whether the parties desire the court to incorporate their agreement into an order.³⁸

relevance in proving the "authenticity" and thus the admissibility of most ESI, and consequently for this and other reasons, metadata should be preserved and produced. *Id.* at 16-17.

³⁴ *Zubulake IV*, 220 F.R.D. at 218.

For example, a litigant could choose to retain all then-existing backup tapes for the relevant personnel (if such tapes store data by individual or the contents can be identified in good faith and through reasonable effort), and to catalog any later-created documents in a separate electronic file. That, along with a mirror-image of the computer system taken at the time the duty to preserve attaches (to preserve documents in the state they existed at that time), creates a complete set of relevant documents. Presumably there are a multitude of other ways to achieve the same result.

Id.

³⁵ *Zubulake V*, 229 F.R.D. at 432.

³⁶ FED. R. CIV. P. 26(f)(1)-(2).

³⁷ FED. R. CIV. P. 26(f)(3)(C)-(D).

³⁸ FED. R. CIV. P. 26(f)(3)(D). In such an agreement, the parties could agree that _____ disclosures of privileged material do not constitute a waiver of the attorney-client or work product privilege. In this regard, two types of agreements are commonly utilized: (1) a "clawback" agreement; and (2) a "quick peek" agreement. FED. R. CIV. P. 26 advisory committee's note (2006 Amendment); *see also* BARTON, *supra* note 6, at 63. A "clawback" agreement "is a formal understanding between the parties that production of privileged and protected information is presumed to be inadvertent and does not automatically waive the privilege." BARTON, *supra* note 6, at 63. There is no waiver "so long as the responding party identifies the documents mistakenly produced," and the documents generally should be returned under those circumstances, pending resolution of the privilege issue. FED. R. CIV. P. 26 advisory committee's note (2006 Amendment); BARTON, *supra* note 6, at 63; *see also* Williams v. Taser Int'l, Inc., Civ. A. No. 1:06-CV-0051-RWS, 2007 U.S. Dist. LEXIS 40280, at *21-23 (N.D. Ga. June 4, 2007) (including *sua sponte* clawback provision in court order establishing protocol for search of email database). A "quick peek"

2. Rule 26(a) Initial Disclosures

Rule 26(a)(1) requires each party to disclose to the other party or parties certain information “without awaiting a discovery request.”³⁹ In this regard, the party must produce a copy, or a description by category and location, of ESI that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses (unless to be used solely for impeachment).⁴⁰ In addition, a party claiming damages or other monetary relief must disclose a computation of damages and make available for inspection and copying any documents or other evidentiary materials – including ESI – on which the party bases its computation.⁴¹

3. Rule 16 Pretrial Conference and Scheduling Order

The district court usually will conduct a pretrial conference under Rule 16 where it may consider and take action on controlling and scheduling discovery, including orders affecting disclosures and discovery.⁴² Furthermore, pursuant to Rule 16(b), the court shall issue a scheduling order, “as soon as practicable,”⁴³ that limits the time to complete discovery, and also may provide for disclosure or discovery of ESI and incorporate any agreements reached by the parties regarding the procedure for asserting claims of privilege or work-product protection after production of information.⁴⁴

4. Discovery/Subpoenas

a. Rule 34 Requests for Production of ESI

A party may serve on another party a request to produce and make available for inspection, copying, testing, or sampling “any designated documents or [ESI] – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations – stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.”⁴⁵ The requesting party may specify the form or forms in which ESI shall be produced.⁴⁶ The responding party, in turn, has thirty days after service of the request to respond in writing stating

agreement is “where a requesting party’s counsel is allowed to *see* a responding party’s entire data collection before production and designate those items which they believe are responsive to the discovery requests. Any privileged information found by the requesting party’s counsel is presumed inadvertent and does not constitute a waiver.” BARTON, *supra* note 6, at 63. Ideally, the producing party’s counsel will review a smaller set of ESI for privilege and produce only ESI responsive and non-privileged, as well as a privilege log. *Id.*; *see also* FED. R. CIV. P. 26 advisory committee’s note (2006 Amendment).

³⁹ FED. R. CIV. P. 26(a)(1)(A).

⁴⁰ FED. R. CIV. P. 26(a)(1)(A)(ii).

⁴¹ FED. R. CIV. P. 26(a)(1)(A)(iii).

⁴² FED. R. CIV. P. 16(a), (c)(2)(F).

⁴³ FED. R. CIV. P. 16(b)(1)-(2).

⁴⁴ FED. R. CIV. P. 16(b)(3)(A), (B)(iii)-(iv).

⁴⁵ FED. R. CIV. P. 34(a)(1)(A).

⁴⁶ FED. R. CIV. P. 34(b)(1)(C).

objections to the form or forms requested for producing ESI.⁴⁷ If the party so objects, or the requesting party does not specify a form for production, the responding party must specify the form or forms it intends to use.⁴⁸

Absent court order or stipulation to the contrary, if the requesting party does not specify the form or forms in which ESI shall be produced, the responding party must produce ESI “in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms,”⁴⁹ but need not produce the same ESI in multiple forms.⁵⁰

b. Rule 33 Interrogatories

If a party’s answer to an interrogatory is derived from an examination, audit, compilation, abstract, or summary of the party’s business records – including ESI – and the burden of deriving the answer will be substantially the same for either party, the party may answer by (1) “specifying the records that must be reviewed in sufficient detail to allow the interrogating party to locate and identify them”; and (2) “giving the interrogating party a reasonable opportunity to examine and audit the records and to make copies, compilations, abstracts, or summaries.”⁵¹

c. Rule 45 Subpoena

While Rule 34 provides the procedure for requesting ESI from a party, Rule 45 sets forth a similar process for requesting ESI from non-parties. A subpoena may command a person to produce at a specified time and place ESI in that person’s possession, custody, or control.⁵² Such subpoena may be combined with a command to attend a deposition, hearing, or trial, and may specify the form or forms in which ESI is to be produced.⁵³ “A command in a subpoena to produce [ESI] requires the responding party to permit inspection, copying, testing, or sampling of the materials.”⁵⁴

