E-DISCOVERY AND THE COMPLEX HEALTH CARE CLAIM

J. Matthew Shadonix and Gordon K. Wright
Cooper & Scully, P.C.
900 Jackson Street, Suite 100
Dallas, TX 75202
214/712-9500
Fax 214/712-9540
matthew.shadonix@cooperscully.com
gordon.wright@cooperscully.com

7th Annual Forum on Health Care Liability
Fall 2006

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

MISCELLANEOUS

E-Discovery and the Complex Health Care Claim

J. Matthew Shadonix and Gordon K. Wright

I. Introduction

Dear Reader:

By this letter, you and your clients are hereby given notice not to destroy, conceal or alter any paper or electronic files and other data generated by and/or stored on your clients' computers and storage media, or any other electronic data, such as voice mail.

Signed,
Plaintiff

The above letter is a sample of the "new wave" in litigation: e-discovery. By the time you get this letter, it is probably too late to ask any of the following questions:

1) What exactly do the terms "storage media", "electronic files", or "any other electronic data" mean?;
2) How do I organize and produce all of those things the other side is requesting?;
3) How much will all of this cost and who has to pay?; or
4) Does anyone know a good attorney?

While many use computers in the ordinary course of their business, everyone has their limitations. Even among attorneys, whose job it is to stay ahead of the curve on litigation techniques for the benefit of their clients, many have turned a blind eye to e-discovery.

In fact, CyberControls, a data forensics company, gave a series of lectures explaining the technology associated with e-discovery to commercial litigators this past summer. They asked each attendee to complete a short survey in which they found that fewer than ten percent of attendees had ever utilized electronic discovery during litigation. Seventy-one percent had not used e-discovery out of fear of a "retaliatory attack" by the opposing side.

In reality, as we progress more into the age of computers, it is important to be proactive; looking the other way will only work for so long. As CyberControls advertizes, "eliminating the element of surprise will significantly diminish one's hesitancy in going forward."

Another hurdle is that eighty-four percent of those commercial litigators believe that their client will not pay for an e-discovery request or a computer forensic investigation of opponent's computer systems. Compounding that problem is that seventy-seven percent admitted they had not discussed an incorporation of e-discovery with their clients. This is all while sixty-four percent admit lacking confidence in the technical aspects of data retention or creation, and fifty-five percent said they do not have knowledge regarding how to formulate an e-discovery plan.

With that many people admit to knowing nothing, even the smallest bit of knowledge will certainly put you ahead.

The purpose of this paper is to clarify issues regarding e-discovery.

II. The Law

In 1996, the Texas Rule of Procedure first differentiated e-discovery from traditional discovery.[1] This rule 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." 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.

In sum, Texas's rule creates two rules. First, it 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). Second, it mandates that the requesting party may pay for the production of unavailable electronic data.[2] Mississippi and California followed suit and enacted similar law differentiating between discovery of electronic documents and hard copies.[3]

In January 2002, Arthur Andersen disclosed that its employees had destroyed documents relating to Enron.

---

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

[2] *See* Sarah A. Philips, *Discoverability of Electronic Data under the Proposed Amendments to the Federal Rules of Civil Procedure: How Effective are Proposed Protections for "Not Reasonably Accessible" Data?*, 83 N.C. L. REV. 983 (2005).

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

In the ensuing fallout from the securities fraud scandal, the importance of those destroyed or "spoliated" documents was minimized in the public eye. However, Congress took note.

Congress responded by passing the Sarbanes-Oxley Act, which extended the reach and lengthened the potential penalties of the obstruction statutes.[4] The intent of the Act was to focus on the securities industry and financial services, but, incidentally, Sarbanes-Oxley applies most strongly 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.

This slow progression towards adopting and enforcing rules to address e-discovery and retention of electronic documents surged into overdrive when a New York District Court handed down a monumental decision.

A.. ***Zubulake***

In *Zubulake v. UBS Warbus, LLC*,[5] Laura Zubulake filed a charge of sexual discrimination against her employer, UBS Warbus, with the Equal Employment Opportunity Commission. After filing the charge, she was fired. She then brought suit 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's 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.[6]

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 the court held that an adverse inference instruction charge to the jury was warranted. Pursuant to such charge, the jury was permitted to infer that, had the lost e-mails been produced, they 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."[7] 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 how a court should allocate 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 this case as it estimated that the cost of restoring e-mails on its backup tapes, a time-consuming

[4] *See* 18 U.S.C. § 1512.

