Author: Nathaniel V. Thompkins, Esq.
The Law Offices of Nathaniel V. Thompkins
http://www.nm-ny-pa-law.net
Date: August 18, 2006

E-DISCOVERY[1]

(Version 1.0 to Be Released - December 2006)

Introduction

On December 1, 2006, amendments to the federal rules of civil procedure are scheduled to become effective. The amendments are intended to expand upon and refine the discovery rules as they apply to electronically stored documents or data, or also known as "electronic discovery" or "E-discovery".[2] While the announcement of the Amendments to both the federal rules was not accompanied by much fanfare and is not the stuff of headline news, it is nonetheless a revolution of sorts. This article will discuss how the amendments will have a profound affect on both federal and state[3] civil justice systems. Therefore, practitioners and businesses alike should appreciate and understand what has been changed and the relevant importance. The article will discuss briefly the subject of electronic data and data storage. It will look briefly at the history and purpose of the federal discovery rules in order to better appreciate the necessity of these amendments. Finally, the article will discuss the case of Zubulake v. UBS Warburg[4] which provides greater incentive for counsel and parties involved in litigation to consider the importance of understanding the universe of data that resides on a company's computer system and the system's capacity to retrieve the data in the context of discovery demands.

It is important to understand and appreciate from whence the amendment to the federal discovery rules came and the underlying subject of electronic digital storage. In 2004 the Judicial Conference of the United States approved extensive amendments to the federal rules of civil procedure. The Committee submitted the new rules and amendments to the Judicial Conference on July 25, 2005 for consideration at its September 2005 session with recommendations that they be approved and transmitted to the Supreme Court.[5] The

[1] This Article is not an exhaustive look at the Amended Federal Rules, as that would or has been the subjected of books on the topic, however, this article is intended to provide some important history and recent developments as we approach the December 2006 enactment of the Rules.
[2] http://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp
[3] The impact on states will be felt where, as in most cases, a state follows the Federal Rules of Civil Procedure or uses the rules a authority and for guidance.
[4] Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003)
[5] http://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp

July 25, 2005 submission contained substantial revisions to the comments.

The amendments were an effort to narrow the scope of discovery and impose judicial oversight on the discovery process. However, the subject of discovery of electronically stored data or electronic data, known as "electronic discovery" or "E-discovery" was a unique topic that required a broad breath of consideration.[6]

The subject matter triggered a storm of articles, the development of law firm specialties, computer forensic data retrieval businesses, Lexis™ and Thompson/Westlaw™ services on E-discovery, and books specifically written on the topic of "E-Discovery". While much has already been written on this topic, it is anticipated with their enactment, the rules will be the subject of considerable debate, articles and books.

Advancements in computer technology have been an incredible tool for businesses of all kinds. It has also created something that did not exist in earlier paper based storage systems – electronically stored data. Data, more specific, electronic data is stored on computer systems and in some instances forgotten, at least until, there's a law suit. With the proliferation of electronic data storage, the Judicial Conference of the United States, suggested amendments to the federal rules that would help to rein in this electronic beast. Since the promulgation of the amendments, countless businesses have developed ways to assist in managing corporate electronic data and provide trial management electronic discovery services. Fueling the growth of a cottage industry is the fact that 90 percent of all documents produced since 1999 were created in digital form.[7]

I. The Age of Computer Reason

The invention of the first computer and computer application to businesses resulted in a development and improvement trend that makes today's new technology tomorrow's museum object. The average life cycle of software and hardware is approximately five years. This phenomenon is referred to as "Technological Obsolescence" and is when hardware used to run specific software is no longer available.[8]

---

[6] *Two Tiers and a Safe Harbor:* Federal Rule Makers Grapple with E-Discovery, Ken Withers, August 23, 2004, pg. 3.
[7] *Electronic Discovery Primer*, Law Technology News, Albert Barsocchini, August 28, 2002, pg. 1.
[8] http://www.millarch.org/francisco/papers/Dissertation.htm *The Digital Information*
An analysis of information overload, and document preservation in cyberspace

The computer while revolutionary in terms of how an organization functions has also fundamentally changed every business's ability to transact business around the world with the click of a mouse or the stroke of a computer keyboard. Which brings up the question, how fragile is the data that is created and stored by these businesses?[9] As technicians point out, the "usable lifetime of digital storage media generally exceeds the life of the technology that supports it."[10] In the case of long term storage, this presents a larger more complex set of problems. Digital information created on one particular technological platform may only, in some instances, be usable on that particular platform. In most instances the data can be "manipulated" for use on other platforms. However, if the manufacturer has not built-in "backward compatibility" into the software, manipulation of the data may be too costly a solution. Thus a company may be holding data that it can no longer access or use.

