E-Discovery

John Wesley Raley
Jackie Cooper
COOPER & SCULLY, P.C.
Founders Square
900 Jackson Street
Suite 100
Dallas, Texas 75202
(214) 712-9500
(214) 712-9540 (fax)

The Cooper & Scully, P.C. Transportation Seminar
June 20, 2008

TABLE OF CONTENTS

E-DISCOVERY

I. INTRODUCTION

"E-Discovery" refers to the practice of using electronically stored information as evidence in litigation. E-discovery incorporates different methods of technology including e-mails, word processing files, accounting programs, websites and raw data, among other things. E-discovery is becoming a more widely used practice as a result of the world's progression towards a technology driven society/economy. In contrast to "paper discovery," electronically stored information can lend itself to efficient and comprehensive organization. However, the issues which can arise from e-discovery are innumerable and are beginning to garner much attention in federal and state courts.

Electronically stored information is more difficult to identify, manage and dispose. For example, a deleted document is still recoverable until it is written over. Many systems automatically update, copy and transfer electronic files, all of which alters their content. Electronically stored information may also be found in handheld wireless devices, mobile telephones and audio systems such as voice mail, as well as in desktop or laptop computers. Another consideration involves "metadata," which is information that describes how, when and by whom a document was collected, created, accessed, modified and formatted. In a patent infringement case, the court found that the original electronic media containing metadata would be more relevant to the plaintiff's infringement claims than print-outs because they would allow him to "piece together the chronology of events and figure out, among other things, who received what information and when."[1]

Although this area of the law has been developing relatively slowly until recently, a corporate scandal in 2002 involving paper documents led Congress to look more closely at the need for document retention policies. The result ultimately impacted the formulation of policy related to electronically stored documents. The accounting firm Arthur Andersen disclosed that its employees had destroyed documents relating to Enron. Congress responded by passing the Sarbanes-Oxley Act, which extended the reach and lengthened the potential penalties of the obstruction statutes.[2] The intent of the Act was to focus on the securities industry and financial services, but, incidentally, the Act is most applicable to regulated industries, such as health care. The effect of the Act was to encourage the creation of retention policies and mandate compliance with the policies.

II. Rules of Electronic Discovery

A. Federal Rules of Civil Procedure

The United States Supreme Court approved E-Discovery amendments, concerning the discovery of "electronically stored information," which went into effect on December 1, 2006. The amendments involved six Federal Rules of Civil Procedure, including Rules 16, 26, 33, 34, 37, and 45, as well as Form 35. As a result of the changes, Federal Courts must accommodate modern business practices of electronically-based businesses and address the importance of computerized information and the increasing costs of using E-technology.

The phrase "electronically stored information" is meant to include any type of information that can be stored electronically and is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and technological developments.

The amendments cover five related areas:

- definition of discoverable material;
- early attention to electronic discovery;
- discovery of electronically stored information from sources that are not reasonably accessible;
- procedure for asserting claim of privilege or work product protection after production; and
- a "safe harbor" limit on sanctions under Rule 37 for the loss of electronically stored information as a result of the routine operation of computer systems.

Rule 16 concerns scheduling orders that may address "disclosure or discovery of electronically stored information and any agreements for asserting claims of privilege or protection as trial-preparation material after production."

Subsection 26(a)-1-B was proposed to replace electronically stored information for data compilations as a category of the required initial disclosures. **Subsection 26(b)-2-B** is affixed to excuse a party from providing discovery of electronically-stored information that is not reasonably accessible because of undue burden or cost, but the burden remains on the producing party to make the required showing. **Subsection 26(b)-5-B** helped provide a procedure for a party to maintain a claim of privilege or of protection

[1] Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., No. 04 C 3109, 2006 WL 665005, at 3 (N.D. Ill. March 8, 2006).

[2] See 18 U.S.C. § 1512.

as trial preparation material concerning any discovery even after it is produced. Lastly, Rule **26(f)**, which is referred to as the "meet-and-confer" rule, requires the parties to meet "as soon as practicable" after the inception of litigation to discuss the scope of e-discovery during the ensuing months. The two sides are to discuss the scope of e-discovery and the types of information sought, and then to disclose the systems the other side maintains and the "native" file format of the documents. A report (Form 35) detailing this "26(f)" conference must then be issued to the court, at which time the judge will consider this information and enter a pre-trial scheduling order pursuant to Rule 16(b). Any issues relating to claims of privilege or protection should also be discussed and memorialized in an agreement, which the parties can request that the court include in a scheduling order. The goal is to encourage the parties to resolve as many discovery issues as possible at the beginning of the litigation. This includes attorneys and their clients considering issues, involving technical personnel and becoming familiar with the company's hierarchy and information systems.

