ELECTRONIC DISCOVERY:
LEGAL ISSUES AND PRACTICAL CHALLENGES

DAVID CHAUMETTE
De la Rosa & Chaumette
770 South Post Oak Lane
Houston, Texas 77056
(713) 395-0991
(713) 395-0995 (fax)
dchaumette@delchaum.com

State Bar of Texas
BEST OF 2009
Dallas - November 12-13, 2009
Houston – November 19-20, 2009
Austin – December 3-4, 2009

CHAPTER 17

DE LA ROSA & CHAUMETTE

David A. Chaumette
Partner
770 South Post Oak Lane
Suite 420
Houston, Texas 77056
tel: (713) 395-0991
fax: (713) 395-0995
dchaumette@delchaum.com
www.delchaum.com

David Chaumette represents corporations in numerous industries on litigation matters pending across the United States. Those matters have included oil and gas, securities, software licensing, and employment–related disputes. He has tried several cases to jury verdict has prosecuted appeals. He is also a leading lawyer on issues related to electronic discovery and data management and is presently teaching E-Discovery at the University of Houston Law Center, the first class of its kind in the state of Texas.

Representative Matters:

- Litigation against a publicly-held company and one of its officers against claims of commodities fraud,
- Representation of a publicly-held company (specifically, extensive work related to electronic discovery) against securities fraud claims of over five billion dollars,
- Advising clients on records management system implementations, given heightened requirements developing as to corporate records,
- Oversight of collections efforts related to discovery in a multidistrict litigation,
- Litigation on behalf of companies against its former consultants and employees on issues related to trade secrets and other protected materials,
- Coordination of national defense efforts for a window manufacturer against product liability claims in 15 states, and
- Representation of the purchaser of a bankrupt entity's assets as part of that entity's plan of reorganization.

Selected Articles:

- David Chaumette, co-author, "Privilege Under the New Rules: New Mines in the Litigation Minefield," The Commercial Law

Connection (National Bar Association Commercial Law Section);
Summer 2007.

- David Chaumette and Michael Terry, "The World of E-Discovery or How I Learned to Stop Worrying and Love the New Rules," The Houston Lawyer; November/December 2006.

- David A. Chaumette and Brad Harris, "Authenticating Electronic Evidence: From Collection to Production," E-Discovery Advisor Magazine and LJN's Legal Tech Newsletter; May 2006.

- David A. Chaumette and Lynnea Myers, "Force Majeure Clauses Protect Companies from the Unexpected," Houston Business Journal, February 13, 2006.

- David Chaumette, co-author, "Zubulake or Zubuluck: A Lesson in Litigation Reading (aka FRCP Readiness)," Corporate Counsel Magazine, February 2006.

- David A. Chaumette, "Divining the Future: Anticipating Tomorrow's EDD Standards, Defend Corporate Communications Today," Digital Discovery & Evidence, August 2005.

- David A. Chaumette and James A. Hurd Jr., "Monitoring Electronic Data Now Can Spare Litigation in the Future," Houston Business Journal, August 1, 2005.

- David A. Chaumette, co-author, "Back-Up Tapes, Metadata and 'Delete': Questions Surround Proposed Federal E-Discovery Rules," Texas Lawyer, April 4, 2005.

- David Chaumette, co-author, "Don't Wait for Waters to Rise Before Making a Plan Continuity," Houston Business Journal, May 5, 2003.

Selected Presentations:

- "E-Discovery: Legal Issues and Practical Challenges," State Bar of Texas CLE, 31th Annual Advanced Civil Trial Course, Fall 2008.

- "Common Pitfalls in E-Discovery" State Bar of Texas CLE, Suing and Defending Governmental Entities, July 2008.

- "Electronic Discovery Update," State Bar of Texas – Texas Minority Attorney Program, May 2008.

- "Litigation Update / Daubert Update," State Bar of Texas, January 2008.

- "Top Ten Tips on E-Discovery," Texas Minority Counsel Program, November 2007.

- "E-Discovery After the New Federal Rules," West Legalworks, September 2007.

- "Electronic Evidence," State Bar of Texas CLE, 30th Annual Advanced Civil Trial Course, Fall 2007.

- "Surviving the last 90 Days before Trial or Getting Motions, Discovery, and Order Ready for Trial Without Letting Anything Slip," University of Houston Law Foundation, August 2008.

- "Settlement Thoughts and Strategies," University of Houston Law Foundation, April 2007.

- "Morgan Stanley: An E-Discovery Tale Gone Bad," SHB E-Discovery Program for IT Professionals and Corporate Counsel, November 2006.

- "Lawyer as Fortune Teller: Avoiding Tomorrow's Sanctions Today," Fios/Compliance Resources Podcast, November 2005.

- "Keeping Your Secrets Secret: Covenants Not to Compete and Trade Secrets in Texas," Advanced Employment Law Institute, University of Houston CLE, August 2004.

- "Electronic Discovery: Treasure Trove or Sinkhole," Litigation Tactics Seminar, University of Houston CLE, July 2004.

- "Personal Jurisdiction and the Internet," ABA Conference: A National Institute on Representing High Technology Companies, San Francisco, California, November 13, 1998.

Awards and Honors:

In 2004, David was selected as one of the Five Outstanding Young Houstonians by the Houston Junior Chamber of Commerce and one of the Five Outstanding Young Texans by the Texas Junior Chamber of Commerce. That year, he was also selected as a Volunteer of the Year by both the Girl Scouts of San Jacinto Council and Volunteer of the Year of Aspiring Youth of Houston. In 2005, David was named to Visitors Committee of the South Texas College of Law in Houston. In 2003, David was admitted into the Pro Bono College of the State Bar of Texas because of his commitment to pro bono work.

In 2006, David was named one of the 500 New Stars by Lawdragon.com. He has also been named "Texas Rising Star" and a "Super Lawyer" by Law & Politics Magazine for several years.

Professional Affiliations

- Member of the Board and Executive Committee of the Houston Bar Association

- Member of the Board of The Holocaust Museum Houston

- Member of the Board and Executive Committee of Neighborhood Centers, Inc.
- Member of the Board and Executive Committee of the First Colony Little League
- Member of the Board of Young Audiences of Houston
- Fellow, American Law Institute
- Fellow, Litigation Counsel of America
- National Bar Association
- Houston Lawyer Association
- College of the State Bar of Texas
- Pro Bono College of the State Bar of Texas

Education & Bar Admittance:

Mr. Chaumette is admitted to practice before the state courts of Texas, the U.S. District Court for the Northern, Southern, Western and Eastern Districts of Texas and the District of Colorado, the U.S. Court of Appeals for the Fifth Circuit and the U.S. Supreme Court. Dave received his J.D. degree from the University of Chicago Law School, his M.S. degree from Stanford University (Aeronautics/Astronautics), and his B.S.E., cum laude, from Princeton University.

TABLE OF CONTENTS

ELECTRONIC DISCOVERY: LEGAL ISSUES AND PRACTICAL CHALLENGES

I. INTRODUCTION.

The electronic revolution has changed the way business is done. In the past, hard copies of paper documents occupied large physical spaces and represented a significant part of the discovery process. Today, in contrast, almost all business communication is conducted electronically from word processing programs to internal and external e-mail accounts. Researchers at the University of California at Berkeley announced that 93% of all information created during 1999 was generated in digital form, on computers of some sort.[1] That means that only 7% was generated using other media, like paper, phonograph records, clay tablets or smoke signals.[2]

This generation of communication has created new efficiency and effectiveness of business management in many respects. The increased presence of technology in the workplace, however, has also required significant changes in the way litigation, and specifically discovery, is handled. Adapting to these changes, litigants face an ever-changing arena referred to as electronic discovery, which can be a veritable treasure trove or minefield depending on the level of preparation taken by the client and the client's counsel prior to the arrival of any legal dispute.

The limited number of overarching rules to govern electronic discovery frequently leads to unique burdens for parties seeking to comply with a request for electronic data. Electronic discovery can be expensive, difficult, time-consuming, and sometimes fatal to the underlying case — typically not results that satisfy clients.

Given these issues, should *you* be concerned about electronic evidence? Consider this: one in 20 companies have battled a workplace lawsuit triggered by e-mail, and 14 percent of companies have been ordered by a court or regulatory body to produce employee e-mail.[3] Even if you have not been asked to produce electronic documents to date, learning about electronic discovery now can be very beneficial when you do receive your first request for electronic data, and it can lessen your risk of sanctions due to a lack of understanding regarding the preservation of electronic evidence. This paper outlines some of the major issues and considerations for lawyers involved in the electronic discovery process.

II. ELECTRONIC DOCUMENTS AND GOOD OLD FASHIONED DISCOVERY.

In the United States, the issue of "e-discovery" was being addressed ad hoc in the federal courts until the Civil Rules Advisory Committee of the United States Judicial Conference adopted new rules for discovery of "electronically stored information," which became effective on December 1, 2006.[4] According to the Advisory Committee, the new rules are intended "to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments."[5]

Both the Texas and Federal Rules of Civil Procedure, as well as case law interpreting the rules, already recognize an obligation to produce electronic data in response to requests for production (even prior to the amendments to the Federal Rules).[6] Texas Rule of Civil Procedure 196.4 specifically addresses the duties of the requesting and responding parties regarding the production of electronic or magnetic data. Under that rule, the requesting party "must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced."[7] If the responding party cannot produce the material in the form requested after expending reasonable efforts, the party must state an objection in compliance with the terms of the rules.[8] 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.

In federal court, Federal Rule of Civil Procedure 34 requires production of electronic data in

---

[1] Kenneth J. Withers, Federal Judicial Center, *Electronic Discovery* (presentation at National Workshop for U.S. Magistrate Judges, June 12, 2002).

[2] *Id.*

[3] American Management Association, 2003.

[4] The Advisory Committee report, dated May 5, 2005, can be found at http://www.uscourts.gov/rules/Reports/CV5-2005.pdf. The rules are applicable in the federal courts. State courts in the United States must develop their own rules, state by state, although the Conference of Chief Judges of the State Supreme Courts has issued guidelines on e-discovery which, for the most part, mimic the federal e-discovery rules. See *Guidelines For State Trial Courts Regarding Discovery Of Electronically-Stored Information* (August 2006) which can be found at http://www.ncsconline.org/WC/Publications/CS_ElDiscCCJGuidelines.pdf.

[5] *Id.*

[6] Many of these issues are discussed in Tammy Wavle Shea, *Discovery of Electronic Information*, 40 HOUS. LAW. 29, 30 (Jan/Feb. 2003).

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

[8] *Id.*

"reasonably usable form." This rule allows a request for production of "other data compilations from which information can be obtained, translated, if necessary, by the respondent through detective devices into reasonably usable form . . . [.]"[9]

Both Texas and federal courts mandate that parties produce data in electronic form, even after the information has already been produced in "paper" form. This requirement is not new. For example, in *City of Dallas v. Ormsby*, the Amarillo Court of Appeals upheld a trial court's sanctions for failure to produce data contained in computer records.[10] The plaintiff requested documents concerning a roadway where a fatal accident had occurred, but the city argued it did not withhold documents because it supplied the information as a memorandum rather than a computer printout.[11] The court disagreed, and compelled the production of the electronic version of the information.[12]

The Amarillo court recognized that documents are to be produced as they are kept in the usual course of business.[13] The court then held that the rules of civil procedure made clear that the term "documents" includes data compilations from which information can be obtained and translated.[14] Therefore, the court found a duty to produce such electronic data in electronic form and held the failure to do so was sanctionable.[15] More recently, the fight over form of production is focused on cost issues, which will be discussed in further detail below. Interestingly, several companies now find it easier to produce electronic data electronically.

A. Electronically Stored Information Versus Paper.[16]

The digital world differs from the paper world in many respects, but there are several key differences.

1. Everyone Is A File Keeper.

In the paper world, documents are given to staff persons for filing. In the digital world, every computer user who sends or receives e-mail, creates word processing documents, prepares spreadsheets or information slides, or maintains databases decides whether to store files and has the ability to modify or delete a file. Even if the digital file keeper takes no action, eventually e-mail will move to backup tape and usually that backup tape will be overwritten after a period of time, and the file may be lost forever.[17]

In the paper world, when an employee leaves employment, the employee's documents, already archived, may remain in that state until records retention schedules call for their destruction. In the digital world, when an employee leaves employment, the employee's desktop or laptop hard drive (or both) may be reformatted, destroying all data on the drives unless someone decides that there are litigation reasons to maintain that employee's digital status quo.[18]

In the paper world, when, say, a major construction project was completed, all of the paper associated with the project might be boxed and stored in a warehouse. In the digital world, the desktop and laptop computers used by everyone in the field will be moved to the next job and file management will be a function of project organization or perhaps serendipity, depending upon the individual file-keeping habits of each person on the job.

2. Metadata.

A second key difference is the existence of "metadata." Metadata "is information about a particular data set or document which describes how, when and by whom it was collected, created, accessed, modified and how it is formatted."[19]

---

[9] FED. R. CIV. P. 34.

[10] 904 S.W.2d 707, 712 (Tex. App.—Amarillo 1995, writ denied).

[11] *Id.* at 710-11.

[12] *Id.*

[13] *Id.* at 710.

[14] *Id.* at 711.

[15] *Id.*

[16] This portion of the paper is adapted from portions of Barkett, *E-Discovery For Arbitrators Under the IBA Rules For Taking Evidence* (Shook, Hardy & Bacon 2007), available at www.shb.com.

[17] An individual user can archive an e-mail in local storage media, and that may be the only place to find a document. See *Hynix Semiconductor Inc. et al. v. Rambus Inc.*, 2006 U.S. Dist. LEXIS 30690, *27-28 (N.D. Calif. Jan. 5, 2006) (explaining that Rambus changed to a backup recycling schedule of three months and that employees should create their own archive copies of documents; for e-mail that meant printing them or keeping them "on your hard drive").

[18] See, e.g., *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc. et al.*, 2007 U.S. Dist. LEXIS 15277 (D. Colo. Mar. 2, 2007) (wiping clean the computer hard drives of former employees, among other conduct, was sanctionable under the circumstances, but since the prejudice was not substantial, sanctions were limited to $5,000 and reimbursement of certain court reporting costs).

[19] This definition comes from *The Sedona Conference Glossary: E-Discovery & Digital Information Management*, p. 28 (May 2005) available at http://www.thesedonaconference.org/content/ miscFiles/ tsglossarymay05.pdf (Sedona Glossary).

3. Deleted Data.

A third key difference is that digital data can survive deletion, while paper that is discarded is not likely to be found again. The Sedona Glossary (p. 11) gives this definition of "deleted data:"

> Deleted Data is data that existed on the computer as live data and which have been deleted by the computer system or end-user activity. Deleted data may remain on storage media in whole or in part until they are overwritten or "wiped." Even after the data itself have been wiped, directory entries, pointers or other information relating to the deleted data may remain on the computer.

So, for example, a computer user moves data to "trash" or the "recycle bin." Until the trash or bin is emptied, the data remain fully restorable, often by any user. Once the trash or bin is emptied, the data may be restored by forensic experts who may be able to reconstruct data fragments to recreate the deleted file, unless the storage media in question has been "wiped," typically by software designed to achieve this aim.[20]

4. Multiple Sources of Data.

A fourth key difference is the proliferation of data sources over paper. A "key player" in any dispute may have information stored in a number of places from his or her office computer, to that user's home computer, to administrative assistant's computers, and so on and so on. This proliferation can be very expensive to deal with, if the company is not prepared.

5. Backup Tapes.

Another key difference between the paper and electronic worlds is the existence of backup tapes,[21] typically used for disaster recovery purposes. Backup tapes are, typically, not reasonably accessible, as compared to "active data" which can be easily accessed by a user.[22] Furthermore, backup tapes contain extraordinary amounts of information.