The person commanded to produce ESI may serve on the requesting party a written objection to producing ESI in the form or forms requested or to the inspecting, copying, testing, or sampling of the materials.⁵⁵ If the subpoena does not specify the form or forms in which ESI shall be produced, the person responding must produce ESI “in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms,” but need not produce the same ESI in more than one form.⁵⁶

⁴⁷ FED. R. CIV. P. 34(b)(2)(A), (C)-(D).

⁴⁸ FED. R. CIV. P. 34(b)(2)(D).

⁴⁹ FED. R. CIV. P. 34(b)(2)(E)(ii). *See also* FED. R. CIV. P. 34(a)(1)(A) (producing party must, if necessary, translate ESI into a “reasonably usable form”).

⁵⁰ FED. R. CIV. P. 34(b)(2)(E)(iii).

⁵¹ FED. R. CIV. P. 33(d).

⁵² FED. R. CIV. P. 45(a)(1)(A)(iii).

⁵³ FED. R. CIV. P. 45(a)(1)(C).

⁵⁴ FED. R. CIV. P. 45(a)(1)(D).

⁵⁵ FED. R. CIV. P. 45(c)(2)(B).

⁵⁶ FED. R. CIV. P. 45(d)(1)(B)-(C).

5. Inaccessible ESI: Shifting the Cost to Your Opponent

Despite their observation that “[e]lectronic storage systems often make it easier to locate and retrieve information” and may be designed to provide ready access to information used regularly or not so regularly in ongoing business activities, the drafters of the 2006 amendments were cognizant of difficulties that exist in locating, retrieving, and producing ESI.⁵⁷ In this regard, Rule 26(b)(2)(B) provides that a party is not required to produce ESI “from sources that the party identifies as not reasonably accessible because of undue burden or cost.”⁵⁸ That party, in response to a motion to compel discovery or in its own motion for protective order, must show that the ESI is not reasonably accessible because of undue burden or cost.⁵⁹ If that showing is made, the court may still order discovery, subject to conditions imposed by the court, if the requesting party demonstrates “good cause” for the discovery.⁶⁰ In determining the existence of good cause, the court considers several factors:

(i) [Whether] the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) [whether] the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; [and] (iii) [whether] the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.⁶¹

Although it may order, upon the requesting party’s demonstration of good cause, production of inaccessible ESI, the court may consider shifting the costs, in whole or in part, to the requesting party after balancing the cost and burden of production against the benefit of discovery.⁶² Courts weigh several factors in making this determination:

“(1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce

⁵⁷ FED. R. CIV. P. 26 advisory committee’s note (2006 Amendment).

⁵⁸ FED. R. CIV. P. 26(b)(2)(B).

⁵⁹ *Id.* Motions to compel are filed under Rule 37(a), *see* FED. R. CIV. P. 37(a), and motions for protective orders are brought pursuant to Rule 26(c). *See* FED. R. CIV. P. 26(c).

⁶⁰ FED. R. CIV. P. 26(b)(2)(B).

⁶¹ FED. R. CIV. P. 26(b)(2)(C). A person served with a subpoena under Rule 45 need not produce ESI “from sources that the party identifies as not reasonably accessible because of undue burden or cost.” FED. R. CIV. P. 45(d)(1)(D). Any motion to compel or for protective order will be resolved in the same manner. The person served with a subpoena must show the information is not reasonably accessible, but even if that showing is made, the court may order production if the requesting party demonstrates good cause in light of the factors enumerated in Rule 26(b)(2)(C). *Id.*

⁶² *See* FED. R. CIV. P. 26(b)(2)(B) (“The court may specify conditions for the discovery.”); FED. R. CIV. P. 26 advisory committee’s note (2006 Amendment) (“The conditions may also include payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible.”); *Cronas v. Willis Group Holdings, Ltd.*, 06 Civ. 15295 (GEL), 2008 U.S. Dist. LEXIS 81083, at *11-12 (S.D.N.Y. Oct. 8, 2008); *cf.* *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978) (noting general presumption that responding party is responsible for the costs associated with responding to a discovery request).

relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources."⁶³

These factors were derived from the seven factors enumerated in the first *Zubulake* decision:

[(1)] [t]he extent to which the request is specifically tailored to discover relevant information; [(2)] [t]he availability of such information from other sources; [(3)] [t]he total cost of production, compared to the amount in controversy; [(4)] [t]he total cost of production, compared to the resources available to each party; [(5)] [t]he relative ability of each party to control costs and its incentive to do so; [(6)] [t]he importance of the issues at stake in the litigation; and [(7)] [t]he relative benefits to the parties of obtaining the information.⁶⁴

Where the requesting party shows that the ESI is relevant, that its request is specific or narrowly tailored, and that the information is unavailable from other sources, courts are more inclined to rule that the expense should remain with the producing party. This is especially true where the total cost of production is low compared to the amount in controversy or to the resources available to the producing party.⁶⁵

6. Motions to Compel or for Sanctions

A party may file a motion to compel disclosures under Rule 26(a),⁶⁶ to compel answers or production under Rules 33 and Rule 34,⁶⁷ for sanctions for failure to comply with an order compelling disclosure or discovery,⁶⁸ or for sanctions for failing to answer, object, or respond in writing to discovery requests under Rule 33 or Rule 34.⁶⁹ Nevertheless, “[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide [ESI] lost as a result of the routine, good-faith operation of an electronic information system.”⁷⁰ As will be seen below, this is an extremely important provision which can allow parties to avoid substantial discovery costs through routine deletion of ESI pursuant to a reasonable document management system.