[5] *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 and determining that the balance tipped in favor of cost-shifting so that the defendants--the requesting party--would bear 75% of the costs of production); 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).

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

[7] *See Zubulake IV*, at 219.

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% 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 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.

Put another way, 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*

In an employment discrimination case, *Broccoli v. Echostar*,[8] the court examined a Echostar's email/document retention policy and found it "extraordinary." 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 "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 by failing to suspend document destruction and preserve essential documents after being put on notice of potential litigation.

The court found that management had a duty to preserve employment and termination documents when it learned of the potential litigation, but little had been preserved and subsequently produced. Echostar admitted that it never issued a company-wide instruction to suspend the destruction of relevant documents. The court held "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."

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. Rules and Amendments

Seemingly in response to *Zubulake* and its progeny, at its June 2005 meeting, the Standing Committee on the Federal Rules approved amendments to the Federal Rules of Civil Procedure in large part to accommodate e-discovery. As Texas did ten years earlier, the proposed changes amend the discovery rules to construct a two-tiered process for electronic discovery production requests. The first tier requires responding parties to produce all *relevant accessible* data stored on their digital storage systems *along with a description by category and location* of all relevant *not reasonably accessible* data that may be on their systems.[9] Data that is "not reasonably accessible" is presumptively outside the scope of discovery unless the requesting party can show "good cause."[10]

Upon a showing of "good cause" litigants enter the second tier of the e-discovery process. The court will then hear arguments from the requesting and objecting sides and weigh the cost of production against the

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

[9] For the complete text of the proposed amendments and Comments from the Advisory, *see* http://www.uscourts.gov/rules (last visited on Sept. 15, 2006).

[10] FED. R. CIV. P. 26(b)(2)(B) (as proposed). The committee note regarding this rule use the seven *Zubulake* factors to determine if good cause exists.

purported need.[11] In taking a step further than the Texas Rules, the new Federal Rules provide that even if the requesting party agrees to pay the discovery costs, a court can nevertheless prohibit data discovery if the producing party's burden in reviewing the information for relevance and privilege exceeds the purported need.[12]

The proposed Federal Rules have also expanded to encompass other concerns regarding e-discovery that have cropped up in the ten years since the Texas legislature took the first step.

D. Early Discussions of Preservation

Proposed Rule 26(f) is referred to as the "meet-and-confer" rule as it 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 will address the scope of e-discovery, the types of information sought, and the sides are expected to disclose what systems the other side maintains and what the "native" file format of the documents typically is. 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 scheduling order.

The rule has been supplemented so any issues relating to preserving discoverable information, as well as disclosure or discovery of Electronically stored information (including the form or forms in which it should be produced), must be discussed. Any issues relating to claims of privilege or protection also should be discussed and preferably memorialized in an agreement, which the parties can request the court to 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 rule encourages attorneys and their clients to get together early to think about issues, involve the technical people, get to know the company's hierarchy and information systems and then go to the other side and exchange information.

In addition, current Rule 16(b) requires the presiding judge to enter a scheduling order addressing pretrial issues. It has been amended to include provisions for the disclosure of electronically stored information and agreements reached by the parties relating to the assertion of privilege or protection claims.

E. Zubuluke's "Reasonably Inaccessible" Data Revisited

The amendments to Rule 26(b)(2) specifies that a responding party need not produce electronically stored information that it identifies as "reasonably inaccessible because of undue burden or cost," to address the issue of electronic information that is regarded as too burdensome to produce. The requesting party can dispute this assertion through a motion to compel production, and the responding party can seek a protective order prohibiting production, but only after the parties confer on the issue.

In either case, the burden falls on the responding party to prove that the information is reasonably inaccessible. Even if that showing is made, if the requesting party demonstrates good cause, the court still might order production. Just as in *Zubulake*, the factors comprising reasonable accessibility all seem to amount to how difficult or expensive it would be to obtain the information, the phrase "undue burden and cost" has been included to provide context in defining the phrase "reasonable inaccessibility." In fact, the Committee Note lists the same seven requirements as established in *Zubulake* as guide posts.

The responding party must disclose sources of potentially responsive information that is 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. It is extremely important to note: preservation duties exist even as to sources that 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.

This rule essentially constructs two tiers of discovery: accessible and inaccessible data. It is important for counsel to possess a strong understanding of these types of data, in general and as implemented by the individual company, to effectively argue that a client's records are inaccessible or that its opponent's records are not.

F. "Clawback" Provisions

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

[11] FED. R. CIV. P. 26(b)(2)(C) (as proposed).