Perhaps as significant as volume, backup tapes may be the only place that certain documents reside. Unless they were printed, prior versions of a document may only exist on backup because they would be overwritten each time a computer user edits the file contained in active data storage. An individual that does not archive an email on his or her individual hard drive will lose that e-mail to backup after a period of time. Backup tapes may also reveal whether an individual has deleted an e-mail. However, backup tapes will not capture an e-mail received by an individual and deleted the same day.

Retrieval of information from backup tapes can also be costly. There is both the cost to retrieve and the cost to review. A well known example, in *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003),[23] there was a battle over the production of 77 backup tapes. The district court ordered UBS Warburg to restore at its expense five tapes to give the district court an idea both of the cost to restore and the relevance of the information contained on the backup tapes. The cost to restore five backup tapes was $19,003.43 which resulted in the

---

[20] See, e.g., *Kucala Enterprises, Ltd v. Auto Wax Co., Inc.*, 2003 U.S. Dist. LEXIS 8833 (N.D. Ill. 2003) (discussing a program called "Evidence Eliminator" which is designed to clean computer hard drives of data that may have been deleted by the user but still remain on the hard drive).

[21] The Sedona Glossary defines "backup tapes" as follows: "Magnetic tapes used to store copies of data, for use when restoration or recovery of data is required. Data on backup tapes are generally recorded and stored sequentially, rather than randomly, meaning in order to locate and access a specific file or data set, all data on the tape preceding the target must first be read, a time-consuming and inefficient process. Backup tapes typically use data compression, which increases restoration time and expense, given the lack of uniform standards governing data compression."

[22] One court has described the difference between data that are "accessible" and data which are "inaccessible." Data which are (1) "online" or archived on current computer systems (such as hard drives); (2) "near-line" such as that stored on optical disks or magnetic tape that is stored in a robotic storage library from which records can be retrieved in two minutes or less; or (3) "off-line" but in storage or archives, such as removable optical disk (e.g., CD-ROM or Digital Versatile Disc (DVD)) or magnetic tape media (e.g., Digital Linear Tape (DLT) tape), are readily accessible using standard search engines because the data are retained in machine readable format. *Zubulake v. UBS Warburg LLC,* 217 F.R.D. at 318-320. On the other hand, (4) routine disaster recovery backup tapes that save information in compressed, sequential, and non-indexed format, and (5) erased, fragmented, or damaged data, are generally inaccessible, because a time-consuming, expensive restoration process is required to obtain information. *Id.* at 319-320.

[23] Zubulake alleged she was a victim of gender discrimination and was eventually terminated and then filed an additional claim that she was retaliated against for complaining about the employment practices of her supervisor. 216 F.R.D. at 281. The district court explained that under the federal rules of civil procedure, the presumption is that the producing party pays for production of accessible data. In addition, the district court held that the cost to review should always be borne by the producing party. With respect to the cost to retrieve, the district court evaluated each of seven factors identified by the district court as relevant to the determination of who should pay this cost, and decided to shift 25% of the cost to the requesting party, Zubulake. 216 F.R.D. at 283-90.

production of 600 e-mails responsive to the plaintiff's request for production. UBS Warburg estimated that the cost to restore the remaining 72 tapes was $273,649.39 and the cost to review the data before production would be $107,694.72.

6. Key Players.

In the paper world, there is not necessarily a premium placed on the correct identification of persons with knowledge or information about a claim—"key players"—because paper is kept for a long time by many companies. In the electronic world, the identification of key players is much more significant because a delayed identification of key players can result in the loss of relevant information.

For example, in *Consolidated Aluminum Co. v. Alcoa*, 2006 U.S. Dist. Lexis 66642 (E.D. La. July 19, 2006), four key players initially were identified in November 2002 when Alcoa sent a demand letter to Conalco for costs associated with an environmental cleanup. Conalco then decided to sue in 2003 seeking a declaration of nonliability. In 2005, Conalco issued a request for production which prompted Alcoa to identify eleven more key players. In the interim, however, the emails of these eleven individuals had been erased because of Alcoa's email backup retention protocol.[24] Conalco moved for sanctions. The district court refused to award punitive sanctions, but required Alcoa to pay the reasonable costs and fees Conalco incurred to bring the motion for sanctions and also to pay the cost of re-deposing up to thirteen people, in addition to allowing Conalco to serve certain additional discovery requests.

7. Forms Of Production.

In the world of electronically stored information, there are also choices on the form of production. A requesting party may seek production in "native" format: the file as it exists on the storage media on which it is stored with its associated metadata. A producing party may prefer to produce documents in "Tagged Image File Format" (TIFF)[25] or "Portable Document Format" (PDF)[26] in order to bates-label the documents. Vendors should be able to link meaningful metadata to an associated TIFF or PDF image depending upon the agreement of parties or the scope of a court's order on production of electronically stored information.[27]

III. THE "NEW" RULES OF E-DISCOVERY.

In August 2004, the Federal Rules of Civil Procedure Advisory Committee proposed significant changes to the Federal Rules with regards to discovery of electronically stored information.[28] Those amendments to the Federal Rules became effective on December 1, 2006. The new provisions amended Rules 16, 26, 33, 34, 37, and 45, along with Form 35, including:

- **Early Discussion of E-Discovery Issues: Rule 16(b), Rule 26(f), & Form 35.** The

[24] Alcoa submitted an affidavit describing the protocol: "Once every week, all messages older than thirty days in a user's Exchange mailbox are moved to a "System Cleanup" folder. At the same time, all messages older than fifteen days (forty-five days total) in a user's System cleanup folder are deleted and are no longer directly recoverable by the user. . . . In addition, Alcoa's disaster recovery system retains email for the trailing six months." That prompted the magistrate judge to say: "Thus, it is possible that relevant emails for the six months prior to November 2002 could have been retrieved, had Alcoa properly suspended its routine document destruction policy when it became aware of potential litigation with Consolidated in November 2002."

[25] The Sedona Glossary defines TIFF as: "One of the most widely used and supported graphic file formats for storing bit-mapped images, with many different compression formats and resolutions. File name has .TIF extension. Can be black and white, gray-scaled, or color. Images are stored in tagged fields, and programs use the tags to accept or ignore fields, depending on the application."

[26] The Sedona Glossary defines PDF as: "An imaging file format technology developed by Adobe Systems. PDF captures formatting information from a variety of applications in such a way that they can be viewed and printed as they were intended in their original application by practically any computer, on multiple platforms, regardless of the specific application in which the original was created. PDF files may be text-searchable or image-only. Adobe® Reader, a free application distributed by Adobe Systems, is required to view a file in PDF format. Adobe® Acrobat, an application marketed by Adobe Systems, is required to edit, capture text, or otherwise manipulate a file in PDF format."

[27] According to the Sedona Glossary definition of "native format," "static" formats such as TIFF or PDF "are designed to retain an image of the document as it would look viewed in the original creating application but do not allow metadata to be viewed or the document information to be manipulated."

[28] Eight jurisdictions have adopted rules to govern electronic discovery: Mississippi Court Order 13 (May 29, 2003) amending Mississippi Rule of Civil Procedure 26; Texas (TEX. R. CIV. P. 193.3(d), 196.4), District of Arkansas, Eastern and Western, Local Rule 26.1; District of Delaware, Default Standards for Discovery of Electronic Documents; District of Kansas, Electronic Discovery Guidelines; District of New Jersey, Local Rule 26.1; and District of Wyoming, Local Rule 26.1. Some of these rules will survive the adoption of the new overarching rules, so they are worth a review if counsel has a case pending in one of those jurisdiction.

new rules amend Rules 26(f) and 16(b) as well as Form 35 to prompt counsel to discuss early on how to handle e-discovery issues. This will necessitate additional or more extensive interaction with opposing counsel at an earlier point in the case. The question is whether—even before the scheduling conference—these concerns are being raised too late?

- **Definition of Electronically Stored Information. Rule 34(a).** Revised Rule 34 indicates that electronically stored information is subject to production and discovery. This is not a significant change.

- **Form of Production: Rule 34(b).** The revised Rules allow requesting parties to specify production format, but the rules do not direct counsel to pick one production format over another. The key point here is to determine the form of production early, with an emphasis on the need for parties to try to come to an agreement as early as possible.

- **Option to Produce Electronically Stored Information in Response to Interrogatories: Rule 33(d).** Under the new Rule 33, the responding party is allowed to produce electronic data when responding to interrogatories as long as the requesting party is able to locate and identify the information as easily as the responding party. There is a significant trap here contained in the Committee's notes. In the old days, litigants used to respond by saying that the answer is in the documents. Today, that response may allow the opposing counsel to come in and inspect your client's computers, which may not always be a desired outcome.

- **Reasonably Accessible Information: Rule 26(b)(2)(C).** This change requires the requesting party to obtain a court order compelling the responding party to produce the information that is not "reasonably accessible." This has the potential to be a key battleground issue in the future.

- **Belated Assertion of Privilege: Rule 26(b)(5)(B).** A party who unintentionally discloses privileged information may get it back from the receiving party unless the receiving party can prove it is entitled to the information. This issue **is** one of the key battlegrounds in this area.

- **Safe Harbor on Sanctions: Rule 37(f).** The safe harbor provision prevents judicial sanctions for failing to hand over electronically-stored information if the information was destroyed during the "good faith" routine use of a computer system. After much debate about this particular provision, the new rule here is weak and does not provide much protection to companies.

The new rules force companies to determine "reasonable" preservation steps. Data is regularly destroyed through automatic processes, and merely opening a document or starting a computer can alter files and metadata. As such, corporations and law firms should be concerned that they cannot act quickly enough to preserve data and avoid allegations of spoliation.[29] The failure to understand this can be extremely costly.

IV. FIRST STEPS TO E-DISCOVERY CHALLENGES.

The proliferation of data, combined with heightened scrutiny from courts, forces practitioners to consider these issues from an early point in time. That might be before any litigation is filed or when the company first sees a demand letter. However, even if nothing is done early, the company should take proactive steps as soon as it realizes that the potential for these issues exist. The question is what do those early steps look like.

1. Familiarity Breeds Consent.

A good first step takes place before anything actually even begins. By understanding the structure of the client's organization, attorneys can take the first step toward identifying relevant electronic data and the sources. This means meeting with the client's IT staff and its personnel so that, when the need arises, the client can immediately begin to preserve data. At a minimum, this meeting should cover: the computer systems in use, the document retention program in place, relevant legacy problems, the nature of any encrypted data, and the physical location of any potentially discoverable data.[30] One of the bigger challenges may be "buy in" from the corporate management, but given the increased technological sophistication of the workplace, this task should be easier today than in the past.

---

[29] Spoliation is discussed further below.

[30] The real first step is even understanding the vocabulary of electronic discovery. For example, "legacy data" is data which is read by systems no longer in use by the client in question, such as WordStar or Lotus 1-2-3. This data might be relevant but hard to access.

This meeting can have several other benefits as well, mostly related to improved communication between the different people and departments. For example, many companies today have policies in place regarding discrimination in the workplace. Others focus on safety issues, but few have training on appropriate use of e-mail and other technology assets of the company. There are several steps that can improve the company's position and reduce litigation costs before those costs are incurred. However, these steps require a coordinated approach between diverse parts of the company, from IT to records to legal.[31]

2. Understanding Your Data.

Everyone knows what e-mail is, but fewer contemplate how pervasive a single e-mail can be or how many different forms of electronic information can exist within one company. A single piece of electronic information, like an e-mail, can be stored in numerous places ranging from earlier versions and drafts of documents to "deleted" e-mail stored on back-up tapes. If your client has changed or upgraded software at any point, there may also be responsive discoverable documents in numerous formats. The proliferation of personal digital assistants (or PDAs) has only exacerbated these problems.

E-mail can be particularly problematic, not only because of its sheer volume, but because there is no logical filing method for most e-mail systems. As a result, business e-mails are mixed with personal e-mails, ranging from love letters to chain-forwarded jokes. Accordingly, retrieval and screening of e-mail messages for relevance and privilege can be difficult, costly, and time consuming. While requests for e-mail tend to be most common, other types of electronic information may be valuable.

Generally, electronic information falls into three categories: active, backup, and residual. Active data files are information readily available and accessible from personal computers. This active data can include word processing documents, spreadsheets, databases, and calendars, as well as e-mail, and is relatively easy to view and obtain. Easy here means inexpensive, therefore, unless special circumstances exist, companies should limit the production (but not necessarily their collection and preservation) efforts to active data.

Backup data are usually files created automatically by various applications. These documents were never saved, and the user probably may not even be aware that they exist. Nevertheless, they may still be retrievable, and therefore discovered. Each time a file is automatically backed up, a "file clone" is created and stored on the user's hard drive, but usually not on the network server. As a result, these back-ups continue to reside on the user's hard drive even after the document or file is deleted from the network server. These documents are rarely well organized, at least not from a human's point of view.

Another source of backup electronic discovery is "back-up tapes." These tapes capture everything from e-mail messages, old drafts of word processing documents, and hidden information on spreadsheets. They typically record when the document was created, the author of the document, subsequent edit dates to the document, and which users have access to the revised document, as well as the number of versions of the document. However, the data on back-up tapes are not organized for retrieval of individual documents or files, but for wholesale, emergency uploading onto a computer system. Therefore, special programs may be needed to retrieve specific information, and the process can be costly and time consuming.

In the past, back up tapes were the source of great consternation and concern. While it was once true that restoring back up tapes was expensive, it is more economical now. The infamous Morgan Stanley case turned on the production of back up tapes. Morgan Stanley could not restore its tapes in a timely fashion and got an adverse inference instruction against it.[32] Prepared future litigants know that if back up tapes are only used for disaster recovery then it is much less likely that the company will need to restore those tapes.

Residual data are data that continue to exist after the user has "deleted" files. Hitting the "delete" key merely renames the file, making it available for overwriting if space on the hard drive is needed in the future. One could think of deletion as removing the card describing a book from the card catalog at the local library without removing the book from the shelves. Because the information does not vanish at the point where the user deletes it, it continues to exist on the hard disk space until the space it occupies is overwritten. Computer forensic experts can recover this information because it may have been backed up before it is actually overwritten and because the deleted files may have been only partially overwritten. This process can be extremely expensive and may not yield any "smoking guns."

3. Data Maps and People Maps.

The process of electronic discovery can be inefficient and ultimately unproductive if a lawyer does not know who to ask or how to ask for the information

[31] This, of course, presumes that there is a records department in the company which is not always the case. Nevertheless, there is always a records function.

[32] Morgan Stanley made other mistakes as well on its way to the $1.6 billion verdict.

sought. As most lawyers know, there are many individuals in the business world who rely heavily on the experience and knowledge of secretaries and others who perform electronic data entry. While these data entry personnel are not likely to yield the information a lawyer may be seeking during the course of discovery, the relationship is emblematic of a common hurdle facing those seeking complex electronic discovery. Specifically, the person a lawyer may have asked to respond may not be knowledgeable about the specific information requested. For this reason, it is essential to consider questioning representatives from the opposing party who are intimately familiar with the hardware, software, and networking system employed by the business entity.

For example, it may be worthwhile to depose the information technology (IT) manager, the chief information officer, or someone in a similar role in order to determine the parameters of the opposing party's computer system. This person may also be the most informed about the company's electronic document retention policy. Interrogatories may also represent a useful tool to probe for information about the opposition's policies regarding the maintenance of electronic information. The specifics of such policies should help to determine the scope of the initial requests. Key questions to address in the deposition or interrogatory include the number, types, and locations of all electronic communication devices used (including desktops, laptops, PDA's, cell phones, etc.), electronic records management policies and procedures, and corporate policies regarding employee use of company computers, data, and other technology.

It is often useful to interview individual data custodians so that the lawyer can best understand how the data is organized and what it contains. The focus of such an interview would be what resources the custodian uses, as well as more substantive issues as well.[33]

With this information in hand, a lawyer can conduct a more focused, reasonable, and cost-effective search that will help undermine objections that discovery demands for electronic evidence are overbroad, unduly burdensome, or cumulative.[34] Thus, time spent analyzing personnel and corporate structure could be valuable in locating an employee whose deposition will shape the initial discovery requests.

