E-Discovery: The Federal Rules, The Legal Hold, and Strategic Considerations

REAL Conference
September 27-28, 2007
Houston, Texas

Scott McIntosh, Esq.
DLA Piper US LLP
1200 Nineteenth Street, N.W.
Washington, D.C. 20036
(202) 861-3979
scott.mcintosh@dlapiper.com

Scott McIntosh

Associate

DLA Piper US LLP
1200 Nineteenth Street, NW
Washington, DC 20036-2412
(202) 861-3979 T (202) 689-7417 F
scott.mcintosh@dlapiper.com

PRACTICES

Franchise Litigation
Franchise and Distribution

EDUCATION

- Georgetown University Law Center (1998) J.D. cum laude
  Articles Editor, Georgetown International Environmental Law Journal
  Law Fellow, Legal Research & Writing Program

- Georgetown University (1998) M.S.

- University of California at Los Angeles (1993) B.A.
  Phi Beta Kappa

ADMISSIONS

District of Columbia
Virginia
United States Court of Appeals for the Fourth Circuit
United States District Court for the Eastern District of Virginia
United States District Court for the Western District of Virginia

EXPERIENCE

Scott A. McIntosh has a broad-based practice in franchising law, with significant experience in myriad business, litigation, and regulatory issues that confront franchising companies. He has represented franchise clients in both state and federal litigation, including complex multiple party lawsuits. Mr. McIntosh also has represented clients in various forms of alternative dispute resolution, including binding arbitration before the American Arbitration Association. He has successfully represented a number of clients in responding to inquiries and investigations into potential violations of federal or state franchise statutes and regulations by the Federal Trade Commission and various state attorney general offices.

Mr. McIntosh has handled various facets of electronic discovery under the new electronic discovery provisions of the Federal Rules of Civil Procedure, as well as under the pre-2006 amendment version of the Rules. Mr. McIntosh has assisted clients in implementing document retention policies, formulating litigation hold memoranda, retrieving electronically stored information for review and production, and managing electronically stored information for effective use in litigation.

Mr. McIntosh also counsels clients on franchise relations, terminations, transfers, and regulatory compliance. His experience includes preparation of franchise and license agreements, area development agreements, numerous collateral agreements, and disclosure materials for domestic and international development. He has created documents for a variety of franchise business transactions, including the creation of advertising cooperatives and the sale of a domestic subfranchisor's assets.

In the June/July 2001 issue of *Franchise Times* magazine, Mr. McIntosh was profiled as one of the up-and-coming attorneys in the franchise bar.

PUBLICATIONS

- Co-author (with Barry M. Heller), "California Decision Clarifies Franchise Termination Damages," *FranCast* (April 1, 2004)
- Co-author (with Barry M. Heller), "When Franchisee Counsel Goes Too Far: Court Issues Sanctions in Connection with Withdrawn Superfluous Claims," *FranCast* (September 22, 2003)
- Author, "Mediation Before Litigation: Delaware Court's Expanded Jurisdiction Offers Remedy to Franchise Disputes," LJN's Franchising Business & Law Alert (July 2003 edition)
- Co-author (with Erik B. Wulff), "Are Franchisors Caught in the Broad Web of the Anti-Terrorism Devices of Executive Order 13224 and the USA PATRIOT Act?," *FranCast* (May 10, 2002)
- Co-author (with Erik B. Wulff), "The Separate Product Test in Franchise Tying Cases: Through the *Microsoft* Lens of Reason," ABA *Franchise Law Journal* (Fall 2001)
- Author, "Fair Criticism, Cyberlibel, and Unlawful Coordinated Action over the Internet," in the ABA *Franchise Law Journal* (Spring 2001)
- Co-author (with Erik B. Wulff), "Electronic UFOCs Now A Reality," *The Franchise Lawyer* (Summer 2000)

SEMINARS

- "Franchise Legal Issues in a Volatile Economy," International Franchise Association 2002 Legal Roundtable Series, Philadelphia (September 2002)

PROFESSIONAL MEMBERSHIPS

- American Bar Association

Table of Contents

I. SCOPE OF ARTICLE

This article provides a brief introduction to e-discovery, including an overview of electronically stored information and some of the differences between e-discovery and traditional paper discovery. Next, the article provides a summary of the 2006 amendments to the Federal Rules of Civil Procedure, as well as their practical implications for the discovery process. The article then explains legal holds, including what they are, steps for initiating and managing the legal hold process, potential risks associated with an inadequate legal hold process, and strategies for pro-actively managing the legal hold process. Finally, the article concludes by discussing strategic considerations that arise in connection with electronically stored information, including managing electronically stored information for effective use in litigation and protecting a company's confidential information.

II. INTRODUCTION TO E-DISCOVERY

A. What is Electronically Stored Information?

Electronically Stored Information ("ESI") is a term added to the Federal Rules of Civil Procedure (the "Rules") in connection with the 2006 amendments to the Rules. **ESI is a broad term that "includes any type of information that is stored electronically."** F.R.C.P. 34 at Advisory Committee Notes to 2006 Amendment. While most people would correctly assume that ESI includes email and Word or Excel documents contained on their computers, ESI also encompasses less obvious forms of data such as instant messages; text messages; web pages; computer databases; erased, fragmented or damaged data; metadata associated with computer files; and essentially any other information that is stored on a computer or other electronic devices such as personal digital assistants and cell phones. ESI is also intended to be a flexible term that encompasses future technological developments. The notes accompanying the 2006 amendments to the Rules specifically state that ESI "is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments." *Id.*

B. How Does E-Discovery Differ From Traditional Paper Discovery?

Discovery of ESI differs from traditional paper discovery in a number of ways, particularly with respect to the volume of information, the number and types of sources, the additional layer of metadata, unpredictability, and the procedures for review and production. In addressing the differences between traditional paper discovery and discovery of emails, one court observed as follows:

> Chief among these differences is the sheer volume of electronic information. E-mails have replaced other forms of communications besides just paper-based communication. Many informal messages that were previously relayed by telephone or at the water cooler are now sent via e-mail. Additionally, computers have the ability to capture several copies (or drafts) of the same e-mail, thus multiplying the volume of documents. All of these e-mails must be scanned for both relevance and

> privilege. Also, unlike most paper-based discovery, archived e-mails typically lack a coherent filing system. Moreover, dated archival systems commonly store information on magnetic tapes which have become obsolete. Thus, parties incur additional costs in translating the data from the tapes into useable form.