⁶³ PSEG Power N.Y., Inc. v. Alberici Constructors, Inc., 1:05-CV-657 (DNH/RFT), 2007 U.S. Dist. LEXIS 66767, at *32 (N.D.N.Y. Sept. 7, 2007) (quoting FED. R. CIV. P. 26 advisory committee's note (2006 Amendment)).

⁶⁴ *Zubulake I*, 217 F.R.D. at 322.

⁶⁵ See, e.g., *PSEG Power N.Y.*, 2007 U.S. Dist. LEXIS 66767, at *32-35; *Zubulake I*, 217 F.R.D. at 321.

⁶⁶ FED. R. CIV. P. 37(a)(3)(A).

⁶⁷ FED. R. CIV. P. 37(a)(3)(B)(iii)-(iv).

⁶⁸ FED. R. CIV. P. 37(b)(2)(A).

⁶⁹ FED. R. CIV. P. 37(d)(1)(A)(ii).

⁷⁰ FED. R. CIV. P. 37(e)

7. Asserting claims of Privilege or Work Product Protection

During the course of discovery of ESI, the very distinct possibility exists that privileged communications between parties and their attorneys, or the mental impressions and work product of counsel, may be inadvertently disclosed to the opposing party. The Rules, and a new Rule of Evidence recently enacted by Congress, afford various steps that can be followed to protect such information.

The 2006 amendments added Rule 26(b)(5)(B), which provides a mechanism to assert a claim of privilege or work-product protection in the event of inadvertent disclosure.⁷¹ If, after producing information (including ESI), the party claims the information produced is subject to a claim of privilege or protection, the party may notify any party receiving the information of the claim and basis therefor.⁷² Upon notification, the receiving party shall “return, sequester, or destroy” the specified information promptly and shall not use or disclose the same until the claim is resolved.⁷³ To the extent the receiving party disclosed the information before being notified of the claim, the party must “take reasonable steps to retrieve the information.”⁷⁴ The receiving party also may present the information to the court under seal for a determination.⁷⁵ Until the claim is resolved, the producing party must preserve the information.⁷⁶

Additionally, the Federal Rules of Evidence were amended recently to add new Evidence Rule 502, which addresses waiver of attorney-client privilege and work-product protection.⁷⁷ As relevant here, the new rule provides that, in a federal proceeding, disclosure of information claimed to be privileged or protected does not operate as a waiver if “(1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following [Rule 26(b)(5)(B)].”⁷⁸

Rule 502 of the Federal Rules of Evidence has the force of federal statutory law, having been enacted by Congress and signed by the President.⁷⁹ The Evidence Rule preempts state privilege laws, such that, through compliance with Rule 502’s requirements, a party will be

⁷¹ See FED. R. CIV. P. 26(b)(5)(B). The rule does not address whether the privilege or protection is waived by inadvertent production of information. FED. R. CIV. P. 26 advisory committee’s note (2006 Amendment). Instead, the drafters deferred to the courts, which “have developed principles to determine whether, and under what circumstances, waiver results from inadvertent production of privileged or protected information.” *Id.* New Rule 502 to the Federal Rules of Evidence, discussed *infra*, should fill the void created by the 2006 amendments.

⁷² FED. R. CIV. P. 26(b)(5)(B).

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ *Id.* See also FED. R. CIV. P. 45(d)(2)(B) (providing same procedure to assert claim of privilege or work product protection after producing information in response to a subpoena).

⁷⁷ See FED. R. EVID. 502.

⁷⁸ FED. R. EVID. 502(b).

⁷⁹ See Act of Sept. 19, 2008, Pub. L. No. 322, 122 Stat. 3537; see also Bill Tracking Report S. 2450, 2008 Bill Tracking S. 2450 (indicating bill passed by the Senate on February 27, 2008, and by the House on September 8, 2008, and signed by the President on September 19, 2008).

protected from having waived privilege through inadvertent disclosure, not only in the pending action, but for all purposes. The Evidence Rule does require that the parties reach an agreement on the effect of inadvertent disclosure of privileged material in discovery, which agreement will then be binding on the parties.⁸⁰ Further, the Evidence Rule provides that if the court enters an order that the attorney-client privilege or work product protection is not waived as a result of disclosure in connection with the litigation pending before the court, that order governs all persons or entities in all state or federal proceedings, whether or not they were parties to the matter before the court, if the order incorporates the agreement of the parties before the court.⁸¹ Consequently, prudent counsel will, as part of the initial Rule 26(f) conference, press to enter into an agreement regarding non-waiver of privileges, and will cause that agreement to be approved by order of the presiding court.