4. Litigation Holds

Along with custodian interviews, litigation holds are the cornerstone of a response to new litigation. The litigation hold is a memorandum typically sent from the legal department and contains a general description of the litigation and the need to preserve documents relevant to the suit. There is a debate as to whether the litigation hold is privileged. *Capitano v. Ford Motor Co.*, 2007 WL 586586 (N.Y. Sup. Ct. Feb. 26, 2007). It is also important to make sure that the right people receive the hold notice. *Consolidated Aluminum Corp. v. Alcoa, Inc*., No. 03-1055-C-M2, 2006 WL 2583308 (M.D. La July 19, 2006).

5. Dynamic Databases.[35]

Dynamic databases have become increasingly ubiquitous and provide companies with substantial convenience and efficiencies, but they can complicate discovery. By definition, dynamic database is any database that can constantly change in both structure and content with activity. Most are integral to a company's daily operations, which makes it difficult, if not impossible, to pull them offline for preservation or production. Because they are used in routine job functions that involve creating, modifying, or deleting data, preserving potentially relevant data is a unique challenge. While several of the steps set forth in other sections of this paper are equally relevant here, there are some unique steps to be considered:

Step 1: **Remember the unique aspects of databases.** Often no single user can provide complete information on any given database. Therefore, in considering how to produce a particular database, it is important to understand all of the uses for a given database by its users. By reaching out to those users within the relevant groups, counsel can ensure relevant data is properly preserved and ultimately produced.

Step 2: **Discuss Databases with Opposing Side.** Courts appreciate candor, even though the candid exchange of information between the parties runs counter to the natural inclination of most litigators. *Hopson v. City*

---

[33] Among topics to be covered should be passwords, all email accounts used, and any idiosyncratic shorthand used at the company or in the industry.

[34] *See, e.g.*, *Carbon Dioxide Indus. Antitrust Litig*., 155 F.R.D. 209, 214 (M.D. Fla. 1993) ("[D]epositions to identify how data is maintained and to determine what hardware and software is necessary to access the information are preliminary depositions necessary to proceed with merits discovery."); *Demelash v. Ross Stores, Inc.*, 20 P.3d 447, 520 (Wash. Ct. App. 2001) ("[A] trial court must manage the discovery process in a fashion that promotes full disclosure of relevant information while at the same time protecting against harmful side effects.").

[35] Portions of this section are adapted from David D. Cross, *10 Steps for Conducting E-discovery Involving Dynamic Databases*, A.B.A. Sec. Litig. Spring 2008, at 4.

of Baltimore,[36] discussed below, is but one example of a court's examination of the changes in the approach in discovery. The more recent *Mancia v. Mayflower* also counsels lawyers to work together.[37]

Step 3: **Examine Data Dictionaries.** A database will typically have a data dictionary that describes the design and structure of the database and all its key characteristics. This dictionary enables programmers and users to identify and understand the fields, codes, procedures, processes, and other information in the system. When such a data dictionary exists, it should narrow the amount of data that the party has to preserve and produce by enabling the requesting party to identify specific data rather than blindly serve over-inclusive discovery requests.[38]

Step 4: **Produce Sample Records and Reports.** Sample records and reports can be helpful because they enable the requesting party to determine what fields and codes are actually used in the databases (many fields and codes may appear in a data dictionary, but users often disregard some fields and codes and have their own way of entering or altering data), and the accuracy of labels of the fields and codes (users often enter data that does not correspond to the field or code used because the database lacks a corresponding field or code, and so the users improvise). It may be possible to produce a version of the reports rather than allowing the other side unfettered access to a proprietary database.

Step 5: **Estimate Cost.** The cost of preserving and producing data within a dynamic database can be enormous—even crippling when compared to the amount in controversy. The volume of data also is a key consideration in determining the potential cost of any discovery effort. (This is another reason to produce reports if that is possible.)

V. ETHICAL CONSIDERATIONS.

Several issues arise when considering the duty to preserve evidence. Generally, no duty arises before the litigation is filed, threatened, or reasonably foreseeable unless that duty is voluntarily assumed or it is imposed through other means. The duty to preserve documents or tangible evidence in a given instance can arise from the existence of pending, threatened, or reasonably foreseeable litigation. This duty also can arise from a number of other sources, including a contract, a voluntarily assumed duty, a statute or regulation, or an ethical code.[39]

Given the variety of approaches to these issues applied in different courts, the duty to preserve and the determination of available remedies are dependent on a choice of law analysis. To further complicate the issue, federal courts sitting in diversity disagree as to whether spoliation that occurs during pending litigation is substantive (and therefore governed by state law) or procedural (governed by federal law).[40] An in-depth analysis of the choice of law question may be beyond the scope of this paper, but it merits further consideration once these issues arise. That said, as these continue to arise, some consistency has developed, but this analysis is still important.

A. Professional Responsibilities.

There are several sources for the rules in this area. In addition to the applicable case law, the professional responsibility codes have rules which touch upon this issue. The ABA Civil Discovery Standards set forth the general rule on the preservation of documents:

> "When a lawyer who has been retained to handle a matter learns that litigation is probable or has been commenced, the lawyer should inform the client of its duty to preserve potentially relevant documents and of the consequences of failing to do so."[41]

The ABA Task Force has amended these Civil Discovery Standards to account for electronic evidence. Standard 29 has been modified to provide a checklist of sources of electronic data that should be preserved in order to avoid a spoliation claim. The amendment provides:

---

[36] 232 F.R.D. 228 (D. Md. 2005).

[37] *Mancia v. Mayflower Textile Services Co.*, Civ. No. 1:08-CV-00273-CCB (D. Md. October 15, 2008).

[38] In some cases, a data dictionary can be produced automatically, or manually by examining the fields and codes, or through some combination of automatic and manual processes. Approaching clients before litigation begins might also represent a future cost savings to a thankful client.

[39] *Trevino v. Ortega*, 969 S.W.2d 950, 955 (Tex. 1998) (Baker, J., concurring).

[40] *See, e.g.*, *Keller v. United States*, 58 F.3d 1194, 1197-98 (7th Cir. 1995) (noting the split of authority).

[41] Standard 10. Preservation of Documents, ABA Civil Discovery Standards, August 1999.

> Electronic data as to which a duty to preserve may exist—and the platforms on which, and places where, such data may be found—include: (a) Databases; (b) Networks; (c) Computer systems, including legacy systems; (d) Servers; (e) Archives; (f) Back-up or Disaster Recovery Systems; (g) Tapes, disks, drives, cartridges and other storage media; (h) Laptops; (i) Personal computers; (j) Internet data; and (k) Personal digital assistants.[42]

Other potential data sources include video and web conferencing, company websites, and mp3 players.[43] Additionally, the amendment to Standard 29 adds the language, "electronic data as to which a duty to preserve may exist include data that may have been deleted, but can be restored."[44]

Voice-mail may also be included in electronic sources for clients to preserve, even though it is not included on the amendment to Standard 29. Voicemail can be stored as e-mail attachments, on personal digital assistances, and cell phones.[45] Most businesses, however, typically delete voicemail in a matter of days from the original message. Furthermore, voicemail is easily retrievable from its source, but it is not indexed or readily searchable by any commercially available system.[46] Attorneys who want to retrieve any preserved voicemail should ask for it early in the discovery process so that the opposing party is on notice not to destroy it. The preservation letter should also include a request for the switches to voicemail, which provide a time and origin of the message. Businesses should be proactive and expect that a judge will enter a very broad preservation order, instead of waiting for a spoliation instruction to the jury.

Texas lawyers must also follow Rule 3.04(a) of the Texas Disciplinary Rules of Professional Conduct, which provides "a lawyer shall not unlawfully obstruct another party's access to evidence; in anticipation of a dispute unlawfully alter, destroy or conceal a document or other material that a competent lawyer would believe has potential or actual evidentiary value; or counsel or assist another person to do any such act." However, the Texas Supreme Court rejected an independent tort of spoliation of evidence, finding that spoliation does not give rise to independent damages.[47] The best remedy for spoliation is within the lawsuit affected by the spoliation.[48]

B. Third Parties.

Generally, there is no duty to preserve evidence related to potential claims against a third party. However, if there is a special relationship between the entity and that third party, there may be some duty to preserve the evidence in question. This special relationship may be attorney-client, accountant-client, or something similar. If that special relationship exists, then a party may be held responsible for the acts of a third party. The existence of that relationship mandates that the potential spoliator take affirmative steps to prevent the destruction of the evidence.

This issue is particularly important in the context of destructive testing. If a party delivers an important piece of evidence to an expert or insurer for destructive testing without properly notifying or consulting the opposing counsel, the party could risk potential exposure to a spoliation claim even if the party is not conducting the tests. In general, courts will hold the party responsible for the destruction or damage of evidence if the party entrusted the person who destroyed or damaged the evidence with that evidence.[49]

As a side note, there are a limited number of cases involving the spoliation "victim" attempting to claim damages from the third party, independent of any issue with the other party in the lawsuit. In those cases, courts have been reluctant to allow an independent tort of spoliation, preferring instead to treat the claim as negligence.[50] Given that Texas does not recognize a separate tort of spoliation for parties, it is even less

---

[42] Standard 29. Preserving and Producing Electronic Information. A. Duty to Preserve Electronic Information, Draft Amendments to ABA Civil Discovery Standards, October 2003.

[43] Frazier, Jake and Maher, Heidi, "The X-Files: Issues Surrounding Exotic Forms of Electronically Stored Information," *Expert Evidence Report,* July 23, 2007, Vol. 7 at 383-385.

[44] Standard 29.

[45] David Sumner and Damon Reissman, E-Discovery May Target Unexpected Sources, Law.com, Legal Technology, December 4, 2006, *available at http://www.law.com/jsp/legaltechnology/pubArticleLTN*; Paul D. Boynton, *Voicemail Poised to Become the Next Target of E-Discovery,* LAWYERS WEEKLY USA, July 2003, *available at* http://www.lexisone.com/news/nlibrary/lw070003z.html.

[46] *Id.*

[47] *Ortega*, 969 S.W.2d at 951.

[48] *Id.*

[49] *See, e.g.*, *Thompson v. Owensby*, 704 N.E.2d 134, 140 (Ind. Ct. App. 1998) (finding party culpable for acts by insurance company).

[50] *Elias v. Lancaster Gen. Hosp.*, 710 A.2d 65, 67-68 (Pa. Super. Ct. 1998) (rejecting the spoliation claim without the existence of a special duty).

likely that such a tort would be recognized against third parties in Texas.

Recently, there has been a further complication with regard to third parties, specifically third parties which are repositories for emails and other electronic information. On June 19, 2008, the Ninth Circuit found that a wireless carrier violated the Stored Communications Act by disclosing the contents of text messages to a subscriber without the consent of individuals who sent or received messages using the city-owned pagers.[51] The *Arch* decision relied heavily on the Stored Communications Act, which prevents such disclosure.[52] *See* 18 U.S.C. § 2702 *et seq.* The City of Ontario (the defendant below) had argued that the wireless company in question was a "remote computing service," but the Court held that it was functioning as an "electronic communication service."[53] The Court also held that individuals sending and receiving text messages have a reasonable expectation of privacy under the Fourth Amendment. This decision may have far-reaching impact in that providers can no longer turn over the contents of messages unless they follow the Stored Communications Act. For messages that are 180 days old or less, that means a search warrant instead of a subpoena for cases involving law enforcement. In cases involving private litigants, consent of an originator, addressee or intended recipient will be an important new requirement for disclosure.

VI. MANAGING A PRODUCTION.

Unfortunately, most times, the attorneys are not called in until litigation has already started. At that point, the client's in-house attorneys, other outside counsel, IT staff, and key employees, are all critical in locating relevant electronic data. That said, relying solely on the IT staff may be a mistake. The basic function of the IT department is to make sure that nothing is lost. It is not to make sure that only necessary things are kept—which is the goal of a document retention program. As part of an attorney's role in this process, the attorney should be asking:

- How to implement strategic e-discovery plans, including identifying, locating, retrieving, preserving and authenticating electronic evidence;
- What is the most cost-effective means for responding to discovery requests, with requests with minimum disruption; and
- What are the special considerations for the responses and objections to interrogatories and requests for production.

Given these challenges, it is often advisable to hire an expert on these types of issues at a very early stage.

Ignoring systems that are antiquated, damaged or burdensome to be searched may also put you in hot water with the courts.[54] There are a number of experts that are well-equipped and professionally trained to work with these types of systems so don't assume that you can use the seemingly inaccessible nature of the data as a defense. The important thing to do is get involved with experts early to determine what can and can not be done with your data and systems.

The amount of data that is potentially relevant is often underestimated at the start of discovery projects, and if the Court issues an order directing retrieval of a document originally not produced, it could give the appearance of impropriety and may lead to sanctions. **It is critical that practitioners understand these nuances before agreeing to any protective orders or production schedules. The cost ramifications can be significant.**

It is critical to understand where relevant data is stored and how much data is at issue. Even before a lawsuit involving electronic data is commenced, in-house and outside counsel should understand how their company's information systems are set up, and what procedures are in place to store—and destroy—electronic data.

It is important to emphasize the difference between electronic data and paper documents.[55] Unlike shredding or burning a paper document, using the "delete" key does not necessarily discard an electronic document. The electronic document is

---

[51] *Quon v. Arch Wireless*, ---F.3d----, 2008 WL 2440559 (9th Cir. June 19, 2008).

[52] *See* 18 U.S.C. § 2702 *et seq.*

[53] *Id.*

[54] One particular type of media that warrants additional discussion is backup tapes, which were designed for recovering information in the event of a disaster, not for litigation purposes. As a result, data is not organized in a document production-friendly manner. In fact, e-mail, accounting, word processing documents, and databases information are often commingled on the same tapes making it more difficult to locate the key documents you are looking for. Another aspect of backup tapes that makes them a significant challenge with regards to litigation is that these tapes are generally rotated every 30, 60, or 90 days. Failure to halt these policies immediately on anticipation of litigation will result in lost data and subject the company to potential spoliation sanctions. *See E*Trade Sec. LLC v. Deutsche Bank AG*, 230 F.R.D. 582 (D. Minn. 2005)(noting that the failure to preserve DVDs containing voicemail and backup tapes warranted sanctions).

[55] *See* Robert A. Creamer, *Ethics and Lawyer Liability Issues in Electronic Discovery* (May 13, 2005) at 1-2 (on file with author).

likely to reside in various locations. Additionally, embedded information called metadata is contained in electronic documents. The metadata does not appear on paper documents or on the computer screen. It allows an expert to determine what edits were made to the documents, how many versions are in existence, and the date and time of creation.[56]

Also, a significant difference between discovery of paper documents and discovery of electronic documents is the organization of each. The process by which team members organize paper documents differs from the organization process involving electronic documents. Since electronic documents can be searched by name, key phrase, or date, one has the ability to organize the document review chronologically, by sender, or by conversation topic. The headache of sorting through documents as they appear in a pile is somewhat eliminated.

That said, electronic documents are not always easier to sort than paper. A common dilemma one may encounter is legacy data. Legacy data cannot be read by the software used to review the documents. This problem occurs because of the IT staff's tendency to often upgrade or replace software. The software that can read the older documents may not be available immediately.

In sum, gone are the days when paper documents were found only in someone's office or briefcase. Today it is not uncommon for individuals to secretly carry around slim thumb or lipstick drives—which, despite their small sizes, can hold hundreds of thousands of pages of data. In the much publicized Kobe Bryant case, District Judge Terry Ruckriegle ordered AT&T to turn over text messages that were sent from the cell phone of the woman who accused Bryant of rape and that might be "highly relevant" in determining whether Bryant is guilty. As these situations demonstrate, data can be found in many different places today and on an increasing number of devices. The most common locations are desktop and laptop computers, network hard drives, removable media (floppy disks, tapes, CD-ROMs, thumb or lipstick drives), back-up tapes, personal digital assistants and cell phones. Third parties, such as Internet service providers, may also be in possession of data.