Byers v. Illinois State Police, 53 Fed. R. Serv. 3d 740, 2002 WL 1264004, *10 (N.D. Ill. May 31, 2002). Each of these factors tends to increase the costs of discovery of ESI, when compared with traditional paper discovery.

Considering ESI for production increases exponentially the volume of information that may be relevant. The average person sends or receives hundreds of emails each day. According to a Reuters report from April 2006, more than 60 billion emails are sent daily worldwide. Given the ease of including an additional recipient, or sending a document to a pre-defined distribution list, a company's system may have dozens, hundreds, or thousands of copies of the same email, including any attached documents. Many companies have thousands of back-up tapes containing ESI, with no current employees who know what is contained on the back-up tapes.

Whereas paper documents are likely to be contained within specific identifiable files, electronically stored information may be found on individual computers including laptops, central servers, portable hard drives, optical disks (CDs or DVDs), magnetic tapes or backup tapes, memory cards, thumb drives, personal digital assistants, cell phones, and other devices. While paper files tend to be located at the company's offices or indexed at an off-site storage facility, many of the aforementioned electronic devices, such as laptop computers, thumb drives, personal digital assistants, and cell phones are mobile and pose challenges for centralized collection of information.

Information available from most paper documents is limited to the information contained on the face of the document. However, most ESI also contains metadata. Metadata is a second layer of information associated with an electronic document that may reveal additional useful information not apparent on the face of the records, including the identity of the creator or author of the document, the date the document was initially created, the identity of the last person who edited the document, and other information.

Because much electronically information is created quickly and oftentimes informally, especially in the case of email, ESI is much more prone to containing "smoking guns" or comments that in hindsight appear intemperate. This factor is enhanced by the fact that ESI lacks tone or body language, unlike personal communications, and the meaning of sarcastic or "tongue-in-cheek" comments may be further distorted.

In light of these factors, different considerations and procedures apply to the discovery of ESI.

III. 2006 AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE

While discovery of ESI was frequently sought and obtained by litigants prior to the amendment of the Rules which went into effect on December 1, 2006, the amendments have put even non-technology savvy attorneys and clients on notice regarding the role of ESI in litigation. The Rule amendments also formalize and standardize various processes and procedures governing ESI. This section briefly sets forth the 2006 amendments relating to ESI, as well as their practical implications for the discovery process.

A. Rule 16(b)

> *The scheduling order also may include . . .*
>
> *(5) provisions for disclosure or discovery of electronically stored information;*
>
> *(6) any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production;*

The amendments to Rule 16(b), which operate in connection with the Rule 26(f) conference of the parties (*see* discussion regarding Rule 26(f) below), have two primary purposes. **The first purpose is to involve the court early in ESI discovery issues in the event ESI will be, or is likely to be, produced in the case.** Consistent with this goal, Form 35 ("Report of Parties' Planning Meeting") was amended to include reporting on the issue of ESI, as well as any agreements regarding claims of privilege. According the Advisory Committee notes, these changes were made to facilitate "the court's involvement early in the litigation [which] will help avoid difficulties that might otherwise arise." F.R.C.P. 16(b) at Advisory Committee Notes to 2006 Amendment.

The second purpose is to include any agreements the parties reach with respect to materials protected by the attorney-client privilege or the work product doctrine that may facilitate discovery in the matter. A variety of different types of agreements are contemplated by this provision, including "quick peek" or "clawback agreements," discussed below in the context of Rule 26(f), as well as other agreements the parties may reach as to privilege issues. The amendment clarifies the court's authority to make such agreements part of the court's order. This provision works in tandem with amended Rule 26(b)(5)(B), discussed below, which establishes a procedure for raising inadvertent production issues.

B. Rule 26(a)(1)

> *Except in categories of proceedings specified in Rule 26(a)(1)(E), or to the extent otherwise stipulated or directed by order, a party must, without awaiting a discovery request, provide to other parties: . . .*
>
> *(B) a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the*

> *possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;*

The amendment to Rule 26(a)(1) confirms that ESI is on the same footing as other documents in the context of initial disclosures. **In other words, a party may not await discovery requests specifically directed at ESI, but must voluntarily provide, or identify, ESI that a party may use to support its claims or defenses.** Because initial disclosures are due within 14 days after the Rule 26(f) conference, which is fairly early in most cases, this amendment highlights the need for companies to have a working understanding of the types of ESI they possess, where particular types of ESI are maintained, how the ESI is retained and destroyed, and how ESI may be efficiently retrieved, without inadvertently altering the ESI, including any metadata.

C. Rule 26(b)(2)(B)

> *A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.*

While ESI, like other information sought in discovery, may be the subject of a motion for protective order under Rule 26(c) in appropriate circumstances, amended Rule 26(b)(2)(B) recognizes that there are unique potential costs and burdens associated with producing some ESI. Rule 26(b)(2)(B) provides that ESI is deemed "not reasonably accessible" and need not be produced when production of such information would impose undue burden or cost. On a motion to compel or for a protective order, the party possessing the ESI bears the burden of establishing that production of the information would entail undue burden or cost.

However, even when the party possessing the ESI satisfies its burden of showing undue burden or cost, the court may still require production upon a showing of "good cause." *See Ameriwood Industries, Inc. v. Liberman*, 2006 WL 3825291, *4-5 (E.D. Mo. Dec. 27, 2006) (holding that defendant was required to produce ESI that was not reasonably accessible due to cost because plaintiff established "good cause" for production where the ESI was directly relevant to plaintiff's claims, including a claim under the Computer Fraud and Abuse Act). The Advisory Committee Notes set forth some factors that are appropriate for consideration in determining whether good cause exists to require production, notwithstanding the undue burden or cost:

(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 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.

F.R.C.P. 26(b) at Advisory Committee Notes to 2006 Amendment.