Rule 33(d) was amended to specify that electronically-stored information may qualify as appropriate business records from which an answer to an interrogatory may be derived or ascertained.

Rule 34 addresses production of documents and electronically-stored information, as well as other materials. The amendment references electronically-stored information and provides a procedure for specifying and objecting to the form in which electronic information is to be produced. Subsections of the rule explain that the default manner of production is the manner in which it is ordinarily maintained. A party need not produce the same electronically-stored information in more than one form.

Rule 37(f) states that "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 routine, good-faith operation of an electronic information system."

Rule 45 was changed to incorporate the modifications from Rule 26(b) and Rule 34 as applied to the production of documents by third parties pursuant to a subpoena.

B. Texas Rule of Civil Procedure

The Texas Rules of Procedure first differentiated e-discovery from traditional discovery in 1996.[3] **TEX. R. CIV. P. 196.4** requires production of all responsive electronic data which is "reasonably available to the responding party in its ordinary course of business" and allowing an objection if it cannot be retrieved by "reasonable efforts."

> Electronic or Magnetic Data. To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot-through reasonable efforts-retrieve the data or information requested or produce it in the form requested, the responding party must state an objecting with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.

The rule distinguishes between electronic data that is available in the ordinary course of business (discoverable) and that which is not reasonably available (discoverable only pursuant to a court order). In addition, if the court finds that the information sought is relevant to the case, then the court has discretion to order the requesting party to pay the costs of production.[4] Mississippi and California followed suit and enacted similar law differentiating between discovery of electronic documents and hard copies.[5]

C. Other States

States courts have adopted rules governing E-discovery. New rules in Idaho and New Jersey took effect in 2006, and rules in Indiana, Minnesota, Montana and New Hampshire began in 2007. Arizona's rules became effective in 2008. Maryland, Nebraska and Ohio have proposed new rules, while groups in California, Illinois, Tennessee and Washington are studying the issue.

III. Understanding and Applying E-Discovery Law in Transportation Litigation

[3] TEX. R. CIV. P. 196.4.

[4] Id.

[5] MISS. RULE CIV. P. 26(b)(5) (2004); CAL. CIV. PROC. CODE § 2017(e) (2004).

Issues involving E-discovery have arisen in the context of most types of law, including transportation law. Cases about transportation can be document-intensive. While many of the documents are on paper, an increasing number of documents and communications, among other things, are being exchanged and stored electronically. Those who manage projects and oversee contractors and subcontractors house massive amounts of documents, plans and correspondence, both on paper and in electronic format. The rules regarding E-discovery apply to all forms of litigation and are especially important when dealing with large amounts of documents and materials accessible to multiple parties. Not only do you have to be aware of your policies, you have to be aware of the policies of those for which you are ultimately responsible.

A. Zubulake- Landmark Case

In Zubulake v. UBS Warbus, LLC,[6] Laura Zubulake was fired after filing a charge of sexual discrimination against her employer, UBS Warbus, with the Equal Employment Opportunity Commission. She sued for sexual discrimination and retaliatory termination. This seemingly straightforward case turned on the many technical electronic discovery issues emanating from a litigant's failure to preserve, and produce, relevant e mails. Ms. Zubulake demonstrated that UBS's backup tapes were likely sources of relevant evidence and should be restored in readable format for use in the case. She discovered that several backup tapes were inexplicably missing, and that several e mails had been deleted.

As a result, Ms. Zubulake filed a motion for sanctions where the court examined, among other things, the remedy for UBS's loss of relevant e-mail and the litigants' and counsel's obligations to help prevent such loss. Judge Scheindlin stated:

> [W]hile a litigant is under no duty to keep or retain every document in its possession ... it is under a duty to 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.[7]

The court held that once a party reasonably anticipates litigation, it should suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. Further, the court held that UBS had breached its duty to preserve relevant e-mails and that an adverse inference instruction charge to the jury was warranted. The jury was permitted to infer that the lost e-mails would have been favorable to Zubulake. The court observed that "[i]n practice, an adverse inference instruction often ends litigation--it is too difficult a hurdle for the spoliator to overcome."[8] The court proved right: On April 6, 2005, the jury awarded Ms. Zubulake $29.1 million--, $20 million of which was for punitive damages.