Of course, a party or person also may withhold from production information that it claims is privileged or protected by following the procedure in Rule 26(b)(5)(A) or Rule 45(d)(2)(A), as applicable.⁸²

C. The E-discovery Process in Pennsylvania

The Pennsylvania Rules of Civil Procedure contemplate discovery of ESI. Rule 4009.1, in part, provides that a party may serve a request on a party or subpoena on a non-party

to produce and permit the requesting party, or someone acting on the party's behalf, to inspect and copy any designated documents (including writings, drawings, graphs, charts, photographs, electronically created data, and other compilations of data from which information can be obtained, translated, if necessary, by the respondent party or [non-party] upon whom the request or subpoena is served through detection or recovery devices into reasonably usable form), or to inspect, copy, test or sample any tangible things which constitute or contain matters within the scope [of permissible discovery] and which are in the possession, custody or control of the party or [non-party] upon whom the request or subpoena is served.⁸³

There is little case law in Pennsylvania discussing in detail ESI or “electronically created data.” Furthermore, neither the rules nor the courts has addressed other matters covered by the Federal Rules of Civil Procedure, such as the discovery planning conference among counsel, the procedure to assert a claim of privilege following inadvertent production of information, the form or forms in which ESI is requested or produced, and the mechanism for shifting costs where ESI is stored in a form that is not reasonably accessible.

Finally, a party's duty to preserve evidence arises under circumstances similar to those that trigger such duty in federal court. A party has a duty to preserve evidence where litigation is pending or likely and it is foreseeable that destroying the evidence would prejudice another

⁸⁰ FED. R. EVID. 502(e).

⁸¹ FED. R. EVID. 502(d)-(e).

⁸² See FED. R. CIV. P. 26(b)(5)(A); FED. R. CIV. P. 45(a)(5)(A).

⁸³ PA. R. CIV. P. 4009.1 (emphasis added).

party.⁸⁴ The courts have not delineated the parameters of this duty other than to note that “the scope of the duty to preserve evidence is not boundless.”⁸⁵ Nor have the courts considered the duty to preserve in the context of electronic discovery. But since Pennsylvania courts have referred to federal case law in their discussions of the duty to preserve, it seems reasonable that compliance with the standards articulated in *Zubulake* and other federal decisions will suffice in Pennsylvania.

III. ESTABLISHING A SUCCESSFUL E-DISCOVERY PLAN

Proactive companies typically begin their e-discovery planning process by forming a team comprised of representatives of the legal department and the IT department, outside counsel, and a technology consultant. A good plan will address document retention/destruction policies, preservation or “litigation hold” requirements, as well as technologies and practices for searching, collecting, and reviewing data for eventual discovery production or use at trial. Effective software programs are available to assist with document management, implementation of legal hold procedures, and searching and reviewing discoverable documents. These e-discovery technologies can be evaluated using “EDRM,” or “Electronic Discovery Reference Model,” developed specifically to chart the flow of electronic data discovery as it might occur in a well designed e-discovery program.⁸⁶ EDRM was designed by its creators to provide a framework for the development, selection, evaluation, and use of electronic discovery products and services.⁸⁷

A. Creating an Electronic Records Management and Retention Policy

For most companies, electronic data is accumulating within its various communications and record keeping systems at an exponential pace. Surely, many of these documents must be maintained to meet the company’s business needs as well as regulatory or other requirements. The e-discovery Rules do not impose any obligation to maintain ESI or other records where there is no reasonable basis to believe that they are relevant to threatened or actual litigation. However, many companies simply store their ESI or other records indefinitely because the cost of such storage is minimal. For many companies, this is a huge mistake.

Once the duty to preserve documents has attached because the company has been sued, or is reasonably aware of the threat of suit, relevant documents must be preserved. Thereafter, they must be searched for responsiveness, reviewed by trained personnel for relevance and privileged material, and produced. This process has the potential to be extremely expensive in many cases. However, as mentioned above, the Rules provide a safe harbor for document destruction that takes place before the duty to place a legal hold arises, where it is done pursuant to a routine,

⁸⁴ Mt. Olivet Tabernacle Church v. Edwin L. Wiegand Div., Emerson Elec. Co., 781 A.2d 1263, 1270-71 (Pa. Super. Ct. 2001).

⁸⁵ *Id.* at 1271 (quoting *Baliois*, 870 F. Supp. at 1290).

⁸⁶ See EDRM.net, The Electronic Discovery Reference Model, <http://www.edrm.net> (last visited Jan. 18, 2009). EDRM’s website contains the entire EDRM flowchart and extensive explanation of its components, as well as the process for its development. The EDRM model contains the following sections: Information Management, Identification, Preservation, Collection, Processing, Review, Analysis, Production, and Presentation. *Id.*

⁸⁷ EDRM.net, EDRM Frequently Asked Questions, <http://www.edrm.net/faqs.php> (last visited Jan. 18, 2009).

good faith operation of an electronic information system.⁸⁸ Consequently, documents that no longer serve a legitimate business or regulatory purpose should be routinely removed pursuant to such a system. For example, duplicate ESI stored through a company's disaster recovery system (as opposed to long term storage of ESI necessary for business or regulatory purposes) should be routinely removed as early as possible once the disaster recovery need is met.