This provision also provides the court with the authority to fashion appropriate limitations on the ESI that is sought, including limitations "on the amount, type, or sources of information that must be accessed and produced." *Id.* **Additionally, the court may require the party seeking discovery of the ESI to bear all or part of the costs associated with obtaining the ESI, when it determines that such cost-sharing is appropriate.** *See Quinby v. WestLB AG*, 2007 WL 38230 (S.D.N.Y. Jan. 4, 2007) (partially shifting cost to plaintiff of restoring backup tapes containing emails of a particular custodian); *Ameriwood Industries, Inc.*, 2006 WL 3825291 at *5 (ordering plaintiff, which did not object to cost shifting, to pay costs involved in imaging, recovering, and translating defendant's ESI into searchable formats as required in the order). Courts are unlikely to award cost shifting when ESI is deemed "accessible." *Hutchens v. Hutchens-Collins*, 2007 WL 319990, *4 n. 2 (D. Or. 2007).

An important issue to be developed in the caselaw is the extent to which the costs of attorney review for relevance and privilege may render certain groups of ESI "inaccessible." In a state court case, which cited the Rules and caselaw interpreting the Rules as instructive authority, the court ordered the plaintiff to conduct sample searches of its backup tapes to determine whether they contained relevant information, but required the defendant to bear the cost of the sample searches, including plaintiff's attorneys' fees incurred in connection with review of the information generated by the searches. *Delta Financial Corp. v. Morrison*, 13 Misc.3d 604, 819 N.Y.S.2d 908 (S. Ct. N.Y. Aug. 17, 2006).

D. Rule 26(b)(5)(B)

Information Produced. If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a

party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

While Rule 26(b)(5)(B) is written to apply generally in discovery, and should be applied to all types of discovery, its provisions were particularly focused on ESI. As the Advisory Committee Notes recognize, "[w]hen the review is of electronically stored information, the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the difficulty in ensuring that all information to be produced has in fact been reviewed." F.R.C.P. 26(b) at Advisory Committee Notes to 2006 Amendment.

Amended Rule 26(b)(5)(B) establishes a procedure for handling an asserted inadvertent production of information subject to protection on the basis of attorney-client privilege or the work product doctrine. However, this is merely a procedural device. **Whether or not an asserted privilege has been waived will be governed by applicable law and any agreements reached by the parties at the Rule 26(f) conference, which may be memorialized in the Rule 16(b) Order, as discussed above.**

E. Rule 26(f)

[T]he parties must . . . confer . . . to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan that indicates the parties' views and proposals concerning: . . .

(3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;

(4) any issues relating to claims of privilege or of protection as trial-preparation material, including—if the parties agree on a procedure to assert such claims after production—whether to ask the court to include their agreement in an order;

As a parallel to the amendments to Rule 16(b), Rule 26(f) has been amended to require the parties to confer regarding "any issues" relating to ESI, as well as "any issues" relating to potential attorney-client privilege or work product doctrine issues.

While the precise scope of "any issues" relating to ESI is inherently case-specific, a variety of factors should be considered for potential discussion in most Rule 26(f) conferences, including the following:

- The form or forms in which ESI will be produced;

- Whether metadata will be produced;
- Whether any ESI potentially containing relevant information is "not reasonably accessible" due to burden or cost;
- Any particular preservation issues that may be presented by ESI;
- Topics and time period for information sought that is likely to be contained in ESI;
- Search terms;
- The sources of ESI that the parties will search;
- Cost sharing

In discussing "any issues" relating to privilege concerns, the parties should particularly address any potential privilege issues presented by the proposals for discovery of ESI. The parties should also discuss whether any agreements regarding privilege issues are desirable. Such agreements could include agreements providing that no waiver of privilege shall apply in the event of inadvertent production ("clawback agreements") as well as agreements that would preserve privilege during an inspection by the opposing party's counsel which would enable the producing party to perform a full privilege review only with respect to the documents requested, rather than all documents made available for inspection ("quick peek" agreements).

Because the Rule 26(f) conference must take place at least 21 days prior to a scheduling conference, and sometimes even earlier by local rule, parties will have very little time to develop their views regarding these ESI and privilege matters, as well as the other topics that must be addressed at the Rule 26(f) conference. Therefore, as discussed below, parties need to have a working understanding of their ESI prior to the onset of any litigation.

When a party is likely to bear a disproportionate burden with respect to retention and production of ESI in a particular litigation matter, that party needs to make appropriate use of the Rule 26(f) conference and to apprise the court of actual and potential ESI issues and burdens in the case in order to prevent ESI discovery issues from becoming the main attraction, while the actual case is relegated to a side-show.

F. Rule 33(d)

> *Option to Produce Business Records. Where the answer to an interrogatory may be derived or ascertained from the business records, including electronically stored information, of the party upon whom the interrogatory has been served or from an examination, audit or inspection of such business records, including a compilation, abstract or summary thereof, and the burden of deriving or ascertaining the answer is substantially the same for the party serving the interrogatory as for the*

party served, it is a sufficient answer to such interrogatory to specify the records from which the answer may be derived or ascertained and to afford to the party serving the interrogatory reasonable opportunity to examine, audit or inspect such records and to make copies, compilations, abstracts, or summaries. A specification shall be in sufficient detail to permit the interrogating party to locate and to identify, as readily as can the party served, the records from which the answer may be ascertained.

Rule 33(d) was amended to clarify that a party may indicate, in response to an interrogatory, that the information may be discerned from specified ESI. While the amendment creates the ability to respond to an interrogatory by referencing ESI from which the answer may be derived, there are two primary obstacles to relying upon such a response. First, while the answer may be discernable from certain ESI, the responding party may have difficulty demonstrating that "the burden of deriving or ascertaining the answer is substantially the same for the party serving the interrogatory as for the party served," particularly if the ESI is being produced in a different format than the format in which it is maintained. Second, where the ESI that must be referenced is maintained within a database or computer program that is not commercially available, the responding party may be required, as a practical matter, to grant the requesting party access to its system in order to derive the answer. Given the potential security, confidentiality, and privilege concerns that would be raised by granting access to the opposing party, the respondent may prefer to derive the answer itself.

G. Rule 34(a)

Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information—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—translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

Amended Rule 34(a) provides that a party may test or sample documents or ESI (as well as inspect or copy such information). This clarification is particularly important with respect to ESI because it may provide parties with a less burdensome means of locating potentially relevant information when dealing with a voluminous universe of ESI. Notwithstanding that a plain reading of Rule 34(a) may appear to contemplate direct access to the responding party's computer system by referring to testing or sampling of electronically stored information, as well

as "testing, or sampling the property or any designated object or operation thereon," the Advisory Committee Notes clarify that "[t]he addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances." F.R.C.P. 34(a) at Advisory Committee Notes to 2006 Amendment.