One solution, from software manufacturers is the method of "migrating data" from one technology to another. However, given the undetermined number of times a company may need to migrate its data, this solution could become a costly prospect. Another option, although equally unappealing, is to maintain a museum of out-dated software to access the stored data. This option is subjected to the vulnerability of computer crashes, virus attacks, corrupted software and the lack of continued support by manufacturers of out-dated software.

Briefly, these subjects are important issues every business should take into consideration when deciding how to address its information technology ("IT") needs. As the author, Francisco Millarch, points out in his dissertation, *The Digital Information*, "we only risk loosing digital information so easily because we have too much of it. And, by having too much of it, we cannot properly evaluate its importance, and critically discern what really should be preserved." [11] Therefore, an important component of a company's IT strategy should involve a clearly defined and easily implemented electronic document retention policy. The program and policies should take into consideration the relevance of the information, the cost of preserving it and the technological issues we have mentioned.

With a clear and effective digital file retention policy a company will gain the benefits of understanding the importance of the data it

[9] *Id.*
[10] *Id.*
[11] *Id.*

retains, quickly and efficiently evaluate the retained data and preserve only that data which is important to the company's mission. By having such a policy and actively enforcing it, a company, faced with litigation, which is a reality for 35% of businesses, can cut down on discovery and eliminate potentially adverse discovery. A company can avoid potential liability in a lawsuit if it has immediate and efficient access to electronically stored data in its possession. More importantly, an effective digital file retention policy provides an important litigation tool. 1) It affords the company easy access to exculpatory data, or at least, supportive data relevant to the defense of a claim; and 2) It conveys litigation readiness which can either help settle a case or make it easier to prepare for trial. While this by no means is an exhaustive discussion on digital document retention policies it suggests that both the practitioner and company should seriously consider these issues as we approach December 1, 2006.

II. What is Electronic or Digital Data?

Computer storage, simply stated, is the holding of data in an electromagnetic form for access by a computer processor. Primary storage is data in random access memory ("RAM") and other "built-in" devices. Secondary storage, is data on hard disk, tapes, and other external devices. However, this begs the question, what is Digital Data?

Digital data consists, at its most basic level, of just 0s and 1s. The 0s and 1s are "binary" terms which mean that it can have only two possible states – 0 or 1. Your computer stores information by using switches (i.e. on-off). The computer that you purchase will record what information the 0 and 1 will represent when you begin imputing data into you computer. One switch can store one "bit" of information. Eight bits are called a "byte". Your computer organizes these magnetic particles (0/1 values) in chunks that are called sectors. A sector on your computer's hard-drive holds 512KB (Kilobytes) of information or approximately 512,000 bytes or 4.2 million 0/1 values.[12]

Briefly, a sector is how your computer hard-drive communicates and a sector is the smallest unit on a hard-drive. The sector is organized by your computer into "clusters". The cluster is a group of sectors that are always a multiple of two and their size is set for all drives in your computer, i.e. there are no one sector clusters. The cluster is the smallest atomic unit that an operating system will

[12] *Digital Forensics in Civil Litigation*, Pennsylvania Bar Institute, authors Leonard Deutchman, Esquire, and Brian T. Wolfinger, September 2005, pg. 10.

address under normal circumstances. Given how the operating systems works the amount of space taken up by clusters is wasteful.[13] However, for purposes of this article, it is not important that you understand the finite processes of data storage but simply understand how mechanically data is created and stored.

Your computer, similar to a file cabinet, is designed to hold information, documents, or data. RAM is your access to the data in the filing cabinet. While you may not be able to look, all at once, at every document in the file cabinet, the RAM allows you to swap documents in an out in an organized and efficient manner. You can increase the size of your RAM should you need to view greater amounts of materials or data at one time or at a faster pace. The data retrieved from the file cabinet, via your computer's RAM, is stored temporarily while it is being worked on. Once the computer has been shut down, the documents that were temporarily stored in RAM are returned to the file cabinet, along with any changes, and the data no longer resides in your computer's RAM.