[56] In March 2005, the New York Times reported that the BTK was caught, in part, because of metadata on a disk he had delivered to a local television station. The police used the disk to track BTK to a local church, and to Dennis Rader, president of the church council, who had recently used the computer. Monica Davey, Computer Disk Led To Arrest In Killings, Pastor Says, NEW YORK TIMES, March 2, 2005, at A 12.

A. Types and Amount of Data.

Determining what type(s) of data you will be producing—and how you will produce them—is imperative. Are you only producing e-mails, word processing documents, spreadsheets, database information, or a combination of these types of data? Once you know this, you will need to determine what packages and versions of software were used in creating this data. For example, is the e-mail Microsoft Outlook, Lotus Notes, Groupwise, etc. The type of data can have bearing on exactly what can be done with the data in the filtering and processing stages, and not all e-discovery vendors have the capabilities to work with all software packages and versions. For example, the 2007 Fulbright Litigation Trends Survey noted that more than half of the survey respondents allowed instant messaging and almost three quarters allowed employees to access the computer from home.[57] These concerns will be important for companies to address when determining the scope of the issue.

The amount of data that is potentially relevant is often underestimated at the outset of electronic discovery projects, especially by those who have little or no prior experience with electronic evidence. There are a few reasons for this. First, employees create more electronic information than you think. And second, people assume that "e-phobic" individuals are not using their computers when in fact their assistants are retrieving and responding to e-mail on their behalf. Keep in mind, if the Court issues an order directing retrieval, or worse yet, the opposing party happens to have e-mail from that individual and those records were not produced, it could give the appearance of impropriety and may lead to sanctions. If you do not have an understanding of how much data you are working with, e-discovery experts can help you estimate page counts based on their experiences if certain information such as the number of custodians (the persons, places or things from which the data was derived) and the type of media is known.

B. Data Collection.

Not many years ago, the destruction of documents meant simply throwing them in the trash or running them through a shredder. Today, the question of whether a document was destroyed or tampered with demands more consideration. Computer users destroy and alter electronic data every day, and often without knowledge. Simply turning on a computer can overwrite documents such as those in "slack" and "temporary" files. And just clicking on a file can

[57] Fulbright & Jaworski's 4th Annual Litigation Trends Survey at 23 (available at www.fulbright.com/litigationtrends).

change the document's metadata (data about the data) such as the "last-accessed" date.

So how can you avoid spoliation issues when data may be relevant to a lawsuit? Best practices dictate that you immediately make a copy of relevant data using mirror-imaging technology and halt electronic document-destruction processes such as the recycling of backup tapes. Mirror imaging creates a copy of every sector in the computer's hard drive. This is very different from simply copying every file, which may result in alterations such as those listed above. While many internal IT departments are familiar with mirror imaging technology, e-discovery experts can also assist you in securing this data and explaining what actions could potentially cause spoliation. An added benefit of working with an outside expert to perform mirror imaging services is that you have independence in the process, lessening the chance of any questions of impropriety.

Those of us who breathe this stuff every day know that mistakes made at the start can be very difficult **(read: expensive)** to fix later. The following mistakes are adapted from an article in Kroll OnTrack's monthly newsletter.[58] Each project (and its incumbent challenges) will be different, but this list is a solid beginning as to the concerns practitioners might face and pitfalls they should avoid:

1. Failing to Have a Data Collection Plan. Having an initial data collection "plan of attack" is vital in every electronic discovery situation.

2. Failing to Prioritize the Data. Clearly defining the collection scope and priority of key players will avoid creating unnecessary delays and increased costs down the road.

3. Neglecting to Conduct Thorough Interviews. Counsel must make it a priority to thoroughly interview the IT team regarding the client's IT systems.

4. Ignoring Key Data Locations & Important File Types. Often, it can be difficult to ascertain where electronic evidence is held.

5. Conducting Do-It-Yourself Data Collection. Many software products allow a client to collect data themselves. This is, unfortunately, the fastest way to create significant problems for the client several months later, when the problems can no longer be fixed.[59]

6. Performing Dangerous Desk-side Collection. Courts have consistently held that diligent and effective ESI preservation and collection efforts are required under the new Federal Rules of Civil Procedure amendments.[60]

7. Failing to Mirror Image v. Imaging Excessively. *Remember that this area of the law is new and, to some extent, untested*. Unfortunately, the person grading performance does so two years after the acts were completed, but with proper documentation, clients can achieve good results.[61]

8. Limiting Names. When collecting data, consider alternative names, including maiden names, initials, nicknames, e-mail addresses, and everything else. I have learned this the hard way.

9. Assuming IT Can Shoulder the Burden Alone. Kroll notes that IT does not always understand how to best handle data subject to legal discovery. I could not agree more.

10. Failing to Maintain Proper Chain of Custody. Proper documentation includes indicating where the media has been, whose possession it has been in, and the reason for that possession. If you do this incorrectly, you might not be able to fix it.

When hiring an outside expert to perform your data collection, you will need to provide them with information about what they should expect onsite:

- Where, and in how many locations, is the data stored?
- When will the collection take place?
- What types of hardware, operating systems and software are involved?

---

[58] Kroll OnTrack, *Practice Points: Top 10 Data Collection Pitfalls*, CASELAW UPDATE AND E-DISCOVERY NEWS, April 2005 (found at http://www.krollontrack.com/newsletters/clu/apr05.pdf).

[59] This portion of the paper is adapted from *The Perils of Custodian Self-Collection*, EnCase Legal Journal, January 2008, at 118.

[60] *See, e.g.*, Samsung Electronics v. Rambus, 439 F. Supp. 2d 524 (E.D. Va. 2006); Cache La Roudre Feeds, LLC v. Land O'Lakes, inc., 244 F.R.D. 614 (D. Colo. 2007); In re Hawaiian airlines, Inc., 2007 WL 3172642 (Bkrtcy. D. Hawaii October 30, 2007); Google Inc. v. Am. Blind & Wallpaper Factory, Inc., 2007 WL 1848665 (N.D. Cal. June 27, 2007).

[61] *See Galvin v. Gillette Co.*, 2005 WL 1476895 (Mass. Super. May 19, 2005) (Court holds that e-mails need not be produced where Gillette demonstrated that compliance would be "daunting" and nearly impossible).

- How many drives are going to be imaged?

C. Filtering

Not every electronic document found on a custodian's computer or on backup tapes is responsive or relevant to a discovery request. Therefore, data filtering is a must. In fact, there is a cost to handling too many documents. Most e-vendors will charge by the document or page (although they vary on when in the process the cost is assessed). Also, the more documents you do not eliminate through some other measure, the more time your people will spend reviewing documents. This cost is not one to be underestimated.

If the amount of data collected in the steps above brings up questions like, how are we going to review and produce all of this data by our discovery deadline, don't panic. One of the characteristics of electronic data that can make your life easier is the ability to filter your documents. Filtering techniques extract documents based on specific dates, custodians, keyword searches, and file types, and they also offer de-duplication options so that you do not have to review the same document twice. Effective filtering parameters can reduce your data by an average of 75 percent, which often results in significant cost savings through lower processing costs and more efficient document review.

When you get to the filtering stage, you will need to make several decisions:

- What dates are relevant to your lawsuit?
- How many custodians' data do you need to review? This will have a significant impact on the amount of data you will be reviewing. Do you have a priority for which custodians' data you want to review first? Where there is a long list of custodians, you may want to prioritize; review documents from a subset of custodians first, and then determine whether you will still need to process and review the data from the additional custodians.
- As discussed above, what file types do you want processed? Are there any you would like excluded, such as graphic or database files?
- Will you be searching for keywords? If so, you will need to create your list of keywords before the filtering stage begins. A list of keywords that is between 30 and 50 terms is recommended to find potentially relevant information while not being over inclusive of irrelevant data. Some other suggestions when creating key words are to use "whole words" instead of the first few letters of a word which will likely take hits on irrelevant words. Avoid noise words (such as "the," "it," "a," "an"), initials and acronyms if possible. Use Boolean searches, such as "and," "or," "not," to help broaden or narrow your search.
- Do you want your electronic discovery expert to tag unusually large files so that you can review them in their original native format before processing them for review?
- Do you want to de-duplicate your documents? At the custodian or universe level? During the de-duplication process every file is analyzed at the bit level to determine exact duplicates.

The answers to these questions are not self explanatory. This is more than picking a list of interesting people. It is developing an overlay of which custodians need which set of keywords and at what time. The important piece is that this work needs to be done early in the case, before any documents are reviewed.

The paradox at the core of electronic discovery is that, in many cases, litigants will know all of the keywords and the relevant time frames, but litigation cases often take unexpected turns that require different keywords and time frames. Some are explicit through amended pleadings, some are less direct. When this happens in paper-intensive cases, the solution is to return to the company's files. In cases that have electronic documents, there is spoliation and increased costs.

Just eliminating documents during the filtering stage can result in an average of 20 to 50 percent reduction of data. If you choose to use your electronic discovery vendor's online review tool to review your documents you will only need to review one instance of a duplicated document, and may have the choice to repopulate your duplicates for production, depending on the technology capabilities of the expert. Adequate handling of electronic duplications can decrease the costs associated with discovery and can provide insight into issues such as privilege, prior negotiations, and other background information.[62]

VII. BRINGING IN ADDITIONAL TROOPS: THE OUTSIDE E-VENDOR.

Given these challenges, it is often advisable to hire an expert on these types of issues at a very early stage. If you choose to work with an outside e-discovery expert, it is extremely helpful to provide them with certain information during early discussions:

- On what media will the data be provided (*i.e.*, PSTs on CDs, word processing documents on a hard drive, etc.)?

[62] Stephanie Sabatini, *The Dilemma of Duplicates* (January 15, 2004), *available at* http://www.law.com.

- How many pieces of media is the data contained on?
- Do you know how much data (often measured in gigabytes) is on each piece of media?
- Which e-mail package(s) and what version(s) were used?
- What is the make and model of the drives used to create the backup tapes?
- What is the type and version of the backup software?
- When will the data be available for your expert to begin?
- What are your deadlines for review and production?

Learning this type of information as early in the process as possible will allow you (and your expert) time to determine if there will be any problems regarding issues such as restoring the back up tapes, working with certain e-mail packages or other applications, or processing and turning around your data in a timeframe that meets your deadlines.

For larger companies and those with a heavier litigation volume, it may make more sense to have an internal team handle the e-discovery.[63] In addition to cost savings, establishing a systemized and consistent process reduces business disruption and mitigates risk by enhancing compliance. A systemic process executed with plugged-in enterprise tools, run by a well-trained internal team familiar with the organization's IT infrastructure and that works alongside corporate legal, is well-suited to meet the "early attention" requirements of the amended Federal Rules. In fact, recent case-law supports the defensibility of organizations handling e-discovery internally where best practices are employed.[64] Over the past few years, the developments in this area have been significant.

However, e-discovery service providers may still be an important part of the process. Many consultants help to design efficient and systemized processes that are largely executed by IT. Companies may want to concentrate on preferred providers in this area. Consultants can also effectively augment company staff for larger engagements, as well as routine overflow. Outsourcing is also usually a good option for mid-sized companies with lighter litigation volume. An untrained ill-equipped and unprepared internal IT team may be the worst of all options, but an internalized process with the right technology, people, training, and well-defined procedures is proving to be the most effective option for large organizations.

A. Processing.

A common debate with regards to the electronic discovery process is whether documents should be kept in their native file format, which is the format in which the documents were created, such as MS Word, MS Excel, etc., or whether they should be converted to a uniform format, such as .tiff or .pdf. This decision should be made at the outset of the electronic discovery process as it impacts almost all of the other steps. There are advantages and disadvantages to both native review and converted file review, which will not be discussed here, but it is important to evaluate these factors before deciding how you would like to review your data.

If you choose to convert your documents, they will be converted to .tiff or .pdf, and at that point you will have the choice to review your documents from a CD or DVD, in a litigation support database, such as Summation or Concordance, or via an online review tool, which is a Web-based tool in which your electronic discovery provider loads your documents so that you can view your documents online and perform review functions such as categorizing, redacting, and searching. Converting too much can be expensive, so it is important to reduce volume as much as possible beforehand.

Presently, the online document repository has become much more common as a way to review large numbers of documents. There are several reasons for this:

- It is easy to share documents between lawyers and law offices.
- It is easier for lawyers to work on the same set of documents and make notes for the other lawyers to find.
- It allows lawyers to access documents from any location.
- Documents are less likely to be overlooked.
- It is easier to track the team's progress, if you choose the right e-vendor. This is also true for categorizing the documents.

Furthermore, an electronic document repository can be used as the manner of production. In other words, once the review of documents is complete, the attorneys can merely transfer the production set to a database established especially for opposing counsel. There should be a discussion as to who should pay for this database.

While there is a lot to consider when evaluating and producing electronic data, understanding the process upfront can result in significant savings in

---

[63] *The Defensibility of an In-House Process*, EnCase Legal Journal, January 2008, at 126.

[64] *See, e.g.*, *Williams v. Massachusetts Mutual Life Insurance Company*, 266 F.R.D. 144 (D. Mass. 2005); *Residential Funding Corp. v. DeGeorge Financial*, 306 F.3d 99 (2d Cir. 2002).

terms of cost and time. It may also obviate the possibility of sanctions due to the inadvertent destruction of data.

B. Finding the right online repository

When selecting an online repository, there are several questions that you should ask. There are several levels of e-discovery providers, and each of their systems has slightly different capabilities. These questions will help with the differentiation.[65]

1. Speed – These days, almost every provider takes advantage of high speed connections. If you do not have one, you need to discuss this explicitly with the vendor in question—or you will spend a lot of time waiting in the future. That said, some providers download the documents directly to your PC; and some of those download one page at a time. On the other hand, some have you log into a secure server that they control. You need to ask and see a demonstration. No system is perfect, but you need to understand what you are getting.

2. Security – This series of questions encompasses several issues. The reviewers should be able to categorize, but not change documents. This is true regardless of how the documents are being maintained (tiff, PDF, or native format). The system must also be secure from outside attack. The level of protection needed will vary from case to case. In some cases, the attorneys will want to discuss this more fully with the vendor.

3. Ease of Use and Functionality – The only way to evaluate this is the test drive. Be sure to include actual review in the testing group. Many of the e-vendors systems look a lot like Outlook, so the basic use should not be a challenge. The second order functions that are worth asking about are: how easy is it to transfer a collection of documents, can reviewers communicate about documents easily within the system, how easy is it to print, how can notes be taken about specific documents, how do reviewers create privilege logs, and how are documents tracked.

4. Avoiding Multiple User Abuse – A review of electronic documents will probably involve a large number of reviewers. The handling of multiple reviewers must be seamless. It may be preferable to have the system lock out reviewers once one is reviewing a document. The logging system discussed below is an important part of this too.

5. Self Administration – Here, the bottom line is that you will want to be in control. Waiting for an admin at the e-vendor to make any change for you is just not efficient. Keep in mind that not everyone is working in your time zone. There are degrees of this, but you will want some autonomy. Among the key functionality you may want to control are adding new reviewers, modifying reviewer profiles, and assigning data sets.

6. No special software – You will probably want to have a system that you can use from anywhere or any computer. Today's firms are not always receptive to having individuals install software on PCs, so the need for additional installs should be avoided. This is not to say that security is not a concern, but focusing on this will hopefully lead to great flexibility and efficiency.

7. Organizational Parameters – With any large document review, the attorneys will need to capture the information gleaned from the review. Critical to this is the way in which the repository is organized and can be managed. At a minimum, there should be an extensive foldering function and the ability to tag and make comments on individual documents. It is also helpful if at least some reviewers can mass-categorize.