H. Rule 34(b)

> *The request may specify the form or forms in which electronically stored information is to be produced. . . . The response shall state, with respect to each item or category, the inspection and related activities will be permitted as requested, unless the request is objected to, including an objection to the requested form or forms for producing electronically stored information, stating the reasons for the objection. . . . If objection is made to the requested form or forms for producing electronically stored information—or if no form was specified in the request—the responding party must state the form or forms it intends to use. . . . Unless the parties otherwise agree, or the court otherwise orders:*
>
> *(i) a party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request;*
>
> *(ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and*
>
> *(iii) a party need not produce the same electronically stored information in more than one form.*

The amendments to Rule 34(b) can be referred to as "the battle of the forms." The requesting party may, but is not required to, specify the form for production of any ESI it seeks to discover. The responding party may either agree to the form requested, or object to the form requested and state the form in which it intends to produce the ESI, provided that it must be produced either in the form in which it is ordinarily maintained or in a form that is "reasonably usable."[1] In the event the parties disagree about the form in which the ESI is to be produced, the

[1] However, the responding party may not convert ESI from the form in which it is normally maintained to a different form that is "reasonably usable" if such conversion degrades the information or adversely impacts its searching functions. *See* F.R.C.P. 34(b) at Advisory Committee Notes to 2006 Amendment ("[T]he 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.").

parties must meet and confer before the requesting party may file a motion to compel. On a motion to compel, the court is not bound to require production in any of the forms proposed by either party.

I. Rule 37(f)

> *Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.*

While Rule 37(f), on its face, appears to provide a valuable safe-harbor in the event of inadvertent destruction of ESI based upon the routine operation of a party's electronic information system, the safe-harbor may be construed narrowly by the courts. First, Rule 37(f) only provides that, absent exceptional circumstances, a court may not impose sanctions "under these rules" in the event of an inadvertent destruction. Thus, a party may still be subject to sanctions under other sources of authority, including the inherent power of the courts, or applicable rules of professional responsibility.

Second, the safe-harbor may be restricted by the reference to "good-faith." According to the Advisory Committee Notes:

> Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. . . . When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold."

F.R.C.P. 37(f) at Advisory Committee Notes to 2006 Amendment.

In *Doe v. Norwalk Comm. College*, 2007 WL 2066497 (D. Conn. July 16, 2007), the court quoted the Advisory Committee Notes in holding that the defendants were not entitled to take advantage of the Rule 37(f) safe harbor because the defendants failed to suspend destruction of ESI and the safe harbor requires a party "to act affirmatively to prevent the system from destroying or altering information, even if such destruction would occur in the regular course of business." *Id.* at *4.

J. Rule 45

Rule 45, governing subpoenas, contains numerous technical amendments that are intended to parallel the amendments discussed above with respect to discovery of ESI from parties. Specifically, the amendments provide the following with respect to subpoenas:

- The party issuing the subpoena may designate the form or forms for production of ESI;

- The person served with the subpoena may object to the requested form or forms;

- If the party issuing the subpoena does not designate a form for the production of ESI, the responding party must provide such information in the form in which it is usually maintained or in a form or forms that are "reasonably usable;"

- The responding party need not produce ESI that is "not reasonably accessible," unless the court orders such discovery for good cause shown, in a manner that will protect a nonparty from significant expense;

- A subpoena may request testing or sampling, as well as inspection or copying; and

- The Rule establishes a procedure for the responding party to assert attorney-client privilege or the work product doctrine with respect to documents inadvertently produced in response to a subpoena

IV. INITIATING AND MANAGING THE LEGAL HOLD PROCESS

A. What is A Legal Hold?

A "legal hold," also sometimes referred to as a "litigation hold" or a "records retention directive," is a communication to a party's employees that suspends the party's routine document retention policy in connection with an actual or reasonably anticipated litigation matter. A legal hold is not the same thing as a document retention policy, but rather operates as an exception to a company's standard document retention policy.[2] **While legal holds are not unique to the ESI context, they obtain a heightened degree of importance in connection with ESI due to the risk that volumes of potentially relevant information could be inadvertently destroyed with a few keystrokes on a computer keyboard or due to the automatic operation of certain electronic systems.**

While legal holds must reflect the particularities of the specific actual or anticipated litigation, as well as a party's individual circumstances, there are certain factors that should be addressed in most legal holds:

- Identification of all custodians likely to have relevant ESI (as well as paper documents) that should receive a copy of the legal hold (it is important to include a key person from the IT department)

- A clear non-legalistic description of the subject matter and categories of documents to be segregated and preserved, preferably in a bullet point or list format

[2] A document retention policy sets forth the length of time that various categories of a company's records should be retained, based upon applicable federal and state statutes, regulations and other law, as well as the company's particular business needs. Document retention policies are discussed more fully in Section V.A. of this article.

- A plain language description of the types of information (both ESI and paper documents) that are covered by the legal hold

- A description of the sources of information that need to be searched (e.g., laptops, home computers used for business purposes, personal digital assistants, etc.)

- Relevant time period

- Contact information for person who can answer any questions

- Reminder of potential severe consequences for failure to comply with legal hold

B. Initiating the Legal Hold Process

A party should initiate the legal hold process, and suspend its standard document retention policy with respect to ESI and other documents covered by the legal hold, "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." *Zubulake v. UBS Warburg LLC ("Zubulake IV")*, 2003 WL 22410619, *2-3 (S.D.N.Y. Oct. 22, 2003).

While it is clear that a legal hold should be put in place when a party is served with a complaint, there is no bright line rule indicating "when a party should have known that the evidence may be relevant to future litigation." **As one court recently observed, when and whether a pre-service obligation to preserve arises, "must be guided by the facts of each case."** *Cache La Poudre Feeds, LLC v. Land O' Lakes, Inc.*, 2007 WL 684001, *7 (D. Colo. March 2, 2007).

In *Zubulake IV*, the court found that the duty to preserve arose when plaintiff's supervisors became aware of the likely possibility of litigation, rather than when plaintiff filed an EEOC complaint several months later. *Zubulake IV*, at *2-3. However, in *Cache La Poudre Feeds*, the court determined that the duty to preserve was triggered by plaintiff's filing of its complaint, rather than any earlier point during a two-year period where the plaintiff exchanged letters with defendant which indicated that plaintiff preferred and was willing to negotiate a business solution to the parties' dispute. *Cache La Poudre Feeds*, at *8-10. While future cases should provide additional guidance as to when any pre-complaint preservation obligation arises, every situation must be considered on its own facts.