Each company should design an electronic records management system that fits its unique business requirements. This is one of the first tasks of the e-discovery planning team. For discovery compliance purposes, the team should consult e-discovery counsel who can review available precedent from cases where the reasonableness of such systems was evaluated by the courts.⁸⁹

B. Legal Holds

When litigation is pending or threatened, parties have an obligation to preserve, or "hold," all information that is potentially relevant to the matter in dispute. This obligation requires that a party suspend its normal document retention and destruction program until reasonable steps have been undertaken to recover and produce relevant matter in discovery. Companies that are parties, or potential parties, to litigation must identify, locate, and maintain relevant information, and ensure that employees in possession of such materials comply with these requirements as well.⁹⁰ Both in-house and outside counsel have a duty to monitor the company's compliance with its document preservation responsibilities.⁹¹

⁸⁸ See FED. R. CIV. P. 37(e). Cf. Disability Rights Council v. Wash. Metro. Transit Auth., 242 F.R.D. 139, (D.D.C. 2007) (explaining Rule 37(e) safe harbor "does not exempt a party who fails to stop the operation of a system that is obliterating information that may be discoverable in litigation," and thus subject to a duty to preserve).

⁸⁹ The key steps common to developing such a plan have been identified as:

- First, establish a cross-functional team to collaborate and create the program.
- Second, conduct a thorough assessment of all record types that the enterprise generates and receives in the normal course of business.
- Third, assess the enterprise's existing information technology and records management capabilities.
- Fourth, identify the legal (including litigation holds) and business requirements to retain the identified record types.
- Fifth, customize a records retention schedule, matching the legal and business requirements to the enterprise's specific types of records.
- Sixth, based upon the foregoing, craft a records retention policy that clearly defines each employee's responsibilities under the policy, establishes clear methods and procedures for managing enterprise records, and establishes standards for implementation, education and accountability.
- Seventh, roll out the program with a strong endorsement from senior management and mandatory initial training.
- Finally, eighth, audit ongoing compliance with the program and review and update the program on a periodic basis.

Jerome J. English, Basic Steps to Creating a Sound Electronic Records Management and Retention Policy, *in* ELECTRONIC DISCOVERY GUIDANCE 2008, *supra* note 33, at 187.

⁹⁰ See, e.g., Heng Chan v. Triple 8 Palace Inc., No. 03 Civ. 6048 (GEL) (JCF), 2005 U.S. Dist. LEXIS 16520, at *16 (S.D.N.Y. Aug. 11, 2005).

⁹¹ *Id.*

It has been suggested that the following “best practices” be employed for implementing a legal hold:

- Make sure that your company or client has an updated records management program that includes procedures for issuing, reissuing and terminating litigation holds;
- Once your client or company is on notice, identify all individuals and employees who may possess relevant information regarding the litigation (i.e., custodians);
- Notify custodians and IT personnel, in writing, of their duty to preserve and specify the types of information that must be preserved. Notice must be written in language that is simple and clear to non-legal recipients and include detailed instructions on preservation and collection efforts;
- When notifying custodians, be sure to include a brief primer on the company’s duty to avoid spoliation (i.e., deletion and destruction) of potentially relevant information, and explain the potential liability to the corporation and the employee for non-compliance. If possible, the notice should refer to the company’s standing records management policy and commitment to records management compliance;
- Include a description of the matter at issue, in sufficient detail to give the reader an informed sense of what types of information may be relevant to the matter and where such information might exist within the reader’s domain;
- Clearly indicate that both paper and electronic information are subject to the legal hold, and offer meaningful but non-exhaustive illustrations of the possible record-types and electronic information that may be involved;
- Identify appropriate resources and designate authorities responsible for responding to questions;
- Map out preservation strategy with IT and, to the extent practicable, include any document collection service provider in discussion;
- Develop strategies to preserve and collect offline data such as backup tapes or archived information;
- Deliver regular reminders or updates designed to keep the obligation and proper procedures fresh in the minds of the employees, as well as update them on case developments;
- Be cognizant of potential need for multiple holds concerning same custodians;
- Terminate holds and evaluate whether previously held information must be retained or destroyed pursuant to document destruction policy.⁹²

Good records should be maintained to show that each of the forgoing steps was carefully followed, in the event that the company’s hold is ever challenged in court as inadequate. Further, special care must be given when releasing litigation holds. Often, a company will have multiple litigation holds in place at one time, and ESI maintained by multiple custodians may be relevant to more than one legal hold. Steps must be taken to ensure that the release of one legal hold does not inadvertently result in the destruction of ESI or other documents that were also the subject of another legal hold. There are a number of ESI vendors that provide software applications that can assist in implementing a satisfactory litigation hold process.

⁹² BARTON, *supra* note 6, at 16-17.

C. Collection, Review, and Production of ESI

Upon becoming aware of the filing of, or reasonable threat of, litigation, a litigation response team should be formed. This team should consist of in-house counsel, a representative of the IT department, a member of the management team knowledgeable about the subject matter of the underlying suit, and litigation counsel. In some cases, companies will seek to handle the search process in-house. In other cases, it will be immediately evident that special discovery counsel and an outside vendor will be needed in order to conduct a document search and review that will withstand judicial scrutiny. This team will undertake to implement a litigation hold, and thereafter develop a plan for collecting and producing relevant ESI. Regardless of who directly performs these functions, both in-house and outside counsel have the responsibility to ensure that reasonable steps to preserve relevant ESI, and to identify and produce it, are being taken.

The litigation response team must determine: (1) the nature of the litigation and the goals of the review; (2) the various types of ESI that will have to be reviewed; (3) the volume of ESI to be reviewed; (4) how the review will take place (hard copy or electronically); (5) the form of ESI production⁹³; (6) how to implement reasonable quality control procedures for the review; and (7) the probable timetable for production.⁹⁴ The team will identify the probable custodians of the ESI, the possible locations of discoverable ESI, and the likely volume of ESI to be searched and produced. It is recommended that a standard form of electronic data questionnaire be prepared and tailored to the specific characteristics of the case, to assist the team in mapping where the responsive ESI may be found throughout the company's various electronic media systems.