In addition to the assessment of sanctions, the *Zubulake* court addressed allocation of costs between parties in retrieving electronic data. As a general rule, the responding party bears the cost of producing documents requested during discovery. However, in *Zubulake*, UBS said that such a rule would be unfair in that case because it estimated that the cost of restoring e-mails on its backup tapes, a time-consuming process, would be approximately $170,000, plus attorney and paralegal review time. The court determined that, because Ms. Zubulake demonstrated that UBS unreasonably failed to maintain all relevant information, UBS should bear 75 percent of the cost of retrieving the data contained on its backup tapes.

The court drew a distinction between production of accessible electronic data, such as active data on a computer hard drive, and non-accessible electronic data, such as data on backup tapes or residual data ostensibly "deleted." Because Ms. Zubulake sought to discover UBS's backup tapes containing e-mails that she knew once existed but were no longer readily accessible on the company's hard drives, the court

[6] Zubulake was actually decided over the span of 5 opinions on various issues. In the interest of space, all five opinions are referred to collectively as Zubulake. For further discussion on these cases see Janet Ramsey, Technology and the Law: Zubulake V: Counsel's Obligations to Preserve and Produce Electronic Information, 84 MICH. BAR J. 26, 27 (2005). See also Zubulake v. UBS Warburg LLC (Zubulake I), 217 F.R.D. 309 (S.D. N.Y. 2003) (listing seven factor test for cost shifting in electronic discovery disputes); Zubulake v. UBS Warburg LLC (Zubulake II), 2003 WL 21087136 (S.D.N.Y. May 13, 2003) (addressing non-ediscovery issues); Zubulake v. UBS Warburg LLC (Zubulake III), 216 F.R.D. 280 (S.D. N.Y. 2003) (applying the seven factor test from Zubulake I. Zubulake v. UBS Warbus, LLC (Zubulake IV), 220 F.R.D. 212 (S.D.N.Y. 2003) (all costs and fees awarded to plaintiff re depose individuals about newly discovered e mails); Zubulake v. UBS Warbus LLC (Zubulake V), 229 F.R.D. 422 (S.D.N.Y. 2004) (jury empanelled to hear the case will be given an adverse inference instruction).

[7] Zubulake v. UBS Warbus, LLC (Zubulake IV), 220 F.R.D. 212, 217 (S.D.N.Y. 2003).

[8] See Zubulake IV, at 219.

focused on how to allocate between the parties the costs of retrieving such data.

When dealing with readily accessible data, the presumption that the responding party pays the cost of its retrieval is not affected. But when a litigant seeks to discover non-accessible data, a weighted, seven--factor test should be applied to the cost--shifting issue: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the cost of production compared to the amount in controversy; (4) the cost of production compared to the parties' resources; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information.

Basically, the Zubulake court imposed a test that asked of the requesting party: "how important is the sought--after evidence in comparison to the cost of production?"

B. Broccoli-Retention Policies

In an employment discrimination case, *Broccoli v. Echostar*,[9] the court commented that "under normal circumstances . . . [the retention policy] may be a risky but arguably defensible business practice undeserving of sanctions." However, the court held that "Echostar clearly acted in bad faith in its failure to suspend its email and data destruction policy or preserve essential personnel documents in order to fulfill its duty to preserve the relevant documentation for purposes of potential litigation."

According to the retention policy at issue, all items in the "sent items" folder which were more than seven days old were automatically routed to the "deleted items" folder. All items in the "deleted items" folder which were more than 14 days old were automatically purged and became irretrievable. They were not stored elsewhere and there were no backups. Electronic files belonging to former employees were completely deleted 30 days after an employee left.

The court found that management had a duty to preserve employment and termination documents when it learned of the potential litigation, but that little had been preserved and subsequently produced. Echostar admitted that it never issued a company-wide instruction to suspend the destruction of relevant documents.Mr. Broccoli did not prevail on his employment discrimination case; however, he was awarded $16,097 for efforts resulting from Echostar's discovery violations and spoliation of evidence. Therefore, Echostar was not found to be a prevailing party and was not awarded costs.