8. Searching Functions and Logging Changes to the Classifications – This is another aspect that you can only understand with a proper test drive. You will need to review to understand how the review is progressing, and to prepare for depositions and other discovery. You will also need to be able to determine who has modified documents and sometimes when it was modified.

9. Output – This is important from a timing point of view. You will be making arrangements with opposing counsel as to when documents will be produced, but before that you will need to fully understand how long it takes, what formats are possible, and how the e-vendor will capture the exact set of documents to be produced. These are not small issues. You should also ensure that some subset of the review database can be moved into a production database if needed.

---

[65] This list is based on the factors contained in Lange, Michele C.S. "E is for Evidence: Using an Online Repository to Review and Produce Electronic Data," originally published in Journal of Internet Law June 2003, and available at http://www.krollontrack.com/.

10. Privilege Searching and Log Creation – Any collection of documents will have privileged documents among them. Most e-vendors have a method for identifying those documents and isolating them from the other documents (which will be produced). Given the inevitable problem of inadvertent disclosure, the attorneys need to reach a high comfort level on this issue.

11. Coordination with Paper Documents. Depending on the review, you may also have a significant number of paper documents as well. Some online repositories allow for the upload of these types of documents. Others do not. If you do upload them, these documents will not have metadata, unless you put it there. This is an additional expense to be considered.

C. Dealing with a Production Team.

Regardless of size, an electronic discovery production team needs to be coordinated. There is substantial non-substantive training that will often be required, and for a complicated case, refresher courses are probably a good idea as well. The key is to keep the communication lines open. This can be done through several mechanisms, including regular calls or meetings with:

1. The review team. These meetings would initially start on substance—making sure that the documents being reviewed by different people get marked the same way. As time goes on, these meetings would become the best way for the team leaders to assess how the review is going and the best use of resources. At some point, the need for these meetings might decrease.

2. The e-vendor. These meetings would initially involve getting all the information to the e-vendor. Then, the topic would become getting all of the information properly loaded, and finally, the topic would migrate to technical issues related to the review and the production. These meetings are essential to the proper scheduling of production and meeting deadlines, particularly if the review involves several different firms.

3. The client. Shocking. These meetings would initially involve collection issues, but because the costs can be so prohibitive, these meetings would provide a vehicle to keep the client onboard with the process. Additionally, if the review needs to expand, this allows the outside lawyer to warn the client as early as possible.

While it is possible to combine these meetings, it is not always the most efficient use of time.

VIII. PRIVILEGE. PRIVILEGE. PRIVILEGE.

Maintaining privilege must be at the core of the entire production process. As one might expect, there are nuances with privilege and electronic data. For example, a court recently ruled that an employee's use of the employer's e-mail system for privileged communication with his personal attorney does not necessarily constitute waiver in a bankruptcy adversarial proceeding.[66] Courts have recognized that e-mails are often internally forwarded and this does not result in waiver of the privilege.[67] In *Premiere Digital Access*, an e-mail from in-house counsel had been forwarded to other employees and produced from those employees' in-boxes. This was not discovered for a year.[68] The Court held that this production was inadvertent and did not waive the privilege.[69]

A. Rule 502.

Recently, President Bush signed a law creating a new rule, Rule 502 of the Federal Rules of Evidence. Under this new rule, inadvertent disclosure of privileged or protected information during discovery would constitute a waiver only if the party did not take reasonable precautions to prevent disclosure and did not make reasonable and prompt efforts to rectify the error.

At present, the proposed rule:

- **i.** Applies in all cases in federal court, including cases in which state law provides the rule of decision.
- **ii.** Applies in state court with respect to the consequences of disclosure previously made at the federal level.
- **iii.** Emphasizes that a subject matter waiver occurs only when the waiver is intentional.
- **iv.** Mandates that parties are not required to take extraordinary efforts to prevent disclosure of privilege and work product; nor are parties required to conduct a post-production review to determine whether any protected information has been inadvertently disclosed.
- **v.** Applies the protections against waiver by inadvertent disclosure to federal offices or agencies.

---

[66] *In re Asia Global Crossing Ltd*, 322 B.R. 247 (S.D.N.Y Mar. 25, 2005).

[67] *Premiere Digital Access, Inc. v. Central Telephone Co., d/b/a Sprint of Nevada*, 360 F. Supp. 2d 1168 (D. Nev. 2005).

[68] *Id.*

[69] *Id.*

vi. Has no language allowing for selective waiver.[70]

B. The Privilege Log.

Privilege logs in the e-discovery universe can be very large—several thousand entries is not unusual. As such, it is often difficult to produce privilege logs. In jurisdictions where privilege logs must be produced simultaneously with the unprivileged documents, attorneys would be well advised to negotiate a several week delay (if not several months) before any privilege log is due. Also, in terms of process, you will want to identify potentially privileged documents automatically and then have a second "high powered" team make these difficult calls. This will hopefully minimize the chance of mistakes

Preparing a privilege log has its own challenges. To protect the privilege as to a certain document, a party must "describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected." FED. R. CIV. P. 26(b)(5). Courts have refined the structure of privilege logs, and in the world of e-discovery, where the lists can have more than 10,000 documents at issue, some standards have developed.

For example, the court in *In re Universal Service Fund Telephone Billing Practices Litigation*,[71] required that the privilege log include:

i. A description of the document explaining whether the document is a memorandum, letter, e-mail, etc.;
ii. The date when the document was prepared;
iii. The authors of the document;
iv. The recipients of the documents (including the persons who merely received copies),
v. A description of the document that supports the assertion of the relevant privileges.
vi. The number of pages of the document;
vii. The specific privilege or protection being asserted; and
viii. Any other necessary information to establish any asserted privilege.[72]

Importantly, *Universal Systems* requires that the privilege log separately address *each individual email within an email thread* for which privilege was claimed.[73] In addition, it is also important to accurately identify every person who received each email within an email string, including the title of each recipient and which recipients are attorneys providing legal advice. The privilege log must also explain how the communication was for the purpose of obtaining legal advice.[74] Lastly, the subject matter description on your privilege log must demonstrate that every email in an email string involved communications involving legal advice. A generic email subject line (e.g., Board Meeting Discussion Topics) or a general descriptions of the topic (e.g., Email string regarding Board Meeting Discussion Topics) may not be enough for the courts.[75]

C. The Privilege After Production.

In addition to Rule 502, amended Rule 26(b)(5) was designed to specifically address inadvertent disclosure when volumes of files containing e-mails and other electronically stored information have been disclosed. Under the amended rule, if information is produced in discovery, which is subject to a claim of privilege or 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. This notice must be in writing unless circumstances—such as the disclosure of privileged information during a deposition—preclude it. After being notified of a claim of privilege or protection, the receiving 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. The advisory committee included this provision, in part, because the receiving party may have included this information in its trial preparation materials. Also, if the party that received the information disclosed it to a non-party before being notified, the party must take reasonable steps to retrieve the information.

The Rule also affords the party receiving the privileged information the right to challenge the assertion. The new rule states that a party receiving a notice of claim of privilege or protection may promptly present the information to the court under seal for a determination of the claim. The producing party shall

---

[70] "Selective waiver" applies when a party has previously produced materials to a government entity performing investigatory functions, and then seeks to protect that information because the information was not waived through the voluntary surrender of the information to the governmental entity. *See In re Qwest Communications International Inc.*, 450 F.3d 1179 (10th Cir. 2006). It is a doctrine that has not been broadly accepted by courts. *Id.*

[71] 2005 WL 3725615 (D. Kan. July 26, 2005).

[72] *Id*. at *3.

[73] *Id*. at *4.

[74] *See generally* Long, *Email and Attorney-Client Communications: A Primer for Creating Privilege Logs*, A.B.A. Sec. Litig. Spring 2008, at 1.

[75] *See, e.g., In Re* CV Therapeutics, Inc. Sec. Litig., No. C 03-03709, 2006 U.S. Dist. LEXIS 38909 at *35 (N.D. Cal. Apr. 4, 2006).

preserve the information until the claim is resolved. Accordingly, notice must be sufficiently detailed so that the receiving party can determine whether to challenge the claim. Also, if challenged, detail is needed to assist the court as to the basis of the claim.

D. Hopson and Victor Stanley.

One of the more often discussed cases on these issues is *Hopson v. Mayor of* Baltimore. 232 F.R.D. 228 (D. Md. 2005). In *Hopson*, a class action alleging race discrimination, plaintiffs served discovery requests seeking electronically stored information (among other documents). The responding party produced privileged information because it did not conduct a full privilege review. Plaintiffs filed a motion to compel additional information based on those privileged, but produced, documents.

The court examined the Rule 26(b)(2) factors to determine whether the less than full review was reasonable given the extent of ESI, the time to produce it, and if full privilege review was feasible. The court also examined whether the procedures agreed to by counsel were reasonable. If the agreed procedures were reasonable, the court would approve those procedures, and those procedures would not result in the waiver of any privilege or work product claim for any inadvertently produced privileged material.

The court focused on the defendants' privilege review, both pre- and post-production. As a baseline, defendants bore the burden of demonstrating with particularity the need for less than full pre-production privilege review, as well as proposing reasonable alternatives.

The court noted that the proposed changes to Rule 26(b)(5) allows a party to raise post-production claims of privilege and work product protection for electronically stored information, and further establish a procedure for resolving disputes regarding such an assertion. However, the court noted: "The proposed amendment does not address the substantive questions whether privilege or work product protection has been waived or forfeited." Instead, the amendment sets up a procedure to allow the responding party to assert a claim of privilege or of work-product protection after production. Rule 26(b)(5)(2) does not address whether the privilege or protection that is asserted after production was waived by the production.

The court described three distinct positions on the inadvertent production of privileged material:

a. the "strict accountability" approach of the Federal Circuit and the First Circuit (which almost always finds waiver, because "once confidentiality is lost, it can never be restored");

b. the lenient, "to err is human," approach of the Eighth Circuit and a handful of district courts (which view waiver as requiring intentional and knowing relinquishment of the privilege, and find waiver only with inadvertent disclosure and gross negligence); and

c. the "balancing test" approach that requires the court to make a case-by-case determination of whether the conduct is excusable so that it does not entail a necessary waiver.

The court concluded that, given the proposed changes to Rule 16(f), "the better approach" is to assume that complete pre-production privilege review is required, unless it can be demonstrated with particularity that it would be unduly burdensome or expensive to do so; and counsel have a duty to take the initiative in meeting and conferring to plan for appropriate discovery of electronically stored information at the commencement of any case in which electronic records will be sought.

E. Non-Waiver Agreements.

It is well documented that the time, delay, and costs associated with an e-discovery privilege review are substantial. To mitigate these costs and the risk of waiver, the advisory committee appears to encourage parties, during their 26(f) meeting and conference, to enter into non-waiver agreements that become part of the Rule 26(f) order. Although helpful, these agreements are not dispositive of whether privilege has been waived. If, however, the assertion of privilege is challenged, these agreements will provide evidence that the parties did not intend to waive the privilege or protection.

One such agreement is called a "quick peek" agreement. Under this type of agreement, the responding party will provide certain requested materials for initial examination without waiving any privilege. The requesting party then designates the documents it wishes to have actually produced. This is the Rule 34 request. The responding party then responds in the usual course, screening the documents actually requested and asserting privilege to those documents as outlined in Rule 26(b)(5)(A). Another type of non-waiver agreement is called a "clawback agreement." Under a clawback agreement, the parties agree that production made without intent to waive privilege or protection should not be a waiver so long as the responding party identifies the documents mistakenly produced, and that the documents should be returned under those circumstances. Other voluntary agreements may be appropriate depending on the circumstances of the particular type of litigation. Once

the parties have reached an agreement, they should have the agreement included in the court's case management order pursuant to the court's discretionary authority under Amended Rule 16(b). According to the advisory committee, in most circumstances, a non-waiver agreement and its inclusion in a case management order should preclude waiver of an inadvertently produced privileged or protected document.

The open question under the new rule is whether the non-waiver agreement will stand up to a challenge by the receiving party. While the tone and direction of the rule is to avoid waiver, the decision as to whether a non-waiver agreement will preserve a privilege or protection is province of the courts. Currently, there are three approaches that courts throughout the country use to determine whether a non-waiver agreement will preserve privilege: a restricted approach, a middle-of-the road approach, and a non-waiver approach. Under the restricted approach, privilege is not preserved despite the non-waiver agreement. Under the non-waiver approach, the non-waiver agreement preserves privilege or protected information, unless the conduct of the producing attorney is viewed as grossly negligent. Under the middle-of-the-road approach, the non-waiver agreement is balanced against the reasonableness of the conduct of the producing attorney. Accordingly, it is vitally important for you to know the approach to non-waiver agreements, if any, in your jurisdiction.

Subsequent to *Hopson*, the defendants' failure to pursue a court-approved non-waiver agreement in *Victory Stanley, Inc. v. Creative Pipe, Inc.*[76] proved fatal to their claim. The defendants attempted to locate and segregate privileged documents by performing simple keyword searches. They failed to identify 165 privileged documents in their review and subsequently produced those 165 documents to the plaintiffs. As the plaintiffs found the documents, they immediately segregated them and notified the defendants of the existence of potentially privileged documents in their possession. The court held that the defendants' keyword searches were not reasonable precautions, and that the privilege was consequently waived as to those documents. The court also indicated that a court-approved non-waiver agreement would have protected the defendants from waiver.

F. The Future.

Although Amended Rule 26(b)(5) gives producing attorneys some direction for preserving privilege, it does not provide any confidence or predictability that the producing parties' pre- and post-production actions will preserve privilege. More help may be on the way if the proposed amendments to the Federal Rules of Evidence are adopted. As mentioned above, proposed Rule 502(a) will offer additional protection, once approved by Congress.

Amended Rule 26(b)(5) is a step towards more effective management of the costs, delays, and risks associated with producing documents in the e-discovery era. However, by no means does its adoption signal the end of the burdensome privilege review. Until a definitive ruling has been made enforcing non-waiver agreements, or until proposed Rule 502(a) is adopted, the wiser approach is for producing parties to engage in a complete privilege review. In addition to a full privilege review, producing parties should, as a matter of course, discuss and enter into some type of non-waiver agreement regarding inadvertent disclosure during the Rule 26(f) conference. The parties should also insist that courts, pursuant to Rule 16(b), make the non-waiver agreement part of the case management order. These actions do not guarantee that privilege will be preserved. However, at this point in the e-discovery era, compliance with amended Rule 26(b)(5) gives producing parties the best chance to avoid inadvertently waiving privileges and protections.

Given the volume of production, there must be a protocol from the outset to minimize the number of privileged documents that are inadvertently produced. Disclosure could result in waiver of privilege for that document or worse still, a waiver of privilege for that document and other documents on the same subject. The easiest way to handle this is to come to an agreement as to inadvertently produced documents early in the litigation.

IX. TRANSLATING THE BYTES: USING E-DOCUMENTS IN LITIGATION.

Once the effort of learning the landscape of electronic discovery has yielded a smoother and more efficient discovery process, a lawyer must use the fruits of discovery in an effective manner. Making effective use of electronic data is primarily important in two phases of litigation: first, in the initial stage of discovery when large amounts of data are received and efficient filtering is necessary, and second, in using the electronic data effectively at trial.