It is at this point that early case assessment may be appropriate. The litigation response team, acting under the guidance of outside litigation counsel, should make an informed assessment of the risk of liability and the amount of potential damages that could be awarded in the case. How much e-discovery is warranted by this level of exposure? What will be the cost of defending and meeting the company's discovery disclosure obligations? Should the company press for early settlement as a result of a cost-benefit analysis? Should the company seek a protective order from the court regarding ESI that is not readily accessible and seek to shift the costs of such production to the opponent? Should discovery counsel, during the initial meet and discuss conference, seek to cooperate with opposing counsel by agreeing in the discovery plan on negotiated search terms and the media to be searched in an effort to reasonably limit expense?⁹⁵ Should a "quick peek" agreement be entered into which allows the other party to

⁹³ Rule 34 permits ESI to be produced in "a form or forms in which it is ordinarily maintained or in a reasonably usable form or form" where no specific form is requested. FED. R. CIV. P. 34(b)(2)(E)(ii). The most typical production of ESI is through static image files (TIFF and PDFs). BARTON, *supra* note 6, at 50. PDFs are often used because they can be made searchable. *Id.* "Native" files are ESI in the form actually created by the original business application. *Id.* Native files usually contain the original metadata, but are less convenient, because they require the original software in order to be read. *Id.* Because native files contain metadata that could be changed with subsequent views, ESI vendors typically will copy the native files and preserve the original in its unaltered state, in order to address chain of custody and other authenticity evidentiary issues. *Id.*

⁹⁴ Ashish S. Prasad et al., Best Practices for Documented Review in Litigation and Government Investigations, in ELECTRONIC DISCOVERY GUIDANCE 2008, *supra* note 33, at 170.

⁹⁵ Rule 26(f) requires parties to meet and confer in good faith regarding their respective ESI. FED. R. CIV. P. 26(f)(1)-(2), (3)(C). Further, by forging agreement with opposing counsel on search terms and other search parameters, one may limit the scope of discovery and avoid the risk and expense of discovery motions practice later. On the other hand, neglecting one's Rule 26(f) obligation to "meet and confer" can expose a party to sanctions. *See R&R Sails, Inc.*, 2008 U.S. Dist. LEXIS 44552, at *11-16 (after noting parties' Rule 26(f) discovery plan made no

simply take a brief look at categories of documents as kept in the ordinary course of business in order to limit what will actually be requested?⁹⁶

To the extent that the company elects to proceed with discovery, there are many search technologies that can make the review for relevant ESI easier and less expensive.⁹⁷ Key word searches and limits on the types of data or files to be searched and the date ranges to be searched are methods that have been accepted by the courts as reasonable under the circumstances of the discovery disputes involved in those cases.⁹⁸ However, a number of courts are requiring the

reference to electronic discovery, court sanctioned defendant for failing to produce electronically stored claim log). Indeed, the lack of cooperation generally in discovery, whether at the outset or during the course of, was bemoaned recently by U.S. Magistrate Judge Paul W. Grimm, a leading e-discovery jurist. *See* *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 359 (D. Md. 2008) (chastising counsel's extreme adversarial posture in pre-trial discovery as a reason that discovery costs are widely criticized as excessive). The solution, Judge Grimm noted, is to engage litigants and other stakeholders with incentives to alter their approach to discovery. *Id.* at 363. To that end, Judge Grimm quoted approvingly of The Sedona Conference's COOPERATION PROCLAMATION, which launched "'a national drive to promote open and forthright information sharing, dialogue (internal and external), training, and the development of practical tools to facilitate cooperative, collaborative, transparent discovery.'" *Id.* (quoting THE SEDONA CONFERENCE, COOPERATION PROCLAMATION 1 (2008), http://www.thesedonaconference.org/dltForm?did=Cooperation_Proclamation.pdf). "If these goals are achieved, the benefits will be profound." *Id.* By meeting and conferring early in litigation in order to agree on search terms and other search parameters, parties will "facilitate cooperative, collaborative, transparent discovery."

⁹⁶ *See* BARTON, *supra* note 6, at 63-64 (identifying factors counsel should consider before entering into a "quick peek" or "clawback" agreement); *see also supra* note 38 (defining "clawback" and "quick peek" agreements).

⁹⁷ There are numerous technology vendors who provide a broad range of applications designed to enable companies to meet their e-discovery obligations. The Sedona Conference has promulgated best practices for the selection of electronic discovery vendors. *See* THE SEDONA CONFERENCE, BEST PRACTICES FOR THE SELECTION OF ELECTRONIC DISCOVERY VENDORS: NAVIGATING THE VENDOR PROPOSAL PROCESS (June 2007), http://www.thesedonaconference.org/dltForm?did=RFP_Paper.pdf. This working group broadly categorized the e-discovery tasks into five categories: (1) "Consulting/Professional Services"; (2) "Data Collection/Processing"; (3) "Data Recovery/Forensics"; (4) "Hosting/Review/Production/Delivery"; and (5) "Other Litigation Support-Related Services." *Id.* at 22. This report set forth a systematic process for soliciting and evaluating proposals for these technologies. *See id.* at 3-29.