C. No Question that Electronically Stored Information is a Document

Rules 26(a), 33, 34 and 45 also contain relevant amendments. Among the most notable is that electronically stored information has been added as a separate category of information to be disclosed. This removes all ambiguity as to whether information stored in a particular form constitutes a "document." In addition, the amendments permit (but do not require) the requesting party to specify the form or forms in which electronically stored information is to be produced by both parties and nonparties. The responding party can object to the form of requested production, but the parties must meet and confer in an effort to resolve the matter before the requesting party can file a motion to compel. If the parties cannot reach an agreement, the court might order the form of production.

D. "Reasonably Inaccessible" Data Defined

The amendments to Rule 26(b)(2) essentially construct two tiers of discovery: accessible and inaccessible data. (Note that preservation duties still exist whether sources are "easily accessible" or not. Merely identifying sources of electronically stored information as reasonably inaccessible does not relieve the company of its duty to preserve evidence.) The Rule specifies that a responding party need not produce electronically stored information that it identifies as "reasonably inaccessible because of undue burden or cost." The requesting party can move to compel production, and the responding party can seek a protective order prohibiting production, after the parties confer on the issue.

The factors influencing a determination of reasonable accessibility amount to the difficulty and expense involved in obtaining the information. The phrase "undue burden and cost" has been included to provide context in defining the phrase "reasonable inaccessibility." Ultimately, the burden falls on the responding party to prove that the information is reasonably inaccessible. The responding party must disclose sources of potentially responsive information that are not being searched or produced, and provide detail about these sources. This enables the requesting party to evaluate burdens, determine the likelihood of finding responsive information and decide whether to challenge the designation. The court may still order production, even after a showing that materials are reasonably inaccessible, if the requesting party demonstrates good cause.

[9] Broccoli, et al. v. Echostar Communications Corp., et al., 229 F.R.D. 506 (D.Md. 2005).

E. "Safe Harbor" Provision Offers Some Protection in Cases of Lost Information

Rule 37(f) "provides limited protection against sanctions for a party's inability to provide electronically stored information in discovery when that information has been lost as a result of the routine operation of an electronic information system, as long as that operation is in good faith." This rule intends to address a unique component of electronically stored information: the routine modification and deletion of data that occurs during the ordinary course of business (e.g., e-mails being deleted to create additional space, storage media being recycled on a scheduled basis, etc.). The rule is limited to the loss of electronic information through routine operations. In fact, experts have opined that this rule truly only protects a party when "an act of God, like a flood or house fire" destroys a computer with electronic data on it.[10]

According to the Committee notes, the information must be destroyed as part of a routine procedure. However, even these "routine procedures" are evaluated. Good faith requires a party to intervene and suspend certain aspects of routine operations to prevent loss of information subject to preservation obligations. Upon the imposition of litigation hold (a directive for corporate employees to preserve records and data that might be relevant to litigation), even the most innocuous of data destroying policies must cease. A party must impose restrictions pursuant to agreements established during meet-and-confer sessions and must adhere to these agreements.

Again, this "safe harbor" rule does not give parties the right to destroy data that is not "reasonably accessible," routinely or otherwise, in the ordinary course of business or not. The Committee notes state: "whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible under Rule 26(b)(2) depends on the circumstances of each case." As foreshadowed in *Zubulake* and as contemplated in proposed Rule 26(b)(2), good faith requires a party to preserve information it believes is reasonably accessible under Rule 26(b)(2) or that may become relevant, once a litigation hold is placed.

F. "Clawback" Provision Allows for Do-Over if Accidental or Inadvertent Production

Rule 26(b)(5) is another that seems to be drawn from the Texas Rules of Civil Procedure. Under Texas Rule 193.3(d):

> A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these rules or the Rules of Evidence if--within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made--the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends that response to assert a privilege, the requesting party must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege.

In light of the volume of data being produced in large litigation, both electronic and traditional, Rule 26(b)(5) addresses the inadvertent production of privileged information. If information is produced that is subject to a claim of privilege or work product protection, the producing party can notify the receiving party of this fact, along with the basis for the claim. After being notified, the receiving party must promptly return, sequester or destroy the information and not disclose the information until the claim is resolved. If the receiving party already disclosed the information prior to being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved. The amendment does not address the substantive question of whether privilege or protection has been waived. The amendment allows for a party disputing privilege to submit the document(s) in question to the court for *in camera* review.