Even when a court determines that a legal hold should have been implemented at an earlier point in time, the courts will generally evaluate whether a failure to timely implement an appropriate legal hold likely resulted in the destruction of relevant evidence before imposing sanctions. *See School-Link Tech., Inc. v. Applied Res. Inc.*, 2007 WL 677647, *4 (D. Kan. Feb. 28, 2007) (refusing to order sanctions where party could not show that failure to implement a legal hold caused destruction of relevant evidence). Nevertheless, given the potentially severe consequences of a failure to preserve information, discussed more fully below, it is advisable to preserve information when in doubt.

Determining the scope of the legal hold generally requires assistance from the IT department and the records management department, as well as the legal department, which may seek input from outside counsel. The legal hold should cover appropriate types and sources of information and should be distributed to all custodians potentially possessing relevant information. Particularly because legal holds are issued at the very start of a litigation, or even before formal litigation has commenced, any errors should be on the side of additional preservation. As the case progresses and discovery proceeds, the issues will come into focus, potentially enabling a narrowing of the types and sources of information to be preserved. Where mere preservation of ESI presents a potentially undue burden or cost, a party should raise the issue with the opposing party as early as possible, and certainly by the Rule 26(f) conference, and seek relief from the court as appropriate.

C. Managing the Legal Hold Process

As discussed above, a party needs to ensure that its legal hold is distributed to all persons who likely possess relevant ESI and other documents. However, merely sending out a blanket email attaching a legal hold, in many instances, will be inadequate to satisfy a party's obligation to preserve records. For example, in *United Medical Supply Co., Inc. v. U.S.*, 2007 WL 1952680 (Fed. Cl. June 27, 2007), the court sanctioned the government for failure to ensure that a legal hold was received and followed by the recipients, particularly when the email was returned as undeliverable with respect to several intended recipients and when the government reasonably knew that other intended recipients did not routinely review their email.

Therefore, the legal hold should be distributed in a manner that ensures it is received by the intended recipients. While an email distribution may be sufficient for certain parties or for certain employees, a party may need to distribute the legal hold by facsimile, by mail, or inter-office mail, or by some other means that is likely to reach certain groups of intended recipients.

Where feasible, delivery of the legal hold should be followed by confirmation. Many companies are electing to attach confirmation pages to the legal hold notices, which must be signed and returned by the recipients as a verification that they have received and complied with the legal hold. When an employee with records that are key to a dispute may soon be departing a company and subsequently difficult to reach, it may be appropriate to obtain a signed declaration or affidavit setting forth the employee's pre-departure record preservation efforts.

After initial distribution and confirmation or verification of the implementation of a legal hold, periodic follow up should be performed, particularly where the relevant information is contained in documents that are being created on an ongoing basis, rather than in a discrete set of historical documents and ESI. New employees who are likely to be custodians of relevant information should be provided with a copy of the legal hold at the time they are hired.

When a litigation matter is resolved, it is equally important that ESI and other documents be released from the legal hold and processed in accordance with the company's standard document retention policy, provided that such information is not the subject of a separate, still

effective, legal hold. When companies fail to handle released documents in accordance with their standard document retention policies, they run the risk of creating a larger set of potentially responsive documents in connection with future unanticipated litigation matters.

D. Potential Consequences of Failure to Implement Effective Legal Hold

A party may be subject to a variety of severe consequences for failure to implement an effective legal hold.

1. Spoliation Claims

Failure to adequately preserve information can lead to spoliation claims, which tend to become a case within a case. "Spoliation refers to the destruction or material alteration of evidence or the failure to preserve the property for another's use as evidence in pending or reasonably foreseeable litigation." *Broccoli v. Echostar Communications Corp.*, 229 F.R.D. 506, 510 (D. Md. 2005) (awarding plaintiff its reasonable attorneys' fees due to spoliation of evidence by defendant). Sometimes a party may face a potentially greater liability from a spoliation claim than from the underlying action. *See, e.g., In re Prudential Insurance Company of America Sales Practices Litigation*, 169 F.R.D. 598, 616-17 (D.N.J. 1997) (requiring defendant to pay $1 million where its document destruction hindered the administration of justice).

In some cases, instructions issued by the court as a result of spoliation can lead to extraordinary liability determinations. For example, in *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, Case No. 502003CA005045XXOCAI (Fla. Cir. Ct. 2005), the court found that Morgan Stanley failed to comply with discovery orders relating to the production of ESI. The court granted an adverse inference order, reversed the burden of proof, and read an instruction to the jury that it could consider Morgan Stanley's discovery violations in determining whether an award of punitive damages was appropriate. The jury subsequently returned a verdict for $604 million in compensatory damages and $850 million in punitive damages. On appeal, Morgan Stanley challenged the propriety of the sanction for discovery misconduct. However, because the court of appeals determined that plaintiff failed to prove any compensatory damages, it reversed and remanded with instructions to enter judgment for Morgan Stanley and did not address the propriety of the sanction. *Morgan Stanley & Co., Inc. v. Coleman (Parent) Holdings, Inc.*, 955 So.2d 1124 (Fla. App. 4th Dist. Mar. 21, 2007), reh'g denied. Notwithstanding the reversal, the *Morgan Stanley* case provides a cautionary tale regarding the potential consequences of spoliation. Another potential consequence is being forced into an unfavorable settlement as a result of spoliation issues.

2. Monetary Sanctions

Monetary sanctions of varying amounts are perhaps the most common consequence of failure to adequately preserve information in connection with an effective legal hold. In *Cache La Poudre Feed*, the court ordered that the defendant pay the plaintiff $5,000 plus additional court reporter fees and transcript costs as a sanction for "Defendants' failure to implement and monitor an adequate record preservation program" where the Court found that such conduct did not substantially prejudice Plaintiffs' case. Higher monetary sanctions have been awarded where

there was a greater likelihood of prejudice or where the court had issued an order regarding the preservation of evidence. *See, e.g., United States v. Philip Morris USA, Inc.*, 327 F. Supp. 2d 21, 26 (D.D.C. 2004) (imposing a monetary sanction of $2,995,000).