A. Reviewing Discovery Results for Useful Information.

Even after analyzing interrogatory responses and deposing the proper corporate representatives to narrow the scope of discovery, lawyers will still likely face a considerable amount of electronic data from which to assemble a case. Many times, the volume of data cannot be predicted in advance because information about how it is processed is only revealed after processing has begun. A cursory examination and

[76] 250 F.R.D. 251 (D. Md. 2008).

selection of information can hide significant facts that once seemed like a negligible amount of data but, after review and restoration, expands significantly beyond original expectations. In order to take advantage of the resource that electronic data can represent, however, it is important to know how to review the data quickly and accurately. As discussed above, there are several possibilities. Recently, a federal judge in New York held that the party responding to a discovery request met its obligation by producing responsive electronic information in a text-searchable format.[77] The court in that case relied in part on the Sedona Conference Working Group paper on electronic discovery.[78]

Metadata, mentioned above, can be valuable background information embedded within the electronic version of a document but not necessarily apparent from a hard copy. For example, categories of metadata embedded in a Microsoft Word document include:

- *Track Changes.* Shows changes that have been made to a document, including text that has been deleted.
- *Last 10 Authors*. Provides names of the last 10 people to have worked on a document.
- *Comments*. Allows people viewing a document to make comments that do not become part of the text.
- *Document Statistics*. Lists people who worked on a document, how long they worked on it and how many revisions they made.
- *Versions*. Displays different versions of the same document.
- *Routing Slip*. Reveals the names of people who have received copies of the document.
- *Template*. Reveals information about the origins of a document.[79]

This metadata can be particularly important where issues regarding revisions to documents are at issue or where establishing that a specific individual had knowledge of such a document or item of information is crucial.[80]

Unfortunately, one of the negative characteristics of e-discovery is that requesting parties frequently are convinced that there is a "smoking gun" somewhere in the electronic files. This leads to suspicions about the thoroughness of ESI production and to discovery on discovery. Likewise, producing parties are likely to cry "fishing expedition" whenever the ESI production is questioned. Recent cases have indicated that discovery on discovery is more likely to be allowed if the likelihood of finding a "smoking gun" is high and that it is less likely to be allowed if the likelihood is low.[81]

B. Getting It Admitted.

In order to make effective use of electronic evidence, the information must be admissible under the applicable rules of evidence governing the proceeding. In addition to knowledge of the relevant case law, preparation before trial for admission and exclusion of the evidence can minimize obstacles to admissibility.

1. General Standards.

In *Burleson v. State*,[82] a former employee convicted of deleting certain payroll data from his computer terminal after his termination argued that the trial court erred by admitting into evidence electronic documents printed from the computer.[83] The Fort Worth Court of Appeals rejected the claim and held that computer generated documents are discoverable and admissible as tangible evidence.[84] The court explained that electronic evidence is admissible if the court, based on the preponderance of the evidence presented, determines that the technology behind the evidence is trustworthy.[85]

Similarly, in *United States v. Sanders*,[86] a defendant appealed his Medicaid fraud conviction, claiming the trial court erred in admitting computer printouts of medical claims paid by the Texas Department of Human Resources.[87] The Fifth Circuit held that the elements for admissibility of computer records are that the data was prepared pursuant to

---

77 *Zakre v. Norddentsche Landesbank Girozentrale*, 2004 WL 764895, at *1 (S.D.N.Y. Apr. 9, 2004).

78 *Id*. (citing The Sedona Conference: Best Practices, Recommendations & Principles for Addressing Document Discovery (2004)).

79 Payne Consulting Group, *Hidden Bounty*, ABA Journal, July 2004 at 27.

80 *See* Grace V. Bacon, *The Fundamentals of Electronic Discovery*, 47 B. BAR J. 18, 19-20 (2003).

81 *See, e.g.*, In Re Ford Motor Company, 345 F.3d 1315 (11th Cir. 2003); Scotts Co., LLC v. Liberty Mutual Insurance Co., 2007 WL 1723509 (S.D. Ohio June 12, 2007); Calyon v. Mizuho Securities USA, Inc., 2007 U.S. Dist. LEXIS 36961 (S.D.N.Y. May 18, 2007); Orrell v. Motorcarparts of America, Inc., 2007 U.S. Dist. LEXIS 89524 (W.D.N.C. Dec. 4, 2007).

82 802 S.W.2d 429, 433-35 (Tex. App.—Fort Worth 1991, writ ref'd).

83 *See id.*

84 *Id.* at 436.

85 *Id.* at 441.

86 749 F.2d 195, 196 (5th Cir. 1984).

87 *Id.*

routine procedures and the procedures were designed to assure accuracy of the records.[88] Because the elements were satisfied, the court affirmed the trial court's decision in admitting the evidence.[89]

As with most evidentiary issues, a threshold question involves the reliability of the electronic evidence.[90] Natural corollaries to authentication include the hearsay rule and its exceptions, chain of custody, and the best evidence rule, which present admissibility issues of electronic information.

2. Authentication

Electronic information raises unique issues concerning accuracy and authenticity.[91] Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling.

Authentication of electronic documents may present a challenge to the unprepared practitioner. For example, courts have found electronic documents discovered over the Internet to be incapable of authentication.[92] In 1999, in electronic discovery antiquity, the court attacked the credibility of information obtained from the internet declaring that "the Court continues to warily and wearily view [the internet] largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, . . . this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon . . . ."[93]

Authentication of electronic records involves demonstrating the accuracy of the process or system responsible for generating or maintaining the information. "Authentication 'is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.'"[94] The Fifth Circuit, in *Capital Marine Supply, Inc. v. M/V Roland Thomas II*,[95] considered a contention that the trial court erred by allowing the balance due on a loan to be proven through computer records.[96] In affirming the trial court's decision to allow the evidence, the court stated that proper authentication required sufficient proof presented at trial to show the accuracy of the records based on routine procedure.[97] Additionally, litigants can satisfy the authenticity requirement by demonstrating that an individual with knowledge of the events recorded maintained a computer record in the ordinary course of business.[98]

In state court, Texas Rule of Civil Procedure 193.7 establishes a presumption of authenticity for documents produced in the course of discovery under certain circumstances.[99] The Rule provides:

> A party's production of a document in response to written discovery authenticates the document for use against that party in any pretrial proceeding or at trial unless—within **ten days or a longer or shorter time ordered by the court**, after the producing party has actual notice that the documents will be used—the party objects to the authenticity of the document, or any part of it, stating the specific basis for the objection.[100]

While the authenticity presumption simplifies the process for the party seeking to admit the evidence, the Rule can be a huge burden for opposing parties. Specifically, the quantity of electronic evidence that may be produced, the ability to modify the evidence, and the ability to create falsified evidence all require the opposing party to search the results of electronic discovery diligently to determine whether any objections should be made within the ten-day window. A practical approach to this dilemma might be to enter into an agreement with opposing counsel regarding how to identify the documents he or she intends to use with sufficient time for the non-introducing party to

---

88 *Id.* at 198-99.

89 *Id.*

90 *See* Manual for Complex Litigation Fourth, Federal Judicial Center 2004, at §11.446; s*ee also* Gregory P. Joseph, *A Simplified Approach to Computer-Generated Evidence and Animations*, 43 N.Y.L. SCH. L. REV. 875 (1999–2000).

91 Manual for Complex Litigation Fourth, Federal Judicial Center 2004, *at* §11.446.

92 *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 774 (S.D. Tex. 1999).

93 *Id.*

94 *Fenje v. Feld*, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003) (quoting FED. R. EVID. 901(a)).

95 719 F.2d 104, 105 (5th Cir. 1983).

96 *Id.*

97 *Id.* at 106.

98 *Longoria v. Greyhound Lines, Inc.*, 699 S.W.2d 298, 301 (Tex. App.—San Antonio 1985, no writ).

99 TEX. R. CIV. P. 193.7.

100 *Id.* (emphasis added).

review, object, and obtain a ruling from the court, before the evidence is presented.

Last but certainly not least, authentication issues abound with perhaps the most commonly used form of electronic documentation used in society—e-mail. Today, the ease at which an email can be forwarded and its content manipulated is staggering, which makes authentication concerns all the more prevalent. In *Fenje*, a medical resident claimed that a state university medical school improperly terminated him from its anesthesiology residency program.[101] The federal district court considered the authentication of e-mail communication for purposes of Defendant's summary judgment motion.[102] The court noted that "[e]-mail communications may be authenticated as being from the purported author based on an affidavit of the recipient; the e-mail address from which it originated; comparison of the content to other evidence; and/or statements or other communications from the purported author acknowledging the e-mail communication that is being authenticated."[103]

3. Hearsay

Texas Rule of Evidence 801 defines hearsay as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."[104] Electronic information, like other written documents, may be hearsay and is inadmissible without applying a recognized exception to the hearsay rule.

Some courts have determined that e-mail messages constitute inadmissible hearsay. For example, in *Taffe*, an employee with a history of misconduct sued her employer for retaliatory discharge.[105] Relying on the hearsay rule, the court struck portions of Defendant's affidavit that contained an e-mail from another employee who reported that he had found computer games on the discharged employee's computer.[106] On the other hand, emails are not always hearsay. A Vermont federal district court held that intra-company emails offered in support of an affidavit were admissible as an admission of a party.[107] The court noted that the content of the e-mails pertained to potential expert testimony from a party but did not implicate the Federal Rules of Evidence concerning admitting expert testimony because the Federal Rules do not prevent a party from testifying as an expert.[108] Presumably, the court also found that that the e-mails were not offered for the truth of the matter asserted, hence not hearsay.[109]

Parties often employ the business records exception to the hearsay rule as a means to introduce electronic evidence during trial.[110] Nearly all jurisdictions recognize this exception to the traditional hearsay rule for records maintained and relied upon in the regular course of business, on the belief that it would not be practical to require every employee of a business to testify in order to establish the matters through personal and direct testimony.[111] However, not every use of the exception has been successful. In an ill-fated attempt to employ the business records exception to the hearsay rule, a criminal defendant claimed that postings on a white supremacist web-site constituted the business records of the internet service providers.[112] The court rejected this argument and noted that because the Internet service providers neither posted what was on the website nor monitored the contents of the web sites, the "Internet service

---

[101] *Fenje*, 301 F. Supp. 2d at 787; *see also Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153 (C.D. Cal. 2002) (discussing authentication of exhibits printed off of the internet). In *Cybernet*, the court held that a declaration submitted in support of the exhibits satisfied the foundational requirement of Federal Rule 901(a) because it would support a finding that the exhibit in question is what its proponent claims. *See id.*

[102] *Fenje*, 301 F. Supp. 2d at 787; *see also Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153 (C.D. Cal. 2002) (discussing authentication of exhibits printed off of the internet). In *Cybernet*, the court held that a declaration submitted in support of the exhibits satisfied the foundational requirement of Federal Rule 901(a) because it would support a finding that the exhibit in question is what its proponent claims. *See id.*

[103] *Id.*

[104] TEX. R. EVID. 801.

[105] *Taffe v. Ill. Dep't of Employment Sec.*, 229 F. Supp. 2d 858, 861, 865 (N.D. Ill. 2002). Further, in *New York v. Microsoft Corp.*, the court determined that several exhibits containing e-mail messages were offered to prove the truth of the matter asserted therein and thus hearsay. CIV. A. 98-1233 (CKK), 2002 WL 649951, at *6 (D.D.C. Apr. 12, 2002).

[106] *Taffe*, 229 F. Supp. 2d at 865.

[107] *Vermont Elec. Power Co. v. Hartford Steam Boiler Inspection & Ins. Co.*, 72 F. Supp. 2d 441, 449 (D. Vt. 1999).

[108] *See id.*

[109] *See id.*

[110] *See* FED. R. EVID. 803(6).

[111] *See, e.g.*, *United States v. DeGeorgia*, 420 F.2d 889, 893 (9th Cir. 1969) (holding that regularly-maintained records upon which a company relies in conducting business assures accuracy not likely to be enhanced by introducing into evidence the original documents upon which the records are based).

[112] *See United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000).

providers, however, are merely conduits."[113] "The fact that the Internet service providers may be able to retrieve information that its customers posted or email that its customers sent does not turn that material into a business record of the Internet service provider."[114]

A valuable resource for introducing large amounts of electronically generated information is the business record affidavit rule contained in Texas Rule of Evidence 902(10).[115] This rule is effective in facilitating the production of accounting and other detailed records that should not require actual witnesses to prove up the documents at trial. The rule requires the filing of an affidavit at least fourteen days before trial stating the information necessary to establish the documents as business records under Rule of Evidence 803(6) or (7).[116] This procedure has been utilized notwithstanding objections that the affidavits contain hearsay.[117] Complying with this procedure allows a witness testifying at trial to provide a summary of the data contained within the larger volume of information.

4. Chain of Custody

Issues related to chain of custody also raise some special concerns at trial for the introduction of electronic information. Parties should be prepared to argue chain of custody issues at trial, both offensively and defensively, as they are likely to come up regarding electronic information.

In *Kupper v. State*,[118] the defendant, who was convicted of aggravated sexual assault, claimed that evidence found on his home computer was inadmissible because the state could not prove chain of custody.[119] The court rejected Defendant's allegation that there was no proof that the images came from a computer he actually used.[120] Further, Kupper argued that some of the evidence was obtained from deleted files, which evinces that the hard drive was tampered or altered with by the prosecution.[121] The court rejected this argument as well, and pointed out that "[i]mportantly, Kupper offers no evidence of any alteration or deletion in the documents themselves or points to any evidence on the documents themselves of alteration or deletion."[122]

5. Best Evidence Rule

The Best Evidence Rule provides that "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required . . . ."[123] Electronic evidence is considered a "document" under the Federal Rules of Evidence.[124] The Federal Rules of Evidence address the concern that electronic information may not constitute an original as required by the best evidence rule. The Federal Rules of Evidence provide, for instance, that "[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."[125]

Courts have considered whether an image copy constitutes the best evidence. For instance, the United States Court of Appeals for the Eighth Circuit concluded that an instruction to the jury to disregard testimony by Defendant's probation officer briefly describing "one image of child pornography found on a computer disk in [Defendant's] apartment," because it violated the best evidence rule, was proper.[126] Further, in *Broderick v. State*,[127] a Texas appellate court held

---

[113] *Id.* Ultimately, the court affirmed the exclusion of the evidence because it lacked authentication. *Id.*

[114] *Id.*

[115] TEX. R. EVID. 902(10).

[116] *Id.*

[117] *See Fullick v. Baytown*, 944 (Tex. App.—Houston [1st Dist.] 1991, no writ).

[118] No. 05-03-00486-CR, 2004 WL 60768, at *1 (Tex. App.—Dallas Jan. 14, 2004, pet. denied).

[119] *Id.* at 2.

[120] *Id.* at 3.

[121] *Id.*

[122] *Id.*

[123] FED. R. EVID. 1002; *see also* FED. R. EVID. 1004.

> The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if—
>
> (1) Originals lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or (2) Original not obtainable. No original can be obtained by any available judicial process or procedure; or (3) Original in possession of opponent. At a time when an original was under the control of the party against whom offered, that party was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and that party does not produce the original at the hearing; or (4) Collateral matters. The writing, recording, or photograph is not closely related to a controlling issue.

Federal Rule of Evidence 1004 provides the exceptions to the best evidence rule. *Id.*

[124] *See* FED. R. EVID. 1001; *see also Encase Legal Journal*, p. 44 Guidance Software, Inc. 2001-2006 (citing FED. R. EVID. 1001).

[125] FED. R. EVID. 1001(3).

[126] *United States v. Crume*, 422 F.3d 728, 730 (8th Cir. 2005).

[127] *Broderick v. State*, 35 S.W.3d 67, 79 (Tex. App.—Texarkana 2000, pet. denied).

that the prosecution could "introduce a duplicate of the hard drive on [Defendant's] computer rather than producing the original . . ." for purposes of satisfying Texas's equivalent to the best evidence rule.[128]

6. Expert Witnesses.[129]

Although trained computer forensic experts have qualified as experts under Federal Rule of Evidence 702 or analogous state rules, litigants frequently opt not to offer the examiner as an expert. This is especially true where the records in question can be authenticated under Federal Rule of Evidence 901(b)(9) or a corresponding state statute, or where the examiner can be offered as a percipient witness presenting more objective and empirical findings of their investigation. In *Furmanite American, Inc. v. T.D. Williamson, Inc.*,[130] the party seeking to introduce the testimony of its retained computer forensics consultant failed to timely designate the witness for trial as an expert, but timely disclosed the consultant as a fact witness for the scheduled trial. The court's decision establishes that a computer forensics professional who performs basic copying, imaging, searching, collection, and production of data arguably is not necessarily performing such duties as an expert witness, and thus can present their results as a fact witness. However, if the computer forensics expert needs to conduct detailed analysis of their recovered data or interpretation of reports and other analytics, then the witness would likely be offering expert testimony.