G. Discovery Requests

1. The Request for all electronic files and the concern with metadata

Please produce all digital or analog electronic files, including, but not limited to, word-processed files, including drafts *and revisions; all spreadsheets, including drafts, revisions, "deleted" files and file fragments, whether such files have been reduced to paper printouts or not, relevant to this matter, in their native file format.*

When a party requests documents in their native form, metadata becomes a primary concern. Metadata can be obtained or extracted about a file from the primary document or file system from which the

[10] Panel Discussion, E-Discovery Roundtable, September 14, 2006, to be published in issue of TEXAS LAWYER, October 2006.

document is saved.[11] For instance, if a letter dated Jan. 1, 2006, is produced as a paper document, no one will be able to analyze the information that lies behind the document. If this letter, which allegedly cancels an order of widgets which forms the basis of the breach of contract litigation, was actually created in May 2006– after the litigation began–then the metadata showing the document's creation date may be quite relevant or at least afford the opportunity to question the origin of the document.-- Forms of production that allow the requesting party to view these metadata and embedded data are called "native."[12]

Embedded data is "hidden" files contained in the document itself. If you have ever hit "track changes" and made a comment to a document, or have formatted a document, or even hit the "tab" button, that data is contained in the document. The program would not be of much help if it showed such items visibly, but the file keeps track of these modifications behind the scenes. Embedded data, however, is not seen if the document is printed on paper or converted to a .PDF or .TIFF image, or other "read-only" file format. This embedded background information may be relevant to the litigation, however, and this is where the problem arises.

As discussed, everything you type into your computer leaves behind a trail long after you delete it. A possible solution involves using a metadata wiping program. While obviously not to be used in anticipation of litigation, it is a good policy to "wipe" the hard drives of every employee's computer. This erases all of the "notes" and "drafts" taken on an open document, and leaves behind only the finished product. Not only does it prevent one from having to explain internal notations. But, even more practically, it helps cut down on the amount of memory used, which means up-front costs are reduced by minimizing data and storage space. Also, in the event of a search for relevant documents, it will take much less time.

1. Request for Emails

Please produce all of your e-mails, both sent and received, whether internally or externally, all internet and *web-browser generated history files, caches and cookies files generated at the workstation of each employee or created with the use of personal data assistants, such as Palm or Blackberry devices.*

The information previously exchanged via snail mail or in person, is now exchanged via email. But what might serve as a surprise is where all of that goes.

Craig Ball propounded a scary scenario:

> Consider a user who first dipped her toes in the online ocean through Hotmail or AOL. Seeking a faster connection, she switched to a local ISP with cable or DSL service and started downloading e-mail using Netscape Messenger or Microsoft Outlook Express. With growing sophistication, a job change, or new technology at the office, she shifts to Microsoft Outlook via an Exchange server or Lotus Notes via a Domino server. Each of these steps can leave a large "abandoned" cache of e-mail on the user's computer that's fair game for discovery.[13]

Now, imagine how much more work is being done via Blackberry or Palm hand held devices. All of the instant messaging or text messaging that is done on a daily basis.

The next dimension includes e-mail through a third-party vendor (Hotmail, etc.), which is saved on storage media owned by that company; E-mail forwarded from one account to another (from work account to personal account); E-mail threads - where the parties to a conversation keep hitting "reply" and the past messages remain in the foot of the text; E-mails that are saved to the desktop and then burned to a CD; E-mail in Outlook or Lotus Notes that is automatically archived or is "deleted," but sits in the "delete box" for months; attachments or drafts of e-mails; not to mention periodic system or server backups or nightly system updates; and, of course, it is important to remember that more than fifty percent of e-mails sent or received are the product of "Spam."

Search most of the storage media used for email is difficult. Many companies use "back up tapes" each night, which are expensive to search because they cannot be search by keyword.

2. Request for everything else

All other files generated by users through the use of computers and/or telecommunications, including, but not limited to voice mail.[14]

[11] Mary Mack, When Does a Document Become Evidence? E-DISCOVERY ADVISOR MAGAZINE, Volume 02, Issue 01 (2006).

[12] Alan F. Blakley, Document Production in a Strange Native Land, Federal Lawyer (July, 2006).

[13] Craig Ball, A Practical Guide to E-mail Discovery, TRIAL 32-33 (October, 2005).

[14] FED. R. CIV. P. 34(a) specifically provides that requests for "sound recordings" are acceptable.