III. Data behind Data = Metadata

Now that we understand the basics of data and data storage it is equally important to understand what data is included with or behind the data. This is known as "metadata". An excellent article in the topic was written in the *New York Time*, Beware Your Trail of Digital Fingerprints, by Tom Zeller, Jr., November 7, 2005, in which it defined metadata as, "Technically, metadata is sort of the DNA of documents created with modern word-processing software. By default, it is automatically saved into the deep structure of a file, hidden from view, with information that can hint at authorship, times and dates of revisions (along with names of editors) and other tidbits that, while perhaps useful to those creating the document, might be better left unseen by the wider world." Metadata, however, is not limited only to word processing documents as it can be found in virtually any digital document that is created and resides on your computer. With most software programs you are able to view some of the metadata in your documents. However, for a more extensive look at a document's metadata, third-party software programs are available and designed to crack open documents and reveal even more metadata.

While there are no examples of significant verdicts turning upon the smoking gun being the discovery of information in a document's

[13] *Id.*

metadata, there have been examples that warrant serious thought as to how you distribute and disseminate documents and data to the public or opposing parties in litigation. The Beware Your Trail of Digital Fingerprints, New York Times article, cited previously, discloses several instances where an unintended release of metadata proved to be highly embarrassing.

An unsupportive memorandum written about Judge Alito was distributed with no-attribution, i.e. no author named. However, because of the document's metadata, which was included in the digital document, the Democratic National Convention's ("DNC") finger prints were found all over it.[14] In another incident, the United Nations issued a report regarding Syria's suspected involvement in the assassination of Lebanon's former Prime Minister, Rafik Hariri. Despite the fact it was a damming report of Syria; the document's metadata revealed certain editing changes in which officials involved in the plot had their names deleted. Two such deleted names were the Syrian president's brother and brother-in-law.[15]

Instances such as the Judge Alito memorandum and United Nation's report on Syria, as well as others, have alerted attorneys' to the advantages of requesting metadata in discovery documents and have spurned debate concerning the scrubbing of metadata from documents.[16]

IV. "Delete" does not mean Deleted!

Before moving on to the topic of litigation, discovery and amendments designed to cover E-discovery, a brief discussion of how documents we think are deleted, actually still reside on our computer hard-drives or corporate network storage devices is helpful. Unlike words on a chalk board, which when erased remain only in our memory, this is not so with an electronic data file. When you "delete" a file, you have not wiped the particular electronic data clean out of existence from your computer's storage. Many documents that you thought were deleted can be found stored in various and different parts of a computer's hard drive. In addition, you may even find different and various versions of the same documents in other storage places within a company's network of computer systems.

For example, when you press the "delete" button on your computer to delete a word processing document, the computer first

[14] *NY Times*, Beware Your Trail of Digital Fingerprints, *supra*
[15] *Id.*
[16] *Id.* pg. 2.

notifies the operating system that the space where the file was stored is now available for use to store other sectors of data. In a Microsoft Windows™ system, the deleted file is listed in the directory as modified; the file name is changed to a Greek sigma character which lets the computer know that the file is deleted.[17] Despite this fact, no other changes are made to the data file. The data file remains on the hard-drive where it can reside for hours, days, or years depending on the size of your computer's hard drive. Also affecting how long a deleted file remains on the computer hard-drive is the Operating System ("OS"), computer usage and/or tasks run on the system.

Virtually all large and increasing most small corporations have corporate networks that are connected to one or more file servers for purposes of data storage. In addition to document metadata, file servers generally provide a log[18] of information that might prove central to pending litigation. An important example is when an opposing party claims to have lost files prior to a certain date. If the loss is allegedly attributed to a network outage/server crash, this fact can be either supported or refuted by an examination of the server's log. The log can show information such as when the system was functioning, when the operating system was reinstalled as well as other important information. Beware of a computer's log being a more accurate historian than the operator or operators of that computer.

Another type of server that might be found in a company is an E-mail server. Like a workstation's computer storage and a data storage server, an E-mail server might contain important information of communications between employees and others outside the company and which may prove relevant to litigation. As with a data storage server, an E-mail server's log can show transactional information, logging data and any efforts to purge data. In some instances an E-mail server may be able to show a parties lack of effort to retain data pursuant to a discovery request or discovery order.