X. EDUCATING CLIENTS.

If nothing else, the material above should indicate that electronic discovery can be a useful tool against unwary opponents in the litigation process. In order to maximize client security and achieve the most consistent results as lawyers, however, steps must be taken even before any impending litigation arises. For example, an effective document preservation program will decrease client exposure to broad and potentially damaging electronic discovery requests. Furthermore, the advice of experts can be invaluable in this stage, as well as absolutely necessary at times once litigation begins. Finally, underlying all of these considerations is the reality that the costs of electronic discovery can be substantial.

A. Document Preservation Programs.

As suggested above, the existence of an effective and reasonable document preservation program serves as an active and early step in preparing for and responding to broad electronic discovery demands. The guidelines of a program should include consideration of the business, regulatory, and tax needs of the organization, including the need to maximize electronic storage space on the entity's server. Thus, a company could establish a document retention policy with guidelines that retain only e-mails with business record significance to avoid the dangers of disclosing sometimes damaging information that might be contained in personal communications. Of course, any system should include provisions for "litigation holds" to prevent destruction of documents related to ongoing or anticipated litigation. The presence and routine compliance with such a system, however, should be a considerable factor in any spoliation analysis.

The Sedona Conference's "Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age" provides commentary and illustrations to assist organizations in implementing sound and justifiable protocols for managing electronic data. Currently, there are several vendors and e-discovery experts who have outlined the creation of the document retention program which will reduce the potential for intentional and unintentional spoliation and make it easier to comply with future litigation requirements.

The importance of routine compliance with any document preservation program cannot be overstated. Failure to implement and monitor document retention programs effectively can result in severe consequences even in the absence of intentional wrongdoing. For example, in *In re Prudential Sales Practices Litigation*, the court imposed a one million dollar sanction on Prudential after finding management had implemented a "haphazard and uncoordinated" policy of notifying employees about their responsibilities of preserving electronic documents.[131]

A few years ago, one court ordered defendants to pay costs relating to the spoliation as well as $2.75 million in monetary sanctions for destroying relevant e-mails.[132] The government had filed a motion for evidentiary and monetary sanctions against the defendants for spoliation of evidence. Although the court had ordered preservation of all potentially relevant documents, the defendants continued to delete e-mail when it became 60 days old, on a monthly system-wide basis for a period of two years after the

---

[128] *Id.*

[129] This portion of the paper is adapted from *Threshold Under Rule 702*, EnCase Legal Journal, January 2008, at 18.

[130] 506 F. Supp. 2d 1126 (M.D. Fla., 2007).

[131] *In re Prudential Sales Practices Litigation*,169 F.R.D. 598, 615 (D.N.J. 1997).

[132] *United States v. Phillip Morris USA Inc.*, 327 F.Supp.2d 21, 26 (D.D.C. July 21, 2004).

court order. Even after learning about their inadequate document retention policy, the defendants continued to destroy documents for several months, including relevant e-mails from at least 11 company supervisors and officers. In addition, the defendants failed to notify the court about the situation until four months after they found out about it. Finding that a significant number of e-mails had been permanently destroyed, the court declared that "it is astounding that employees at the highest corporate level in Philip Morris, with significant responsibilities pertaining to issues in this lawsuit, failed to follow [the] Order . . . which, if followed, would have ensured the preservation of those e-mails which have been irretrievably lost."[133] Granting the government's motion for sanctions, the court stated that it will preclude the defendants from calling a key employee, who failed to follow the retention policy, as a fact or expert witness at trial.[134]

In addition to sanctions, noncompliance could result in discovery of information that falls outside the parameters of the document preservation system. Although document preservation programs should serve to protect an entity and narrow the scope of discovery requests, a skillful adversary will likely request copies of the opponent's policy in order to seek information regarding the level of internal compliance. If policies have not been disseminated throughout the organization or if a client has been lax in enforcing the policies, potentially harmful information may unexpectedly be within the scope of discovery. However, the best program cannot help the situation unless it is fully implemented and there is "buy in" at all levels of the company. Otherwise, the program will hurt more than it will help.

1. Handling Electronic Data Responsibly.

Once a lawsuit is filed, attorneys should instantly direct the client to suspend those document retention policies to prevent discarding relevant data. Then, attorneys should instruct the client to notify its employees to refrain from deleting e-mails or other computer documents. Further, the client should request the IT staff to remove backup tapes from rotation and suspend automatic purges of servers, especially e-mail servers. When the client worries about data on particular computers or servers, attorneys should instruct the client to remove the hardware from operation. Programs containing discoverable electronic data should not be executed. Specifically, programs affecting the operating system should not be used.

One significant pitfall is allowing employees to continue to use the original hard drive, server, or backup tapes. To avoid tarnishing the original, a mirror image of these materials should always be created for use and the original kept in an evidence safe. Thus, using mirror images instead of originals, can decrease the risk of tainting the evidence.

As discussed above, do not assume that only utilizing the client's IT staff to collect data is enough. Although the IT staff is probably knowledgeable about the computer equipment, networks, and firewalls, an outside expert can assist with issues where IT staff is inhibited. The client's IT staff already has full-time jobs and may not have time to collect electronic data. Conflicts of interest and independence issues abound. Also, IT staff generally does not have experience with forensics software, of which, hundreds exist for different purposes, uses, and effectiveness. Perhaps most critical, the IT staff will not have deposition or court experience to defend their work, as experts routinely do.

2. Beware of Spoliation.

Several issues arise when considering the duty to preserve evidence. This is of critical importance in today's litigation environment.[135] Generally, no duty arises before the litigation is filed, threatened, or reasonably foreseeable unless that duty is voluntarily assumed or it is imposed through other means. The duty to preserve documents or tangible evidence in a given instance can arise from the existence of pending, threatened, or reasonably foreseeable litigation. This duty also can arise from a number of other sources, including a contract, a voluntarily assumed duty, a statute or regulation, or an ethical code.[136] Texas courts may punish the spoliators of evidence with any of the sanctions available under Texas Rule of Civil Procedure 215, including the exclusion of the evidence, the striking of pleadings, and the payment of fees and costs associated with remedying the conduct.

One of the most important aspects of the *Ortega* decision is Justice Baker's concurrence addressing the existing remedies for spoliation.[137] Justice Baker examined the duty to preserve evidence, breach of that duty and prejudice to the spoliation victim's ability to present a case. First, Justice Baker noted that parties may have a statutory, regulatory or ethical duty to

---

[133] *Id.*

[134] *Id.*; *see also 3M Innovative Props Co. v. Tomar Elecs.*, 2006 WL 2670038 (D. Minn. Sept. 18, 2006) (ordering adverse inference instruction against Defendant for failure to retain, collect and produce court-ordered documents).

[135] Judge Scheindlin has written a comprehensive article on sanctions in e-discovery cases. Shira A. Scheindlin and Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 MICH. TELECOMM. TECH. L. REV. 71 (2004).

[136] *Trevino v. Ortega*, 969 S.W.2d 950, 955 (Tex. 1998) (Baker, J., concurring).

[137] *Id.* at 954.

preserve evidence.[138] Justice Baker opined that a duty to preserve arises before litigation begins, when a party is "on notice" of litigation.[139] Justice Baker noted that under *National Tank Co. v. Brotherton*, a party is on notice of potential litigation when, after viewing the totality of circumstances, the party either actually anticipated litigation, or a reasonable person in the party's position would have anticipated litigation.[140]

With respect to the scope of the duty to preserve evidence once the duty arises, Justice Baker concluded the only evidence a party must preserve is that which is relevant to the litigation.[141] Justice Baker also maintained that parties should be responsible for both negligent and intentional spoliation.

Any discussion of the penalties for spoliation would be incomplete without considering the potential application of criminal statutes. Generally, the Texas Penal Code does not provide relief for spoliation, but it does provide that a person tampers with physical evidence if that person alters, destroys, or conceals any record or document, knowing of the existence of an official proceeding related to that record or document.[142] This provision has yet to be applied in a civil case, and even if it were, no mechanism exists under this provision to compensate the spoliation "victim."

3. Establish a Protocol Early.

Although electronic data discovery may not sound difficult, the burden on attorneys and their clients may be tremendous depending on the size and the scope of the data. For example, terabytes of data can extend over thousands of miles, and still only include computers and servers currently used. Company organizational charts are effective means for assembling the various sources of electronic data.[143] A chart diagramming each section of the company from the most senior employees to the more junior level employees assists attorneys in tracking which employees housed what data.

By documenting the client's collection efforts, attorneys can ensure that adequate information is collected to shore up the chain of evidence and custody, and, hopefully, avoid problems. Such documentation may include detailing the following information: the origin of the computer evidence, what computer the data is from, what hard drive, the location of the computer, who the computer belonged to, who was authorized to use the computer, and how the drive was imaged. Continuously documenting the electronic data collection efforts helps assist in collecting less non-relevant data and ensures that data, which should be collected, is not overlooked.

4. Implement and Distribute Litigation Holds As Soon As Possible.

Once counsel has identified any regular or automatic deletion or alteration operations affecting its data, users must understand the need to preserve data and work closely with IT personnel. This can be chiefly (but not solely) communicated to all users, and it may ultimately be important to document how this information is sent to the users. In addition, the following issues may also be important:

- Copy the relevant data files as of the date on which litigation is anticipated.[144] This can be difficult and costly depending on the volume of the data, but it may be possible to avoid copying an entire database. It will be important to document these efforts contemporaneously in case the party has to explain its actions later. It may also be necessary to make copies at regular intervals.
- Save backup tapes and extend relevant retention periods as necessary. As with copies, this may be cost prohibitive depending on the volume of the data. This point cannot be overemphasized: retrieving data from backup media often is more expensive and difficult than doing so from live data.
- Consider a text-based "snapshot" of each database or body of data. Text format can be more convenient for production because of its readability, but it also can lose some of the characteristics, functionality, and even content of the data, which may lead to preservation or production problems later. As stated before, negotiate this point with the other side early – before incurring the production costs.
- For databases, understand the reports from the database. To preserve only the electronic data and not any reports (electronic or hardcopy) might be a mistake because those reports are not always

---

138 *Id.* at 955.

139 *Id.* at 955-56.

140 *Id.* at 956 (citing *National Tank Co. v. Brotherton*, 851 S.W.2d 193, 204-07 (Tex. 1993)).

141 *Ortega*, 969 S.W.2d at 957.

142 TEX. PENAL CODE ANN. § 37.09 (Vernon 2003).

143 The American Bar Association Section of Antitrust Law and Center for Continuing Legal Education, *Following the E-Paper Trial: Electronic Document Production Issues in the Digital Age,* (March 12, 2004).

144 This is a particularly important point because the date on which litigation is anticipated is the date that attorney-work product protection begins *and* the date when data must be preserved. If a party seeks protection under the attorney-work doctrine but has not been preserving documents as of that date, it is asking for trouble.

duplicative of the database's data. What's the difference? Each report provides a snapshot of the data at the time the report was created, and data may change or be lost at any time. Conversely, it is equally dangerous to rely only on reports for preservation or production, unless those reports reflect all relevant data and those reports are saved often enough to capture any material changes or deletions.

5. Negotiate Production Issues with Opposing Counsel Early.

Agreements with opposing counsel are necessary so that opposing counsel cannot exploit the discovery process. Before production begins, both sides should agree on production protocol and the anticipated time table. As part of this, an agreement should be executed implementing a method to search the data using certain key words, including a list of actual search terms. Key word searching, such as OCR searches, is a reasonable approach when dealing with enormous amounts of electronic data. By implementing a sampling technique, attorneys can prove to the opposing side the accuracy of key word searches. Be sure to be generous with your timetables; there will always be issues.

Second, attorneys should negotiate the terms and anticipated schedule for a rolling production. A rolling production affords the requesting party the benefit of receiving documents sooner than it would otherwise. In turn, a rolling production allows the responding party extra time to review the voluminous information, before it must produce it. Further, attorneys should negotiate the format of the electronic data to be produced.

Similarly, attorneys should discuss the protocol for inadvertent disclosure of privileged electronic documents. Attorneys should agree to procedures that become effective when a privilege document is inadvertently produced to prevent the need to repeatedly write letters to opposing counsel. If an ISP is hosting the documents for the lawsuit, then have a designated employee of the ISP remove the privileged document from the produced folders and place it in a designated folder. The ISP can notify the opposing side of the removed document. If the opposing side has advance notice of these procedures, then attorneys can possibly prevent the accidental viewing of the privileged document.

6. Costs and Sanctions.

Electronic discovery can result in substantial costs to the parties involved in complex cases. These costs can increase significantly considering that special equipment or experts may be required to translate data from outdated formats and equipment into usable form. The breadth of discoverable information and the ability to efficiently review huge numbers of electronic documents has increasingly shifted the costs of discovery to the responsive parties because it is the responding party that must generally provide the data through an electronic medium. Although some courts continue to take the traditional approach, that companies using electronic documentation assume the risk of the discovery costs, some courts have moved away from this notion because of the prevalence of electronic business applications in recent years.

The leading cases on the cost issue are the *Zubulake* decisions, which provide a framework for dealing with electronic discovery. In *Zubulake I*, the court warned that the prevailing cost-shifting analysis from *Rowe* might favor large corporations when engaged in litigation with private parties, a result which could "undermine the 'strong public policy favor[ing] resolving disputes on their merits,' and may ultimately deter the filing of potentially meritorious claims." [145] *Zubulake I* delineated a set of factors to determine whether costs should be shifted. Those factors included:

a. The extent to which the request is specifically tailored to discover relevant information;
b. The availability of such information from other sources;
c. The total cost of production, compared to the amount in controversy;
d. The total cost of production, compared to the resources available to each party;
e. The relative ability of each party to control costs and its incentive to do so;
f. The importance of the issues at stake in the litigation; and
g. The relative benefits to the parties of obtaining the information.[146]

The *Zubulake III* court examined these factors and ordered the responding party to endure seventy-five percent and the requesting party twenty-five percent of the total estimated cost for restoring and searching the defendant's e-mail backup tapes throughout discovery.[147]

In *Zubulake I*, the court opined that the first two factors, known collectively as the marginal utility test, are the most significant.[148] The marginal utility test,

---

[145] *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 321 (S.D.N.Y. 2003) ("Zubulake I").

[146] *Id.*

[147] *Zubulake v. UBS Warburg L.L.C.,* 216 F.R.D. 280 (S.D.N.Y. 2003) ("Zubulake III").

[148] *Id.* at 323.

initially announced in *McPeek v. Ashcroft*,[149] embodies the theory that the more likely it is the source of data contains information relevant to a claim or a defense, then the fairer it is for the responding party to search at its own expense.[150] The court should then consider factors three, four, and five to determine the relative ability of each party to bear the burden of the expenses.[151] The court held that factor six could be evaluated independent of the other factors if it is relevant to the facts of the particular case.[152] Finally, factor seven weighs the least in the court's cost-shifting analysis because discovery responses commonly benefit the requesting party.[153] Nevertheless, when the production also affords a substantial or strategic benefit to the responding party, the seventh factor becomes pertinent. After weighing all factors, the *Zubulake I* court permitted cost-shifting because of the possibility of more significant information. Given the speculative nature of the additional discovery, Judge Scheindlin opined that the plaintiff should pay some part of the cost.[154] This case highlights the need for litigants to seriously consider the steps to take when faced with electronic discovery.