Some companies with nearly-antiquated voice mail systems may be able to relax at this point. Old voice mail systems would just make sound recordings to a storage drive and erase every few days. The storage devices were unsearchable, except through human transcription, which was tedious and unreasonable task was prohibitive. As technology gets more advanced, the more efficient and cost-effective way to store voice mails is the same way that e-mails and other electronic documents are stored. The new voice mail systems store messages in a sound file that can be exported or translated into any other format, making it easier to be transcribed. Even further, many voice mail systems are developing functions where each person's mail box is compartmentalized and computer-transcribeable, which means, computer-searchable. Each message has its own form of "metadata" as well, including information such as the incoming phone number, the date and time of the call, and the message length.

However, these new systems and the software enabling the search and transcribe functions are very expensive. Even under the new rules, the cost of such production may be prohibitive. However, when specific employees' voice mail boxes have been requested, courts have been liberal in allowing the discovery to take place. As more people are using company cell phones and voice mail boxes are slowly getting bigger and allowing for more storage, and as the line between voice and electronic data storage technology blurs, the possibility of this discovery rises.

It is important to consider these systems when creating a document retention or destruction plan, when implementing a "litigation hold" on your company, and even when considering new technology for your expanding or new business.

H. Protecting Your Company

1. Establish a Good Policy

Please produce all copies of any and all written policies for the retention of documents, for the time period *of* _____ *to* _____.

If your company does not have a document retention policy in place, now is the time to develop one. If your company has a document retention policy, but not everyone (or no one) adheres to it, it is time to implement and enforce it. If your company has a document retention policy, but it is antiquated, it is time to update it. Any of the above actions places your company at risk of:

- Being unprepared for litigation;
- Put in the position of producing damaging information through e-discovery; or
- Spending time and money throughout the discovery process in producing relevant documents or screening for privileges.

In creating a document retention policy, it is most important to recognize that the policy must be followed. Explaining why the retention policy was not followed is more difficult than explaining why there is no policy. Consider the company's unique needs. Speak with the information technology staff. They are in the best position to evaluate the electronic infrastructure because they know:

- What e-mail system is used and how often it backs itself up;
- If the electronic information is all kept on site;
- The storage medium used for each form of data;
- How easy or difficult it is to search each of the storage drives; and
- The mechanisms facilitating internal communications.

However, in order to gain complete knowledge, someone outside of the IT department will need to provide answers to the following:

- How long does your company really need to keep old e-mail files?
- How important is it to back up each system every night?
- Has an employee left and had their system put back into service with another user?

The next step is implementing a temporary litigation hold plan. If an employee hears a rumor of a possible lawsuit being filed by an ex-employee or if a product is released with known defects, it is too late to create a retention plan. Each employee should be notified and trained to follow a litigation hold policy when they are trained regarding the document retention policy. Ideally, the CIO and the intern, and everyone in between would be notified individually within minutes of each other. Form a task force including executives, IT specialists, and other employees to discuss the company's retention needs, with a focus on the following:

- A good policy should spell out the reasons for creating a policy. This statement should address the particular

business needs considered while creating the policy: cost, storage space, expansion, etc.

- A good policy should also indicate the department or specific employees to whom it applies and to whom it does not. Frequently, the IT department should have a different policy from upper-management or the financial department.
- A good policy identifies each document or source and discusses and records the reason for decisions about their various retention periods. For example, personal e-mails should not be saved longer than invoices.
- A good policy addresses the method of retention. When are documents backed up and to what server. Should each version of each document be maintained as long as the final draft? What type of storage media is most appropriate for each type of file? Include a provision that records the "chain of custody" for the media, listing of manipulation done on the data, and the inventory of each location where data is stored. In addition, a log of any automated deletion or separation employed by the IT department should be maintained.
- A good policy addresses issues regarding personal use, confidentiality, and privacy. This is effective in providing each employee with an expectation of the rights they may expect.

Please produce copies of any and all written policies for the destruction of documents, for the time period of _____ to _____.

As discussed, a good document retention policy necessarily involves a methodical destruction of documents. A company must decide what types of files or records must be maintained and for how long. It is important to meet to update methods as the business evolves. In the event of litigation, the other side will ask if such meetings were held in order to undermine the policy itself. The best practice is to keep minutes and results of meetings, and to act on any decisions made. The worst case scenario is to have a functioning destruction policy, but no recorded safeguards regarding when to suspend destruction. Always keep a record detailing any time that destruction or overwriting of documents is suspended. A good record should include the date on which the suspension began. The best response to an opponent's discovery request is to produce a letter dated before the date preservation needed to begin, a log of who needed to be informed and who was actually informed, and some sort of verification that those people received the suspension notice.