Finally, other sources of potential data or metadata exist in the company's connection to the internet, web-mail and Cache on the PC. Internet browsing software (browsers) keep records of internet sites that users have previously visited. These file are commonly referred to as internet history files and may be helpful or damaging in litigation.

---

[17] *Digital Forensics in Civil Litigation*, Pennsylvania Bar Institute, authors Leonard Deutchman, Esquire, and Brian T. Wolfinger, September 2005, pg. 11.

[18] A computer "log" is exactly what the term implies, it takes and makes a sequential record of actives or data that was either accessed or

The Internet Cache files are what makes browsing the internet go faster. Internet data is downloaded, i.e. data such as pictures and text, directly to your computer's Cache. When you navigate back to a page that you previously visited, the data is pulled from your computer's Cache, rather than pulling the data down again from the internet. The computer's Cache can contain extensive amounts of data about a particular user and their actions on the internet. Such things as user habits, web-based e-mail, timelines and other investigative avenues are available via this type of data.

With all the data that is potentially available on a company's computers, there is a growing or cottage industry focused on digital forensics. Forensics involves investigating, locating and analyzing data and/or metadata that reside on computer systems owned by companies involved in litigation. Remember our early discussion about too much data, the more data you have, even irrelevant and no longer important data which is retained because of lack of an effective digital document retention policy, the more expensive the costs of digital forensics on a company's data. These facts create an increasing need for oversight and governance which is embodied in the amendments to the federal rules of civil procedure and concerning E-Discovery.

V. Discovery

A. Purpose of the Federal Discovery Rules:

Historically discovery rules were designed and intended as "… the pre-trial functions of notice-giving, issue-formulation and fact-evaluation …".[19] As noted by the court in Hickman v. Taylor, discovery was "narrowly confined … and … cumbersome in method." Id. Since Hickman many scholarly articles have been written on the topic of discovery.[20] It was observed on the twentieth birthday of the federal rules that:

> Modern instruments of discovery serve useful purpose, as we noted in *Hickman v. Taylor.* … They together with pretrial procedures make a trial less a game of blind man's bluff and more a fair contest with the basic issues of facts disclosed to the fullest possible extent.[21]

Discovery was designed with the intent of having four distinct but interrelated purposes. First, it was designed to narrow and clarify

[19] Hickman v. Taylor, 329 U.S. 495, 500-01 (1947)
[20] *Full Disclousre*, Combating Stonewalling and Other Discovery Abuses, Hare, Jr., Gilbert, Ollanik, (ATLA Press 1994) pgs. 3-4.
[21] *Id.* pg.4 *citing* United States v. Procter & Gamble Co., 35 U.S. 677, 682 (1958).

the issues; Second, it was to allow the parties to identify potentially relevant information, persons, and ascertain how and in what form the information may be obtained; Third, discovery was intended to eliminate unfair surprise; and Fourth, the expeditious, just, and final resolution of disputes with an eye towards the substantive rights of the parties.[22]

B. Why Amend the Rules for E-Discovery?

After the published Amendments of the rules were submitted for comment in August 2004, some significant comments and observations were made by the Advisory Committee on the Federal Rules of Civil Procedure.[23] It was agreed upon by a consensus of the Committee that, "*electronically stored information has important differences from information recorded on paper*." Electronically stored information is "*retained in exponentially greater volumes than hard-copy documents*; *electronically stored information is dynamic,*[24] *rather than static; and electronically stored information may be incomprehensible when separated from the system that created it."* Finally, electronically stored data is causing discovery problems that amendments to the rules can address.[25]

The Amendments are intended to resolve some difficulties peculiar to electronic discovery. As such, they targeted the following areas of concern:

- In what form shall electronic discovery be produced;
- How to preserve electronic discovery for litigation; and
- What privileges and work-product protections apply to electronic discovery?

The Committee's comments suggest early attention in litigation should be paid to the Electronic Discovery issues in a case. This advice becomes clearer as we walk through the Amendment to Rules - 16, 26(a), 26(f), 33, 34, 37 and 45.