The *Zubulake* court ultimately sanctioned the defendants for destruction of e-mail evidence.[155] In this latest motion, the employee contended that the employer, who recovered some of the deleted relevant e-mails, prejudiced her case by producing recovered e-mails long after the initial document requests. Furthermore, some of the e-mails were never produced, including an e-mail that pertained to a relevant conversation about the employee. As such, the employee requested sanctions in the form of an adverse inference jury instruction. Determining that the employer had willfully deleted relevant e-mails despite contrary court orders, the court granted the motion for sanctions and also ordered the employer to pay costs. The Court further noted the defense counsel was partly to blame for the document destruction because it had failed in its duty to locate, preserve and timely produce the relevant information. In addressing the role of counsel in litigation generally, the court stated that "[c]ounsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched."[156] The Court concluded that attorneys are obligated to ensure all relevant documents are discovered, retained, and produced. Additionally, the Court declared that litigators **must** guarantee that identified relevant documents are preserved by placing a "litigation hold" on the documents, communicating the need to preserve them, and arranging for safeguarding of relevant archival media.[157]

In Texas, Rule of Civil Procedure 196.4 addresses cost-shifting. A responding party is required to produce information "reasonably available . . . in its ordinary course of business" and may object to unreasonable discovery requests outside of this scope.[158] If, after the objection, a court orders further production from the party, the reasonable costs shift to the requesting party for "extraordinary steps" necessary to retrieve and produce information.[159] Although there is little or no Texas case law regarding what constitutes extraordinary steps, this represents an area of law likely to develop significantly in the future.[160]

Now that courts and, in the case of Texas, rules are sanctioning cost-shifting, the next question is how common is it? A review of thirty-one recent cases on cost-shifting decided between 1987 and 2004 shows that a total of fourteen courts were willing to shift some costs to the plaintiff. Generally, these cases involved either the recovery of "inaccessible" data or the creation of some new data. Of the cases that shifted cost, the majority did not shift the cost of producing or reviewing the electronic information—only the cost of recovery, extraction, or creation was shifted. Since *Rowe*, only one published decision has shifted 100% of the costs to the requesting party. Moreover, of all thirty-one cases reviewed only five shifted more than 50% of the costs to the requesting party.[161]

---

[149] *McPeek v. Ashcroft,* 202 F.R.D. 31 (D.D.C. 2001).

[150] *Id.*

[151] *Zubulake I*, 217 F.R.D. at 323.

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *Zubulake v. UBS Warburg*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) ("*Zubulake V*").

[156] *Id.*

[157] *Id.*

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

[159] *Id.*

[160] *See In re Lowe's Cos., Inc.*, 134 S.W.3d 876, 880 (Tex. App.—Houston [14th Dist.] 2004, orig. proceeding).

[161] This portion of the paper is adapted from Scott Fletcher, *Cost-Shifting: Is It Worth the Effort?* 2005, at 1 (on file with author).

XI. E-DISCOVERY IN UNITED STATES FEDERAL AGENCIES.[162]

Recent cases have made it clear that federal agencies will be held to at least an equal if not higher standard on e-discovery compliance than private litigants. In *United Medical Supply Company v. United States*,[163] the court noted that "[i]t is the duty of the United States, no less than any other party before this court, to ensure, through its agents, that documents relevant to a case are preserved. Indeed, . . . as the enforcer of the laws, the United States should take this duty more seriously than any other litigant. . . . [T]he court concludes that it must impose spoliation sanctions against the United States. . . . Aside perhaps from perjury, no act serves to threaten the integrity of the judicial process more than the spoliation of evidence . . . . To guard against this, each party in litigation is solemnly bound to preserve potentially relevant evidence." The court further described the government's document retention and preservation policies as "antiquated and inadequate," and then awarded attorneys' fees and expenses to the other side.

The court in *Miller v. Holzmann*[164] noted that the obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. "However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data."[165] This case illustrates a growing trend where FOIA non-compliance will often evolve into district court actions, with the new FRCP e-discovery amendments used to enforce the original requests. As the court indicated, "[l]awyers employed by the Department of Justice, and particularly the competent and experienced ones assigned to this case, knew or should have known that a response to a FOIA request by an agency may lead to exactly what happened here, the retention and non-disclosure by the agency of information that may nevertheless be discoverable in a case then being litigated by that Department."[166] Importantly, the court cited the Sedona Conference as support.[167]

XII. CONCLUSION.

Although e-mail and electronic documents may not constitute a part of all litigation matters today, the ever-increasing use of technology in the workplace signals that electronic discovery is a facet of litigation that is here to stay. With changes in technology and the lack of understanding how the technology works, pitfalls (and opportunities) abound for the litigator. Understanding these issues can lead to a better result for clients and—equally important—compliance with appropriate professional obligations. The information contained in this paper represents only the beginning of the process of learning about electronic discovery; but with this information, any lawyer can establish a firm foundation in order to build a more complete understanding of the topic. Such an understanding will assist not only your clients but an entire law firm as well.

---

[162] This portion of the paper is adapted from *eDiscovery in United States Federal Agencies*, EnCase Legal Journal, January 2008, at 124.

[163] 2007 WL 1952680 (Fed. Cl. June 27, 2007).

[164] 2007 WL 172327 (D.D.C. Jan. 17, 2007)(Facciola, J.)

[165] *Id.*

[166] *Id.*

[167] *Id.*

APPENDIX A[168]

SAMPLE PRESERVATION LETTER - TO CLIENT

June 19, 2008

RE: [Case Name] - Data Preservation

Dear _____:

Please be advised that the Office of General Counsel requires your assistance with respect to preserving corporate information in the above-referenced matter. Electronically stored data is an important and irreplaceable source of discovery and / or evidence in this matter. The lawsuit requires preservation of all information from [Corporation's] computer systems, removable electronic media and other locations relating to [description of event, transaction, business unit, product, etc.].

This includes, but is not limited to, e-mail and other electronic communication, word processing documents, spreadsheets, databases, calendars, telephone logs, contact manager information, Internet usage files, and network access information. Employees must take every reasonable step to preserve this information until further notice from the Office of General Counsel. Failure to do so could result in extreme penalties against [Corporation].

If this correspondence is in any respect unclear, please contact [designated coordinator] at [phone number].

Sincerely,

_____

[168] Excerpted from Jason M. Paroff et al., *Electronic Discovery in Technology Litigation*, *in* COMPUTER LAW 2003, at 345-46 (PLI Patents, Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. G0-018L, 2003).

APPENDIX B[169]

SAMPLE INTERROGATORIES

UNITED STATES DISTRICT COURT DISTRICT OF [jurisdiction]

Court File No.:
_____, Plaintiff,
v.
_____, Defendant.

INTERROGATORIES TO [party name]

- Identify all e-mail systems in use, including but not limited to the following:
  - List all e-mail software and versions presently and previously used by you and the dates of use;
  - Identify all hardware that has been used or is currently in use as a server for the e-mail system including its name;
  - Identify the specific type of hardware that was used as terminals into the e-mail system (including home PCs, laptops, desktops, cell phones, personal digital assistants ["PDAs"], etc.) and its current location;
  - State how many users there have been on each e-mail system (delineate between past and current users);
  - State whether the e-mail is encrypted in any way and list passwords for all users;
  - Identify all users known to you who have generated e-mail related to the subject matter of this litigation;
  - Identify all e-mail known to you (including creation date, recipient(s) and sender) that relate to, reference or are relevant to the subject matter of this litigation.
- Identify and describe each computer that has been, or is currently, in use by you or your employees (including desktop computers, PDAs, portable, laptop and notebook computers, cell phones, etc.), including but not limited to the following:
  - Computer type, brand and model number;
  - Computers that have been re-formatted, had the operating system reinstalled or been overwritten and identify the date of each event;
  - The current location of each computer identified in your response to this interrogatory;
  - The brand and version of all software, including operating system, private and custom-developed applications, commercial applications and shareware for each computer identified;

[169] Excerpted from *id*. at 347-55.

- The communications and connectivity for each computer, including but not limited to terminal-to-mainframe emulation, data download and/or upload capability to mainframe, and computer-to-computer connections via network, modem and/or direct connection;

- All computers that have been used to store, receive or generate data related to the subject matter of this litigation.

o As to each computer network, identify the following:

- Brand and version number of the network operating system currently or previously in use (include dates of all upgrades);

- Quantity and configuration of all network servers and workstations;

- Person(s) (past and present including dates) responsible for the ongoing operations, maintenance, expansion, archiving and upkeep of the network;

- Brand name and version number of all applications and other software residing on each network in use, including but not limited to electronic mail and applications.

o Describe in detail all inter-connectivity between the computer system at [opposing party] in [office location] and the computer system at [opposing party # 2] in [office location # 2] including a description of the following:

- All possible ways in which electronic data is shared between locations;

- The method of transmission;

- The type(s) of data transferred;

- The names of all individuals possessing the capability for such transfer, including list and names of authorized outside users of [opposing party's] electronic mail system.

- The individual responsible for supervising inter-connectivity.

o As to data backups performed on all computer systems currently or previously in use, identify the following:

- All procedures and devices used to back up the software and the data, including but not limited to name(s) of backup software used, the frequency of the backup process, and type of tape backup drives, including name and version number, type of media (i.e. DLT, 4mm, 8mm, AIT). State the capacity (bytes) and total amount of information (gigabytes) stored on each tape;

- Describe the tape or backup rotation and explain how backup data is maintained and state whether the backups are full or incremental (attach a copy of all rotation schedules);

- State whether backup storage media is kept off-site or on-site. Include the location of such backup and a description of the process for archiving and retrieving on-site media;

- The individual(s) who conducts the backup and the individual who supervises this process;

- Provide a detailed list of all backup sets, regardless of the magnetic media on which they reside, showing current location, custodian, date of backup, a description of backup content and a full inventory of all archives.

- Identify all extra-routine backups applicable for any servers identified in response to these interrogatories, such as quarterly archival backup, yearly backup, etc. and identify the current location of any such backups.

- For any server, workstation, laptop, or home PC that has been "wiped clean" or reformatted such that you claim that the information on the hard drive is permanently destroyed, identify the following:

    - The date on which each drive was wiped;

    - The method or program used (e.g., WipeDisk, WipeFile, BurnIt, Data Eraser, etc.)

- Identify and attach any and all versions of document/data retention policies used by [opposing party] and identify documents or classes of documents that were subject to scheduled destruction. Attach copies of document destruction inventories/logs/schedules containing documents relevant to this action. Attach a copy of any disaster recovery plan. Also state:

    - The date, if any, of the suspension of this policy in total or any aspect of said policy in response to this litigation;

    - A description by topic, creation date, user or bytes of any and all data that has been deleted or in any way destroyed after the commencement of this litigation. State whether the deletion or destruction of any data pursuant to said data retention policy occurred through automation or by user action;

    - Whether any company-wide instruction regarding the suspension of said data retention/destruction policy occurred after or related to the commencement of this litigation and if so, identify the individual responsible for enforcing said suspension.

- Identify any users who had backup systems in their PCs and describe the nature of the backup.

- Identify the person(s) responsible for maintaining any schedule of redeployment or circulation of existing equipment and describe the system or process for redeployment.

- Identify any data that has been deleted, physically destroyed, discarded, damaged (physically or logically), or overwritten, whether pursuant to a document retention policy or otherwise, since the commencement of this litigation. Specifically identify those documents that relate to or reference the subject matter of the above referenced litigation.

- Identify any user who has downloaded any files in excess of ten (10) megabytes on any computer identified above since the commencement of this litigation.

- Identify and describe all backup tapes in your possession including:

    - Types and number of tapes in your possession (such as DLT, AIT, Mammoth, 4mm, 8mm);

    - Capacity (bytes) and total amount of information (gigabytes) stored on each tape;

    - All tapes that have been re-initialized or overwritten since commencement of this litigation and state the date of said occurrence.

APPENDIX C[170]
SAMPLE FED. R. CIV. P. 30(b)(6) DEPOSITION NOTICE

UNITED STATES DISTRICT COURT IN THE SOUTHERN DISTRICT OF TEXAS

Court File No.:
_____, Plaintiff,
v.
_____, Defendant.

NOTICE OF TAKING DEPOSITION PURSUANT TO FED. R. CIV. P. 30(b)(6)

PLEASE TAKE NOTICE that, [Plaintiff / Defendant Corporation] take the deposition, before a qualified notary public by oral examination, of [Plaintiff / Defendant Corporation] on [date] commencing at [time], at [location]. The deposition will continue thereafter until adjournment. Pursuant to Federal Rule of Civil Procedure 30(b)(6), [Plaintiff / Defendant] corporate designee(s) shall be prepared to testify regarding the following subjects, all with respect to [Plaintiff's / Defendant's] information technology systems:

1. Number, types, and locations of computers (including desktops, laptops, PDAs, cell phones, etc.) currently in use and no longer in use;

    - Past and present operating system and application software, including dates of use and number of users;
    - Name and version of network operating system currently in use and no longer in use but relevant to the subject matter of the action, including size in terms of storage capacity, number of users supported, and dates/descriptions of system upgrades;
    - File-naming and location-saving conventions;
    - Disk and/or tape labeling conventions;
    - Backup and archival disk or tape inventories/schedules/logs;
    - Most likely locations of electronic records relevant to the subject matter of the action;
    - Backup rotation schedules and archiving procedures, including any automatic data recycling programs in use at any relevant time;
    - Electronic records management policies and procedures;
    - Corporate policies regarding employee use of company computers, data, and other technology;
    - Identities of all current and former personnel who have or had access to network administration, backup, archiving, or other system operations during any relevant time period.

[170] Excerpted from *id*. at 355-57.

APPENDIX D[171]
Questions for 30(b)6 Deposition of Custodian of Electronic Records

System Profile

- Describe the types of computer system(s) used by your company in the course of business.
- Describe/identify the type of software used on your computer system(s).
- Identify the person(s) responsible for the ongoing operation, maintenance, expansion, backup, and upkeep of the computer system.
- Does the staff [or inquire after key witnesses] have home computers used for business purposes? (If yes, repeat questions 1-2).
- Are passwords or encrypted files used on any of the computer systems? If yes:
- Describe how files are protected.
- Who could provide access codes if required?
- Have you modified your use of computers to comply with recent discovery requests?

Backup and Retention

- List all computer systems in the organization that are backed up.
- Describe the backup program(s) used. (Ex: ARCserve, StorageExpress, Maynard, Tecmar, etc.)
- Give details of your backup procedures:
- Have you modified your backup procedures to comply with recent discovery requests?
- Are files ever deleted from the computer system(s)?
- Are archival backups ever created? If yes:
- What files have been archived?
- Where are the archival backups maintained?
- Describe any disaster recovery plans in place now and for the relevant time period.

Maintenance and Access

- Are utility programs used on computer(s) in the office? (Ex: Norton Utilities, MacTools, network maintenance programs) If yes:
- Which program(s)?

---

[171] Excerpted from Joan E. Feldman, *The Expert's Role in Computer-Based Discovery*, ATLA-CLE 157 (February 2003).

- Has the program been used to permanently "wipe" files? (When?)
- Has the program been used to de-fragment, optimize, or compress drives? (When?)
- How do those outside of the company access the computers?
- How are office computers secured?
- Has any computer hardware been upgraded in the past 12 months?
- Has any computer software been upgraded or replaced on office computers in the past 12 months?

Chain of Custody/Authentication

- Are individual directories purged when an employee leaves the company?
- Are passwords and access codes revoked when an employee leaves the company?
- Are workstations reassigned to incoming employees? If yes:
- Are hard drives wiped or re-formatted for the new user?
- Are hard drives backed up before the new user takes system?
- Describe how used or replaced equipment is disposed of or sold.
- Describe how used disks or drives are treated before destruction or sale. (Degaussed? Shredded?)
- Have you used outside contractors to upgrade either hardware or software? (If so, please identify)
- Are changes or modifications made to software recorded? (Electronically? Are hard copy logs kept?)