2. <u>In the event of litigation</u>

It might be helpful to ask the following question early on in the process of litigation:

- Who are the key players in the case?
- Who are the persons most knowledgeable about ESI systems?
- What events and intervals are relevant?
- What data are at greatest risk of alteration or destruction?
- What steps have been or will be taken to preserve ESI?
- What third parties hold information that must be preserved, and who will notify them?
- What are the data retention policies and practices?
- What are the backup practices, and what tape archives exist?
- What relevant databases exist and what is the best search method?
- What metadata are relevant, and how will it be preserved, extracted and produced?

3. <u>Cost Considerations</u>

With the increase in use of e-discovery in the litigation process and the innovations in the technology associated with e-discovery, the amount of money spent on e-discovery is skyrocketing. According to Socha Consulting, LLC, the estimated revenues for the electronic discovery market rose 56% between 2004 and 2005, to a total of $1.3 billion.[15] The revenues are estimated to rise to over $3.1 billion in 2008. Each case presents a unique cost associated with e-discovery depending on what is deemed relevant by a court and what is requested by the other side. However, the more prepared your company is and the more detailed your company's compliance with the implemented retention policy is recorded the easier it will be to estimate the total cost.

The easiest cost to consider is the "sunk cost" of the storage media required by your company's policy. When first evaluating this cost, it is important to

[15] See http://www.sochaconsulting.com/2006surveyresults.htm (Last visited September 15, 2006).

remember the adage, "you get what you pay for." Storing a majority of your media on back-up tapes may save some cost in the short-run as each tape costs less than $50. However, each tape has the ability to save gigabytes and gigabytes of information, and no way to easily search the contents. Any information on a back up tape should be well organized by department, subject matter, and date. However, by spending more on storage media at the present time, future costs will be significantly reduced, allowing more predictability. If your company decides to use an easily searchable type of storage media, the options during discovery significantly increase while the unexpected costs decrease. The "soft costs" of e-discovery include:

In-house resources

- External E-Discovery services
- Outside counsel fees
- Collection of evidence
- Identification of evidence
- Discovery strategy and tactical planning
- Production of evidence
- Collection of evidence
- Review of potentially responsive evidence
- Review of potentially privileged evidence[16]

When creating a retention policy, it is best to keep the above in mind and, perhaps, increase up-front costs. Taking advantage of technology and preparing for what is ahead is the best way to decrease overall costs. There is significant hidden cost in having employees searching each computer to cull potentially responsive documents to hand over to paralegals to reevaluate each before turning them over to attorneys to screen for privilege and evaluate relevance or determine discovery tactics. Associated with the man hours, there are opportunity costs involved and lost revenue opportunities.

Overall, the most cost effective way to handle a discovery response is to be organized and have the ability to search your stored documents for 50 or so search terms, combine and categorize like-documents, eliminate duplicates, parse out e-mail threads, and evaluate relevance and privilege all with the push of a few buttons. Planning ahead, staying organized, and communicating often and effectively will significantly reduce costs. Too often, companies focus narrowly on instituting a technique or method for evaluating and assembling evidence, rather than developing a strategy to solve each particular discovery task in the easiest and most cost-effective way possible.

IV. Conclusion

Everything you type into your computer or view from the web can find its way to your hard drive permanently. This means your online chats, your yahoo e-mail, your bank account password and the confidential client documents that you are drafting or reviewing can resurface. Before becoming the target of a legal proceeding, consider setting up a program to clean out those data closets. This plan also helps protect data if a computer is stolen, prior to donating a computer or transferring intradepartmentally, or before returning a leased computer.

A document retention policy that is both implemented and monitored can dramatically reduce your exposure. Communicate with your IT staff and plan ahead by implementing a document retention policy that is tailored to your company's specific needs. When implementing a practice, including wiping or other forms of document destruction, it is best to document it with a formal policy. Make sure you have provisions to suspend the policy for a "litigation hold."

It is conceivable that in the near future, if not already, at the inception of litigation, each side will weigh the cost of e-discovery against the cost of settlement. The best protection for electronic documents is a paper shield.

[16] Prashant Dubey, Calculating Your Total Cost of Electronic Discovery, Corporate Counsel A3 (March 2006).