3. Adverse Inferences

Another potential consequence is an instruction to the jury that it should assume that the destroyed materials would have been harmful to the party that failed to preserve the information. For example, in *In re NTL, Inc. Sec. Lit.*, 2007 WL 241344 (S.D.N.Y. Jan. 30, 2007), the court issued sanctions including an adverse inference instruction with respect to destroyed email where the party failed to preserve documents to which it had access based upon an agreement with a successor company.

4. Other Potential Sanctions

Courts also have the authority and discretion to award other types of sanctions, including a prohibition on the use of particular types of information in pursuing or defending the case. *See Thompson v. United States*, 219 F.R.D. 93, 104 (D. Md. 2003) (when a party discovered 80,000 email records on the eve of trial, court granted a motion *in limine* precluding use of the email as evidence at trial or for preparing or refreshing the recollection of witnesses). **In the most extreme circumstances, a court may grant summary judgment or a dismissal.**

E. Pro-actively Managing the Legal Hold Process

The foregoing sections discussed initiation and management of the legal hold process once a party is aware of, or reasonably aware of the likelihood of, litigation. However, handling legal holds on an *ad hoc* basis as litigation arises may result in some or all of the following consequences: (a) delays in distribution of the legal hold; (b) confusion among recipients resulting from inconsistent legal hold forms and procedures; (c) greater risk for errors in implementation of legal holds; and (d) increased costs from a global legal hold perspective. Many of these consequences, as well as the potential for sanctions discussed above, can be avoided or minimized by developing a consistent legal hold process.

The best time to create a standardized legal hold process is before you need to initiate your next legal hold. While the details of a legal hold, including the subject matter of the ESI and other documents to be preserved, needs to reflect the particular circumstances of the actual or anticipated litigation, there are many important steps you can take before the need for the legal hold arises:

- Prepare a model form legal hold, with blanks that can be completed based upon the particular circumstances of the litigation triggering the obligation to preserve information

- Determine an effective method to promptly distribute legal holds to various parts of your organization (e.g., headquarters, other offices, “the field,” etc.)

- Designate a point person for legal hold compliance

- Understand your company's policy regarding retention and destruction of ESI
- Determine one or more corporate designees for depositions regarding ESI[3]
- Train employees regarding the legal hold process, in conjunction with a reminder regarding the company's standard document retention policy
- Run a mock legal hold process to gauge its effectiveness
- Coordinate with outside counsel and consultants so they understand your legal hold process and will be able to assist on short notice

V. STRATEGIC CONSIDERATIONS

The 2006 amendments to the Rules, and the developing case law regarding the implementation and management of legal holds, highlight the need for companies to understand their ESI. This section addresses some strategic considerations for strengthening a party's position with respect to its ESI.

A. Managing Electronically Stored Information for Effective Use in Litigation

There are a number of steps that companies can take to ensure they have the strongest possible position with respect to their ESI. Primary focal points include managing what becomes part of the company's ESI, having a functional and effective document retention policy, and understanding the landscape of the company's ESI.

Perhaps the most important, yet most overlooked, tool for managing ESI is taking steps to have an impact on what becomes part of a company's ESI. Given the expense and potential liabilities arising from unnecessary volumes of ESI, companies should consider policies, procedures, and training relating to the following issues:

- *Prohibiting or minimizing personal use of the company's email system.* In addition to creating additional volume of ESI that costs money to store and process, personal emails may be captured in ESI collections in litigation, increasing the volume of data that must be reviewed and creating the potential for disclosure of personal information.
- *Encouraging employees to send email to the smallest number of necessary recipients.* It is very easy to include additional recipients on an email

[3] Under F.R.C.P. 30(b)(6) and equivalent state rules, corporations and other legal entities may be required to designate an individual to testify regarding topics specified in a notice. When disputes arise regarding ESI, parties are frequently requested to designate a witness to testify about the party's ESI, including the retention, preservation and gathering of ESI for production. Selecting one or more potential witnesses as a company's designated ESI witnesses, prior to the onset of litigation, facilitates oversight of the process and enhances the company's ability to designate a knowledgeable person with minimal research and preparation.

transmission, to send an email to a distribution list rather than specific individuals, or to "reply all" when a reply could have been limited to the sender of the email. Adding recipients creates additional copies of the same document. While parties in litigation may agree to removal of duplicates (often referred to as "de-duping") in connection with production of ESI, some parties may insist that de-duping be performed only on a custodian basis, rather than across all custodians.

- *Conducting email etiquette training and refresher courses.* Due to the informal nature of email, text messaging, and other forms of electronic communication, people often write things that they would not include in formal correspondence, or say things that may more easily be misinterpreted.

Designing, and following, an effective document retention policy is likewise very important. Some companies retain ESI which is no longer reasonably accessible, no longer has any business value, or is not indexed in any meaningful manner and has unknown contents. **While a company almost certainly would not attempt to access such information for its own uses, it could be forced to access such information in the context of litigation.** Even with respect to ESI or documents that are "accessible," if there is no legal requirement or business justification for its retention, the storage, administrative and other costs of retaining such information may exceed any potential benefits associated with its retention. Therefore, all companies need a document retention policy that adheres to any applicable legal requirements and reflects the particular company's business needs. However, to be truly effective, the policy must be implemented and followed. Where possible, the document retention policy should be automated to minimize the risk of error.

As suggested above in the discussion of the Rules and effective management of the legal hold process, companies also need to continually have a thorough and current understanding of their ESI. **Ideally, the ESI would be inventoried and documented so that persons outside of the IT department, including counsel, could quickly understand the company's types of ESI, its sources of ESI, and how its ESI is created, retained and destroyed.** In order to effectively implement a legal hold, a company's IT personnel need to understand how to suspend select portions of the company's information systems in order to avoid the inadvertent deletion or overwriting of relevant information. The company needs to explore ahead of time how to best implement a limited suspension of such processes while causing minimal disruption and interference to the company's ongoing business operations. The company needs to be prepared to effectively implement a legal hold by taking some of the additional pro-active steps discussed above.

Finally, in order to strengthen its position at the Rule 26(f) conference, the company needs to be aware of any limitations and weaknesses pertaining to its ESI retention so that it can equip its counsel for negotiating reasonable discovery processes with respect to its ESI. The company should pre-plan its preferred methods for handling discovery of ESI and be prepared, with its counsel, to address ESI discovery issues early in the litigation. Having a thorough understanding of the company's ESI, including where particular categories of information are maintained, will also enable a company to assist its counsel in efficiently locating and organizing information that may be useful to any claims or defenses available to the company.