C. What was amended in the Rules?

1. Rule 16

[22] *Id.* pg. 5.
[23] See Report of the Civil Rules Advisory Committee, Honorable Lee H. Rosenthal, Chair, May 27, 2005 (Revised July 25, 2005)
[24] The dynamic nature of electronically stored information comes from the operator's ability to perform routine maintenance, normal operations, system changes and the deletion of information.
[25] *Id.*

In Federal cases, Rule 16 addressed pre-trial conferences and its management. It gives the court the discretionary authority to enter into case management or other orders. However, this authority is not mandatory and there must be agreement between the parties. The other aspect of Rule 16(b) limits the court's authority to act on motions.

Rule16 was amended by adding subsections 16(b)(5) and 16(b)(6). Subsection (b)(5) allows the parties to agree to include in the scheduling order a "*provision for disclosure or discovery of electronically stored information*". Although intended to alert the court to the need to address the handling of electronic discovery, the amendment also draws the practitioner's attention to the fact that the court's scheduling order may place restrictions and/or burdens upon the parties regarding the disclosure of electronically stored information.

As advised by the Committee's comment, practitioners would be ill advised to wait until a discovery conference before considering and/or discussing how to handle electronic discovery. Thus, counsel should discuss E-Discovery topics early on in a case in an effort to avoid and/or identify potential or actual disputes. This advice is captured in the amendment to rule 26(f) – *General Provisions Governing Discovery; Duty of Disclosure* – to which the committee added, "… *to discuss any issues relating to preserving discoverable information…*" Early discussion can avoid costly and time-consuming searches and wasted production in a case involving electronic discovery.

Second, 16(b)(6) adds protections via an agreement between the parties regarding the assertion of a claim of privilege and protection of trial-preparation materials, post production. The amendment reads, "… *(6) any agreement the parties reach for asserting claims of privilege or protection as trial preparation material after production."* Parties can agree on how to preserve a claim of privilege and attorney-work-product by entering into an agreement covering this topic and including the agreement in the court's scheduling order. Said agreement eliminates or minimizes the risk of a party waiving privilege or rights to claim work-product protection after it has produced E-discovery materials. This type of agreement would reduce the parties upfront cost normally associated with combining through all electronic data that it produces and give the producing party the opportunity to raise their objections to electronic data evidence at some later point in the litigation.

With the amendment, parties may agree to various arrangements that are intended to preserve both privilege and work-product trial preparation materials. The arrangements can be as varied as the attorney's that create them. Some methods that have been entered into include a "quick peek,"[26] while other agreements contain "clawback"[27] provisions. Regardless of the particular provision, a party that receives information under any such agreement may be prohibited from raising waiver of the claim of privilege or of work-product protection as trial preparation material against an opposing party.

2. Rule 26(a)

Rule 26 addresses the General Provisions Governing Discovery and the Duty of Disclosure. Subdivision 26(a)(1) discusses initial trial disclosures and makes mandatory certain categories of information that must be automatically disclosed without waiting for a discovery request from the opposing party. The Committee amended subsection 26(a)(1)(B) and thereby made it mandatory that parties disclose "… a copy of, or a description of by category and location of, all … "electronically stored information".

While patently significant, the rule underwent this necessary modification because the original amendments had an inconsistency concerning electronic discovery issues. The amendment to Rule 26(f) – *Conference of Parties; Planning for Discovery* - referred to disclosures as well as the discovery of electronically stored information. With that amendment [26(f)], the Committee recognized the need to make the disclosure requirements of 26(a)(1)(B) consistent with the "electronically stored information" found in 26(f).

Additionally, Rule 34, which made "data compilation" a subset of "documents" rendered redundant the "data compilation" originally set forth in 26(a)(1)(B). With the above-referenced amendment, Rule 26(a)(1)(B) parallels Rule 34(a) by recognizing that a party must disclose electronically stored information as well as documents that it may use to support its claims or defenses. Thus, deleting "data compilations" was necessary as it was both a subset of both documents and electronically stored information.

---

[26] This is an agreement where the parties agree that a responding party will provide certain requested materials for initial examination without waiving any privilege or protection.

[27] This agreement also provides for production without the intent to waive privileges or protected data. If a party identifies a document mistakenly produced, then the document is returned under the clawback provision.

The meet and confer conference, as it is sometimes referred to, is the subject of Rule 26(f) and provides "… as soon as practical, … or at least 21 days before a scheduling conference or a scheduling order is due … confer to consider the nature and basis of their claims and defenses …" With this amendment, the parties are directed to discuss electronically stored information during the meet and confer conference.