⁹⁸ *See, e.g.,* *In re CV Therapeutics, Inc., Sec. Litig.*, No. C-03-3709 SI (BMC), 2006 U.S. Dist. LEXIS 63155, at *6-7 (N.D. Cal. Aug. 22, 2006) (where plaintiff sought production of 125,000 documents, court allowed defendants to narrow the ultimate production by application of search terms, the employment of which the court explained was a "reasonable means of narrowing the production in this instance"); *Alexander v. Fed. Bureau of Investigation*, 188 F.R.D. 111, 116-17 (D.D.C. 1998) (holding defendant's decision not to search "years-old backed-up and archived e-mail, deleted and archived computer files, [and] shared drive files" was reasonable where defendant established, through declarations of IT personnel, that cost and burden of such searches outweighed likelihood of uncovering relevant information); *cf. In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004) (discussing Fourth Amendment limitations on Government's search of defendant's computer, court observed that computer technology affords Government methods – such as searching a particular date range or certain files or running key word searches – to conduct targeted searches for criminal activity). The Sedona Conference commentators have expressly adopted as a goal placing reasonable limits on electronic discovery:

When responding to discovery requests, organizations should define the scope of the electronically stored information needed to appropriately and fairly address the issues in the case and to avoid unreasonable overbreadth, burden, and cost. Important steps in achieving the goal of reasonably limiting discovery may include: (1) collecting electronically stored information from repositories used by key individuals rather than generally searching through the entire organization's electronic information systems; (2) defining the information to be collected by applying reasonable selection criteria, including search terms, date restrictions, or folder designations; or (3) avoiding collection efforts that are disproportionate to, or are inappropriate in, the context of a particular litigation.

party responding to discovery to justify its selection of search terms, and to prove that its search was reasonable through witnesses who are qualified in the technology used.⁹⁹ This is an excellent reason why serious consideration should be given to negotiating with opposing counsel to reasonably limit the search terms to be used.

In the event of a discovery dispute with the opposing party, the courts will look to determine the reasonable effectiveness of your collection and review techniques, your search terms, and your limiting parameters for the search. Were the methods employed reasonably calculated to locate all relevant documents? Is the method repeatable, in that it would produce the same results if conducted again? Counsel must become familiar with the client's ESI systems in order to defend these searches and discovery efforts. In some cases, a technical expert will be required to testify about the capabilities and reliability of the search mechanisms employed.

As the collection of ESI proceeds, counsel must keep in mind issues of authenticity, chain of custody, and spoliation. ESI must not be altered through the collection process. Steps must be taken to ensure that metadata, if within the scope of required production, is not modified by the search or recovery process. The responding party must be able to establish that the ESI being produced has been preserved in its original form, or produced in a reasonably usable form, and is authentic and complete.¹⁰⁰ Courts have held, for example, that the conversion of emails and other data to PDF format or to paper copies did not constitute reasonably usable form under Rule 34.¹⁰¹

THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 38 (2d ed. 2007) (Comment 6.b "Scope of collection of electronically stored information"), http://www.thesedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf.

⁹⁹ See *D'Onofrio v. SFX Sports Group, Inc.*, Civ. A. No. 06-687 (JDB/JMF), 2008 U.S. Dist. LEXIS 87905, at *5-9 (D.D.C. Oct. 29, 2008) (criticizing defendants' search protocol, developed with assistance from their IT consultant, as "highly restrictive" and, to a certain degree, "incomprehensible"); *but see* *Equity Analytics, LLC v. Lundin*, 248 F.R.D. 331, 333 (D.D.C. 2008) (requiring the party challenging the search terms proposed by other party to present expert testimony to explain their deficiencies). In *Victor Stanley, Inc. v. Creative Pipe, Inc.*, a party sought to establish the reasonableness of its search process in order to avoid waiving attorney-client privilege as to documents inadvertently produced. 250 F.R.D. 251, 259 (D. Md. 2008). The party had used key word searches it deemed reasonable, which had been selected by the party and its counsel. *Id.* at 256. Defendants could not establish their rationale for the key words selected and the qualifications of the party and attorney to design a reliable search and information retrieval method. *Id.* at 259, 262. Further, they did not prove that they analyzed the results of the search to assess its reliability. *Id.* at 259. The court explained that expert witnesses may be necessary to back up a party's positions that its ESI search and information retrieval methodology was reasonable. *Id.* at 260 & n.10.

¹⁰⁰ See *supra* note 93.

¹⁰¹ See, e.g., *White v. Graceland Coll. Ctr. for Prof'l Dev. & Lifelong Learning, Inc.*, Civ. A. No. 07-2319-CM, 2008 U. S. Dist. Lexis 63088, at *33-34 (D. Kan. Aug. 7, 2008). The court's decision in *White* echoed the observations of the advisory committee:

But the option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.

Once the mass of potentially responsive ESI has been collected, it must be reviewed for responsiveness and relevance and to avoid inadvertent disclosure of ESI that contains privileged, confidential, or proprietary information that must be protected. The review process is a critical stage of the e-discovery process. First, inadvertently disclosed attorney-client or work product material can only receive the protection of the court if “reasonable steps” were taken to prevent inadvertent disclosure.¹⁰² Second, on any challenge to the completeness of disclosures made, a party must establish that the review was conducted in a reasonable and reliable way.

In more complex litigations, where ESI discovery is expected to be voluminous, it can be cost effective to seek out contract lawyers or document review vendors to handle some or all of the document review. A few companies have sought to send the review function to an overseas vendor, essentially for cost savings reasons.¹⁰³ However, whether one risks going offshore, or simply utilizes contract attorneys here at home, there remains one constant – both litigation counsel and in-house counsel have a duty to supervise the process and take reasonable steps to ensure that document productions are accurate and complete.