[12] FED. R. CIV. P. 26(b)(2) (as proposed).

> 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, proposed 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 can't 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.

It is important to note that the proposed 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.

This rule operates in conjunction with proposed Rules 26(f) and 16(b), as it encourages the parties to enter agreements regarding privilege early in litigation and to submit them to the court for inclusion in the scheduling order. Such agreements, often referred to as "clawback agreements," generally control whether the parties adopt procedures that differ from the FRCP.

G. "Safe Harbor" Rule

Under current Rule 37 imposition of sanctions is authorized for discovery abuse. It authorizes the imposition of sanctions on a party for destruction or alteration of evidence. In *Zubulake*, Judge Scheindlin used this power to instruct the jury to assume that any information "lost" (read: destroyed) by UBS was harmful to UBS.

Proposed 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."[13]

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.). Many from the plaintiffs' bar worry that corporations will be entitled to delete relevant, discoverable data without fear of being sanctioned.

However, the proposed rule is not nearly this broad. In reality, 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.[14]

According to the Committee notes, the information must be destroyed as part of a routine procedure. However, even these "routine procedures" are evaluated. A party may not allow procedures to continue that might destroy discoverable data in an effort to thwart discovery obligations. 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.

It is worth repeating that this "safe harbor" rule does not give parties the right to destroy data 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

---

[13] *See* Committee Note to Proposed Rule 37.

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

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.

This calls attention to the need for creating prudent records retention policies, and more importantly, and proper implementation of them.

H. Separating and Specifying

Proposed 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."

"Electronically stored information is fair game for discovery in every federal case and is probably going to be in the state cases too," said Ashley Griggs, senior consultant for Electronic Evidence Discovery. He went on to express the idea that before, electronically stored information was elusive. It could be requested, but there was no absolute right to it or bright line test on the circumstances under which it could be compelled.[15]

In addition, these 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.

III. What The Other Side Will Request

Though the new rules will not go into effect until December 1, 2006, because of the relative lack of guidance in case law and existing statutes, some courts have begun to implement the proposed rules already, though not specifically referring to them.[16] The new landscape of discovery requests will be in line with the proposed discovery rules in litigation beginning now. The requests for production will be specific and they will require a knowledge of computer vocabulary mixed with overall computer savvy and a modest (at least) time commitment to respond adequately to each one.

Here, we will explore potential discovery requests that you can expect to see with regularity, and briefly analyze what each term means in an attempt to make it easier to identify sought documents. Then, using foresight, attempt to establish necessary steps to make the process easier and more cost effective, not to mention compliant.

A. Discovery Requests

> *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.*

The first question is, well, if it is deleted, how can we produce it? It used to be that a final draft of each document was handwritten or type-written and then placed in a file. Any notes, drafts, or fragments were thrown away as they were no longer needed. However, when it comes to electronic documents, merely placing a document into the recycle bin and expunging it does not mean that document is "thrown away." Most files created electronically contain two types of "background" data: metadata and embedded data.

When a party requests documents in their native form, metadata become a primary concern. Metadata are data that you can obtain or extract about a file from the document itself or from the file system on which the document is saved.[17] For instance, if a letter dated Jan. 1, 2006, is produced as a paper document, no one will be able to see the information that lies behind the document. If this letter, which allegedly cancels an order of widgets forming the basis of the breach of contract litigation, was actually created in May 2006–after the litigation began–the metadata showing the document's creation date may be quite relevant. Indeed, the metadata could be incorrect, but it certainly would be interesting to ask the author of the letter why the metadata shows its creation in May when the party claims it was sent in January--five

[15] *Id.*

[16] *See, e.g.*, In re Old Banc One Shareholders Securities Litigation, 2005 U.S. Dist. LEXIS 32154; Hopson v. Mayor of Baltimore, 232 F.R.D. 228, 231 (D. Md. 2005).

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

months earlier. Forms of production that allow the requesting party to view these metadata and embedded data are called "native."[18]

Embedded data is more like "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 lost 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. Included on every computer, from that of the CEO of a Fortune 500 company to that of the phone survey employee, is a trace of every tracked change, every edit, every version of every document. A possible solution to this dilemma, is to consider 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 notations on a memoranda from one executive to another saying "I cannot believe they are making us take out this safety feature to cut costs. Someone will be seriously hurt."[19] 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, if the time arises for a search for relevant documents, it will take much less time.

> *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.*

Think about the information you used to send by mail, or the gripes you used to talk about in the lunch room, or even the telephone conversations you used to have "just to talk." It is no surprise to anyone that each of the above has been replaced by e-mail as the medium of conveyance. 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. [20]

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 over fifty percent of e-mails sent or received are the product of "Spam."