When it comes to production of ESI, companies should take the following steps to ensure its preservation and production processes are defensible:

- Preserve accessible and inaccessible information that may be relevant
- Ensure that less-obvious sources of information are not overlooked
- Follow a process that can be defended, if challenged
- Document preservation and production efforts

Taking these proactive steps with respect to ESI is not just good litigation and risk management strategy, but also good business strategy because it can help minimize business disruption in connection with future litigation and is consistent with establishing good business practices.

B. Protecting Your Company And Its Confidential Information

The discussions above regarding managing ESI and the legal hold process are important steps to protecting your company in litigation. Another important consideration is ensuring adequate protection for your company's confidential information. Because ESI may be easily copied and transmitted, with limited ability to trace the origin of its transmission, companies and their counsel must be particularly sensitive to protecting confidential ESI that is to be produced in litigation. Concerns about the security of confidential ESI are heightened when producing documents in native format (i.e., the format in which the documents were created and retained, such as Word or Excel) because there is currently no effective mechanism for including a "confidential" label on ESI produced in native format.

Some considerations for protecting confidential information should be raised early in the litigation, including:

- A stipulated protective order governing confidential information.
- Whether confidential information, or particular types of confidential information, should be produced in a format that facilitates "confidential" branding, rather than in native format.
- Production of documents with MD5 hash values[4] that allow the producing party to determine whether a document has been altered after production.

[4] MD5 hash values are unique sequences of numbers and letters, created using hash algorithms, that identify any amount of data, from a single sentence email to an entire hard drive of data. *See* Craig Ball, *Ball in Your Court: In Praise of Hash*, Law Technology News (Nov. 2006). MD5 hash values can be used as electronic fingerprints because the MD5 hash value of a data set changes whenever any of the data is altered. *Id.*

VI. CONCLUSION

In the short run, some parties may seek to avoid some of the costs and burdens associated with the discovery of ESI by seeking to resolve their disputes in arbitration or in state courts, rather than in federal courts where the action will be governed by the Rules. However, some state courts have already adopted provisions governing the discovery of ESI that are comparable to the Rules, and arbitration increasingly is adopting many of the processes and procedures used in courts. Therefore, companies need to understand the Rules, the legal hold process, and the landscape of their ESI so that they can make ESI an asset, rather than a liability, in litigation.

DLA PIPER

EVERYTHING MATTERS

E-Discovery:

The Federal Rules, The Legal Hold,
and Strategic Considerations

September 27, 2007

Overview

EVERYTHING MATTERS

- Introduction to E-Discovery
- 2006 Amendments to the Federal Rules of Civil Procedure
- Initiating and Managing the Legal Hold Process
- Strategic Considerations

Introduction to E-Discovery

EVERYTHING MATTERS

- Electronically Stored Information ("ESI") added to F.R.C.P. in 2006
- ESI is a broad term that "includes any type of information that is stored electronically."
  - Source: Advisory Committee Notes to 2006 Amendments
- ESI is intended to be broad enough to cover all types of existing computer-based information, as well as all future developments

Introduction to E-Discovery

EVERYTHING MATTERS

- Primary differences between discovery of ESI and traditional paper discovery:
  - Volume of information
  - Sources of information
  - Metadata
  - "Smoking guns"
  - Cost of production

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 16(b) [Scheduling Orders]:
  - Specifically addresses ESI
  - Goal is to involve court early to minimize disputes regarding production of ESI
  - Adds reference to agreements regarding privilege
  - Lays foundation for orders addressing inadvertent production

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 26(a)(1) [Initial Disclosures]:
  - ESI subject to mandatory initial disclosures
  - Parties must voluntarily provide, or identify, ESI that they may use to support claims or defenses
  - Signals importance of understanding own ESI, including creation, retention, destruction, and retrieval

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 26(b)(2)(B) [Limitations on Discovery of ESI]:
  - Party need not produce ESI that is "not reasonably accessible" due to undue burden or cost
  - Party asserting ESI is "not reasonably accessible" bears burden of establishing inaccessibility
  - Even if party establishes ESI is "not reasonably accessible," court may still order its production for "good cause"
  - However, court has authority to limit amount, type, or sources of information that party must access and produce
  - Court may also shift costs as it deems appropriate

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 26(b)(5)(B) [Procedure for Asserting Inadvertent Production of Privileged Materials]:
  - Amendment recognizes substantially greater risk of inadvertent production of privileged information in ESI due to volume and hidden data
  - Establishes procedures in the event of inadvertent production
  - Party asserting inadvertent production must notify other party of production and basis for asserted privilege
  - Receiving party must return, sequester, or destroy the information (and may not use it) until privilege claim is resolved

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 26(b)(5)(B) [Procedure for Asserting Inadvertent Production of Privileged Materials] (cont.):
  - Receiving party may promptly present the information to court under seal for resolution of dispute
  - If receiving party has disclosed the information prior to receiving notice, must take reasonable steps to retrieve
  - Producing party must preserve the information until claim is resolved
  - Rule is merely procedural; substance of waiver governed by applicable law and any agreements of the parties, including agreements memorialized in F.R.C.P. 16(b) Scheduling Order

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 26(f) [Conference of the Parties Regarding Discovery Issues]:
- Parties are required to discuss "any issues" relating to disclosure or discovery of ESI
- Issues may include:
  - Form or forms in which ESI will be produced
  - Whether metadata will be produced
  - Whether any ESI is "not reasonably accessible" due to burden or cost
  - Any preservation issues presented by ESI

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 26(f) [Conference of the Parties Regarding Discovery Issues] (cont.):
  - Topics and time period for information covered by ESI
  - Search terms
  - Sources of ESI
  - Cost sharing

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 26(f) [Conference of the Parties Regarding Discovery Issues] (cont.):
  - Parties are required to discuss "any issues" relating to discovery-related privilege issues
  - "Clawback agreements"
  - "Quick peek" agreements
  - Agreements can be entered as part of F.R.C.P. 16(b) Order and work with procedure in F.R.C.P. 26(b)(5)(B)