What factors should be considered in selecting a document review vendor? First, does the vendor have a strong reputation within the legal community? This allows the vendor to recruit better reviewing professionals and makes it more likely that the vendor can defend its review procedures should they be challenged in court.¹⁰⁴ What is the vendor’s experience providing staff for document reviews? How does the vendor recruit staff? Can it respond on short notice? Does it provide project space and equipment?¹⁰⁵

At a minimum, contract review attorneys must hold an active law license and be in good standing within their jurisdiction.¹⁰⁶ They should also have prior document review experience, practice experience, and subject matter experience, and a working knowledge of the review software.¹⁰⁷ Do they receive fair compensation and benefits from their employer? This could be indicative of the talent pool the vendor can attract.¹⁰⁸ Are good employment hiring practices, such as background checks and in-person interviews, conducted by the vendor?¹⁰⁹

Litigation counsel should make sure that the details of the subject litigation are made known to the search attorneys, with emphasis on important issues and possible types of communications or specific information that may be found within the ESI being searched. A work plan should be created to include all activities associated with the document review,

FED. R. CIV. P. 34 advisory committee’s note (2006 Amendment).

¹⁰² FED. R. EVID. 502(b).

¹⁰³ This practice appears to be extremely limited. The LITIGATION TRENDS SURVEY reports that just 4% of all respondents said they used offshore personnel for review and coding of documents. LITIGATION TRENDS SURVEY, *supra* note 2, at 52.

¹⁰⁴ Prasad et al., *supra* note 94, at 178.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ *Id.* at 179

¹⁰⁹ *Id.*

including review and coding procedures, productivity expectations, use of an issues log (to track and answer frequently asked questions), schedules, and other important items.¹¹⁰ The legal professionals conducting the review should receive detailed training as to what results are expected. They must have a clear understanding of the criteria for determining relevance, how to spot potentially privileged matter, and how to code the ESI.¹¹¹ They should receive written instructions for future reference and checklists of tasks to perform, and must be thoroughly trained on the ESI reviewing software.¹¹² Once work has begun, the case manager and project manager must review work for consistency and accuracy. A sample second level review is useful for this purpose.¹¹³ Other quality control measures, including additional training where frequent mistakes are noted, should be implemented as appropriate. All of these steps should be documented for production should the adequacy of the ESI discovery response be questioned.

IV. RECOMMENDATIONS FOR GETTING STARTED

It is recommended that companies wishing to create an effective e-discovery compliance program begin by putting together a team consisting of in-house counsel, the IT director, a senior operations manager, and outside counsel. It is also recommended that an e-discovery technical consultant be made a part of the team. Begin with an evaluation of current record handling practices. Does the company have a satisfactory information management plan that otherwise meets its business purposes? Improvements to this plan generally could actually lead to efficiencies that would help defray the cost of implementing an e-discovery program. If the company does not have a satisfactory document retention/destruction plan, including reuse of backup tapes, one should be developed, keeping in mind the business needs of the company, first and foremost. If the company does have a document retention program, is it consistently and routinely utilized, and can it be demonstrated to be so should the company ever be accused of failing to meet its document preservation obligations?

If the company does not have policies and procedures for establishing legal holds, they should be established, and policy manuals should be created. The procedure should include appropriate checklists and memoranda outlining all personnel's responsibilities. Staff must be trained in compliance with the document retention system and the legal hold policy. They must also be trained in the uses and dangers of misuse of the company email system. Finally, they must receive training in complying with document compilation and retrieval processes implemented in connection with pending or threatened litigation.

The e-discovery planning team should evaluate and recommend the purchase of reliable legal hold software. If the company does not wish to expend huge sums on outside consultants each time a new ESI discovery matter arises, it should also seek to acquire search and review software. These programs can be expensive, so reliance upon a qualified e-discovery consultant to assist in selecting this software is recommended. Such software can be purchased outright, or leased on a per-case basis, which may be an optimal way of testing the software in order to determine whether it meets the company's needs.

¹¹⁰ *Id.* at 181, 184.

¹¹¹ *Id.* at 181.

¹¹² *Id.* at 181-82.

¹¹³ *Id.* at 182-83.

Consideration should be given to organizing a standing litigation response team, assigned to handle all of the company's e-discovery matters. This could be comprised of the same members of the e-discovery planning team, supplemented as needed by operations managers from the area specifically affected by the litigation. Through implementation of these measures, the use of effective training, and periodic follow up, an effective internal e-discovery compliance program can be established. Use of special e-discovery counsel for all cases in which compliance with the e-discovery rules may be an issue will insure that the company is represented in court by an attorney who is familiar with the company's document management programs and e-discovery policies, and can present the company's compliance efforts in the strongest possible light.

V. CONCLUSION

E-discovery compliance is a corporate requirement overlooked or underestimated at the company's peril. The judges who preside over federal cases and who enforce the Rules are serious about these requirements, and hold litigants to a high standard of compliance. Where full compliance cannot be shown, the risk of sanctions could place the company at a distinct disadvantage, not only when confronting discovery motions, but in its ability to prevail at trial or to negotiate a satisfactory settlement from a position of relative strength. Fortunately, there are procedures and tools available to company management to effectively address these issues in a competent and responsible fashion. Prudent planning and preparedness will limit litigation risk and the cost of compliance to the extent possible. Retention of competent IT consultants and experienced litigation counsel to address these issues on a consistent basis will afford the company the best possible chance to avoid unnecessary cost and sanctions, leading to a settlement or other resolution of the underlying dispute on its actual merits.