Additional discover matters included in an agreement are captured in amendment 26(f)(3) which now reads, "… (3) any issues relating to disclosure or discovery of electronically stored information, *including the form or forms* in which it should be produced." As well, amendments to 26(f)(4) now reads, "… any issues relating to claims of privilege or of protection as trial-preparation material, including – if the parties agree on a procedure to assert such claims after production – whether to ask the court to include their agreement in an order."

With these amendments, the Committee's advisory note regarding the need to address electronic data issues early on takes on even more importance. As disclosed earlier, many companies have too much data and lack a clear and regularly enforced electronic data retention policy. By having too much data, neither the company nor its counsel can properly evaluate its importance and/or discern what should be preserved or produced. Therefore it becomes necessary for counsel to become knowledgeable about the company's data storage systems and the system's capabilities. As well, counsel should identify, with the company's assistance, individuals with special knowledge of the computer system to assist in developing a meaningful and executable discovery plan.

While each discovery plan will be unique, consideration of some general topics to include in a plan are helpful:

1. Identify information within a parties control;
2. Identify information capable of being searched;
3. Determine if data is reasonably accessible;
4. Determine if the burden or cost of retrieving and reviewing;
5. Determine and agree upon the form or forms of production; and
6. Identify early any and all disputes over electronic discovery data.

While the above referenced list is by no means exhaustive it provides some guidance and general topic areas that should be considered.

Another equally important amendment to 26(f), concerns the preservation of discoverable information. The specific language that was added in 26(f) is "… to discuss any issues relating to *preserving* discoverable information …" Although this applies to all kinds of information, it has particular significance to electronically stored information. As you may recall we discussed the "dynamic" nature of electronically stored data in section B of this article. With respect to the preservation of discoverable information, the ordinary operations of a computer, i.e. automatic creation, automatic deletion and/or overwriting, complicates this requirement. Failure to take into consideration these important aspects of electronic data could result in the paralysis of a company's business activities. Also, a "blanket" preservation order may be prohibitively expensive and unduly burdensome. Therefore it is strongly encouraged that counsel understands how a client's computer system works, take into consideration the specifics of the client's system and have a goal of agreeing on reasonable preservation steps in light of the particulars of the client's electronic data storage capabilities.

Rule 26(f)(3) and (f)(4) were alluded to in section B above and suggest both "quick peeks" and/or "clawback" provisions. The amendments were intended to help facilitate the discovery process and to that end, the Committee amended Form 35. The amendment to Form 35, requires the inclusion of a brief description of the parties' proposals on handling the disclosure or discovery of electronically stored information. It would also require inclusion of a brief description of any provisions of a proposed order reflecting the agreement of the parties regarding claims of privilege or protection as trial-preparation material asserted after production.[28]

3. Rule 26(b)

Rule 26(b) addresses the restraints a court may place on discovery by limiting the scope of discovery. One such control is found in amendment 26(b)(2)(B). This subsection authorizes the party responding to a request for electronic discovery to respond that the requested data is not reasonably accessible because of undue burden or cost. In raising this claim, the responding party has the burden to show that the sources are not reasonably accessible. Even though a responding party has met its burden, the court can still order production of electronically stored materials upon an opposing party's showing of good cause supporting the request for production.

[28] http://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp

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

Once again, early resolution could prevent unnecessary disputes regarding electronically stored information that is inaccessible, an undue burden and cost prohibitive to produce. If the parties cannot reach agreement then the available procedures would involve either a motion to compel or a motion for a protective order. In either case, the parties are bound to confer prior to filing a motion. Should the matter reach the motion stage, the court may require a responding party to conduct a sampling of information contained in the electronic data source identified. Other measure may include allowing some form of inspection or taking depositions of witnesses with knowledge of the system containing the requested information. In either scenario this discovery method could prove just as costly. Therefore, counsel would be well advised to understand the universe of electronic data early on in the case. Get a good grasp of the system and the persons that are knowledgeable about its operations and capacity to retrieve electronic data. Armed with this information, start negotiating reasonable discovery terms addressing the electronic discovery involved in the case. Then have your agreement(s) reduced to writing and made a part of the court's discovery order.