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 33(d) [Option to Produce Business Records in Response to Interrogatories]:
  - In response to interrogatory, party may respond by specifying ESI from which the answer may be ascertained
  - However, burden of ascertaining the answer must be substantially the same for requesting party as for responding party
  - Where ESI must be accessed in a proprietary database or program, responding party may be required to grant access to its system if it seeks to rely on F.R.C.P. 33(d)
  - In many situations, responding party may prefer to derive answer itself

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 34(a) [Testing or Sampling ESI]:
  - ESI may be tested or sampled (as well as inspected or copied)
  - May provide a less burdensome means for locating relevant information contained in ESI
  - Not intended to provide a routine right of access to an opposing party's computer systems
  - But, access may be appropriate in some circumstances

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 34(b) [Form of Production—"Battle of the Forms"]:
  - Requesting party may specify preferred form or forms of production
  - Responding party may object to requested form
  - If responding party objects, or if no form was specified by requesting party, responding party should inform requesting party of intended form of production well in advance of actual production
  - Responding party must produce in form or forms in which ESI is ordinarily maintained or in form or forms that are reasonably usable
  - A party need not produce same ESI in more than one form

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 37(f) [Safe-harbor Covering ESI]:
  - Provides that court may not impose sanctions under F.R.C.P.s when ESI is lost due to the routine, good-faith operation of an electronic information system
  - However, only applies to sanctions under F.R.C.P.s
  - "Good-faith" operation requirement may be narrowly construed to require affirmative efforts to suspend automatic operation of electronic information system
  - *Doe v. Norwalk Comm. College*, 2007 WL 2066497 (D. Conn. July 16, 2007)

2006 Amendments

EVERYTHING MATTERS

- F.R.C.P. 45 [ESI Covered by Subpoenas]:
  - Party issuing subpoena may designate form or forms for production
  - Person served with subpoena may object to the requested form or forms
  - Responding party must produce in form in which information is usually maintained or in a form or forms that are "reasonably usable"
  - Responding party need not produce ESI that is "not reasonably accessible," unless court orders discovery for good cause shown; manner of production should protect nonparty from significant expense
  - Establishes a procedure for responding party to assert inadvertent production of privileged ESI

Initiating and Managing the Legal Hold Process

EVERYTHING MATTERS

- A "legal hold" is a communication that suspends an entity's routine document retention policy in connection with an actual or reasonably anticipated litigation matter
- "Legal holds" are also referred to as "litigation holds" or "record retention directives"
- "Legal holds" have received much greater attention in connection with ESI due to the ease of inadvertent destruction of ESI

Initiating and Managing the Legal Hold Process

EVERYTHING MATTERS

- Factors to be addressed in most legal holds:
  - Identification of key custodians (including someone in the IT department)
  - Clear non-legalistic description of the subject matter and categories of documents to be segregated and preserved, preferably in a bullet point or list format
  - Plain language description of the types of information (e.g., email, electronic agreements, etc.) that are covered by the legal hold
  - Description of the sources of information to be searched (e.g., laptops, home computers used for business purposes, personal digital assistants, etc.)
  - Relevant time period
  - Contact information for person who can answer any questions
  - Reminder of potentially severe consequences for failure to comply with legal hold

Initiating and Managing the Legal Hold Process

EVERYTHING MATTERS

- Initiating the process:
  - Initiate legal hold when relevant to litigation or when relevant to anticipated future litigation
  - No bright line rule
  - Fact-specific inquiry
  - *Zubulake IV; Cache La Poudre Feeds, LLC; School-Link Tech., Inc.*
  - Future case law to provide additional guidance, but will remain fact-specific

Initiating and Managing the Legal Hold Process

EVERYTHING MATTERS

- Managing the Process:
  - Legal hold should be distributed in manner that ensures it is received by intended recipients
  - Use of returnable confirmation forms is recommended
  - Periodic follow up communications
  - Provide to new employees likely to be custodians of relevant information at time of hire
  - Return information to standard document retention policy when legal hold no longer applies

Initiating and Managing the Legal Hold Process

EVERYTHING MATTERS

- Potential Consequences of Failure to Implement Effective Legal Hold:
  - Spoliation Claims
  - Monetary Sanctions
  - Adverse Inferences
  - Other Potential Sanctions

Initiating and Managing the Legal Hold Process

EVERYTHING MATTERS

- Steps to Pro-actively Manage the Legal Hold Process:
  - Prepare a model form legal hold
  - Determine an effective method to distribute the legal hold
  - Designate a point person for legal hold compliance
  - Understand your company's policy for retention and destruction of ESI
  - Determine one or more corporate designees for depositions regarding ESI
  - Employee training
  - Run a mock legal hold exercise
  - Coordinate with outside counsel and consultants

Strategic Considerations

EVERYTHING MATTERS

- Front-end management of ESI:
  - Prohibit or minimize personal use of company's email system
  - Encourage employees to send email to the smallest number of necessary recipients
  - Conduct email etiquette training and refresher courses

Strategic Considerations

EVERYTHING MATTERS

- Document retention policy:
  - Should comply with legal requirements and serve business needs
  - Must be implemented and followed
  - Where possible, automate process to minimize risk of error

Strategic Considerations

EVERYTHING MATTERS

- Understand your ESI:
  - Inventory sources of ESI
  - Inventory types of ESI
  - Document sources and types of ESI
  - Ensure your IT personnel know how to suspend portions of your information systems, while minimizing impact on business operations

Strategic Considerations

EVERYTHING MATTERS

- Production of ESI:
  - Preserve accessible and inaccessible information that may be relevant
  - Ensure that less-obvious sources of information are not overlooked
  - Follow a process that can be defended, if challenged
  - Document preservation and production efforts

Strategic Considerations

EVERYTHING MATTERS

- Protecting confidential information:
  - Stipulated protective order governing confidential information
  - Potential production of confidential information in a format other than native format to facilitate confidential branding
  - Use of MD5 hash values

Selected Resources

EVERYTHING MATTERS

- Advisory Committee Notes to the 2006 Amendments (available at http://www.uscourts.gov/rules/congress0406.html)
- J. Edwin Dietel, *Designing an Effective Records Retention Compliance Program*, (West, updated current through Dec. 2006)
- http://www.abanet.org/litigation/issuecenter/issue_ediscovery.html
- Craig Ball, *6 on EDD: Six Articles on Electronic Data Discovery* (available at http://www.craigball.com/Six_on_EDD-February_2007.pdf)
- http://www.thesedonaconference.org

EVERYTHING MATTERS

- Questions?