A far cry from the single letter sent by post, e-mails and instant messages multiply and a lot of times, unknown to the owner, end up in the hands (or hard drives) of people around the company. The cost,

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

[19] *Id.*

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

manpower, and knowledge base needed for an all out e-mail discovery become huge.

Further, it is extremely difficult to search most of the storage media used for email. Many companies use "back up tapes" to back up their hard drives at night. While these back up tapes are relatively inexpensive, they are very expensive to search. These tapes are unlike a hard drive, in that they do not save the material in groups and the information cannot be search by keyword. Back up tapes behave like massive audio cassettes, where the only way to search everything, is to go through it all.

> *All other files generated by users through the use of computers and/or telecommunications, including, but not limited to voice mail.*[21]

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. But most human transcription was difficult because each system stored its messages in a different manner, so the transcriptionist would have to go to the place of business and use the company's machine, shutting down the voice mail system for days on end, until the transcription was complete. The cost and inconvenience of such a 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.

This concern is a growing one, and managing your company's system is imperative. 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.

Thus, 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.

B. Protecting Your Company

> *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:

1) being unprepared for litigation;
2) put in the position of producing damaging information through e-discovery; or
3) spending a lot of time and money throughout the discovery process in producing relevant documents or screening for privilege.

In creating a document retention policy, it is most important to recognize that the policy must be followed. It is even more challenging to explain why your company's retention policy was not followed than to explain why your company does not have one.

Next, you must consider your company's unique needs. Speak with your information technology staff. They are in the best position to evaluate how your electronic infrastructure works. They know, among other things:

I. what e-mail system is used and how often it backs itself up;
II. if the electronic information is all kept on site;
III. the storage medium used for each form of data;

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

IV. how easy or difficult it is to search each of the storage drives; and
V. 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:

1) How long does your company really need to keep old e-mail files?
2) How important is it to back up each system every night?
3) 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. If your company is efficiently minimizing the amount of data that it saves in the ordinary course of business, it could be catastrophic to let even one day go by from the notice of a claim to a litigation retention policy.

Once again, the key to effectively implementing a litigation hold is communication. Each employee should be notified and trained to follow a litigation hold policy at the same time they are trained regarding the document retention policy itself. The best a company can hope for is to have a protocol where the CIO, the intern, and everyone in between are notified individually within minutes of each other.

C. What is Needed for a Good Policy?

It is true that good attorney can be useful and quite necessary in analyzing the legal issues raised by a company's document retention policy and an e-document company is in the best position to facilitate document preservation and destruction methods. However, the people in the best position to adequately create a document retention policy tailored to suit the particular needs of your company, are the employees themselves.

The company should form a task force made up of executives, IT specialists, and other employees to discuss the company's retention needs. In creating a policy, there are a few areas on which your task force should focus.

First, 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. Was cost a factor? Storage space? Perhaps a new policy was needed because of an expansion or a new networking system. Each employee and anyone else who may come to read your policy should know exactly why one was created.

A good policy should also indicate the department or specific employees to whom it applies. Frequently, the IT department should have a different policy from upper-management or the financial department. A good policy specifies the applicable departments and why, but also should indicate any particular people or departments to which the policy should not apply.

Each document or source should be considered when implementing a retention period. Obviously personal e-mails should not be saved longer than invoices, but it is important to discuss and record why. Also, it is important to have a protocol indicating how long a closed file or account should remain open.

In addition to what documents are maintained and for how long, 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.

Each company will have different needs, but each of the above should be considered. Additionally, depending on the type of business, it might be prudent to address 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 a successful policy to have periodic meetings to discuss document destruction as your business and technology evolve. What is more, 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.

IV. Cost Considerations

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.[22] The revenues are estimated to rise to over $3.1 billion in 2008.

When asked how much the discovery process of electronic media would cost, Tom Miller, a partner at Open Door Solutions, LLP, estimates "a couple of thousand a gig."[23] However, he goes on to qualify that number as "the roughest of estimates."

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 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. Therefore, 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[24]

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.

---

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

23 *See* Panel Discussion *supra* note 12.

24 Prashant Dubey, *Calculating Your Total Cost of Electronic Discovery*, Corporate Counsel A3 (March 2006).

V. 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 wiping program on your PC or network 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. Think of it as a systematic shredding of electronic documents.

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. In such an environment, it is an interesting state of affairs that the best protection for electronic documents is a paper shield.