4. Rule 26(b)(5)

Rule 26(b)(5) addresses how parties may withhold materials or, if they have produced materials in discovery, claim privilege or the protection of trial-preparation material. The producing party must notify opposing counsel of the claim or claims and state the basis for such claim or claims. In this instance, after the receiving counsel or party has received notification, he or she must, in the case were materials have already been produced, return, sequester, or destroy the information claimed by the opposing side. The receiving party, in the latter instance, is prohibited from using or disclosing the claimed

information to third parties until the claim is resolved. While the claim is unresolved, the receiving party has the option of submitting the information claimed to the court, wherein the court will determine if the information is protected or a waiver has occurred. In the event that the information is either withheld by the producing party or returned, the producing party is required to preserve the information pending the court's ruling.

As discussed briefly in section V.C.2 above, this provision works in tandem with 26(f) wherein the parties may enter into agreements with either a "quick peek" or "clawback" provision for inclusion in the court's discovery order. Thus, under 26(b)(5)A) a party may withhold information and claim privileged or assert that the materials are subject to protection as trial preparation materials. Or, if the information has been produced, the producing party can notify the receiver of the claim of privilege or assertion of the materials as trial preparation materials. In either instance, the party making the claim or claims must set forth the basis for the claim or claims.

5. Rule 33

Rule 33 governs Interrogatories and Request for Production. The amendment brings the rule up to the information age by making it clear that a responding party has the option, even with electronically stored information, to produce business records or make them available for examination. Difficulty arises or is exacerbated with respect to electronically stored information. In certain situations there may be issues of Technological Obsolescence,[29] inaccessible form of production and/or electronic data is only accessible through the use of a particular computer system. In these instances, Rule 33(d) provides that if the burden of deriving the answer is substantially the same for both parties, then the court will allow the responding party to substitute access to documents or electronically stored information for its answer. The caveat is that, the party electing this option must ensure that the opposing party can locate and identify the information "as readily as can the party served". Additionally, responding parties must give the opposing party a "reasonable opportunity to examine, audit, or inspect" the information.

In some instances, when a responding party takes advantage of 33(d), they may be required to provide a combination of technical support, information about the software, or some other sort of assistance. Therefore, if the responding party is required to provide

[29] Technological Obsolescence is defined in Section I, paragraph 1 of this article.

direct access to its electronic information system, the responding party should be on its guard to protect against the disclosure of confidentiality or proprietary information.

6. Rule 34

The original Rule 34 focused on the discovery of "documents" and "things."[30] In anticipation of the growth of computer usage the rule was amended in 1970 to include the discovery of "data compilations."[31] Again, because of the dynamic nature of electronically stored data there was a need to clarify that Rule 34 applies to information fixed in a tangible form and to information stored in a medium for which it can be retrieved and examined. Therefore, additional clarification involved understanding that "documents" include electronically stored information, unless a requesting party makes a distinction.

Another important consideration made in the amendment to Rule 34 involves the ability of a party to request an opportunity to test or sample materials sought under the rule, in addition to both inspecting and copying the materials. Practitioners are advised to raise any issues or concerns involving both confidentiality and privacy in the requested materials. The inclusion of testing and sampling in the amendment does not create a routine right of direct access. Therefore, if an agreement cannot be reached and when necessary seek the court's assistance in preventing undue intrusiveness resulting from such requests.

Rule 34 allows the requesting party to request what "form or forms" that electronically stored information is to be produced. The responding party, under the amendments, can produce the materials in its ordinarily maintained form or in a form or forms that are reasonably usable. However, with respect to a particularly requested form or forms, the responding party can object to the form or forms selected by the requesting party. If an objection is made or if no form has been requested, the responding party must state the form it intends to use in producing electronically stored materials. The indications drawn from the procedure, gives the parties an opportunity to agree upon a form or forms. Should a dispute arise, the parties can file a motion under Rule 37(a).

---

[30] *Digital Forensics in Civil Litigation*, Pennsylvania Bar Institute, authors Leonard Deutchman, Esquire, and Brian T. Wolfinger, September 2005, pg. 92.
[31] *Id.*

7. Rule 37

Rule 37 governs sanctions that are available when there has been a failure to make disclosure or cooperate in discovery. The ultimate penalty for a violation of the discovery rules is the imposition of sanctions. Rule 37 was amended by adding subsection 37(f). While this subsection brings within the rule the subject of electronically stored information, it takes into consideration that computer systems have routine modifications, overwriting and in normal business operations, deletions. The amendment provides limited protection against sanctions for the routine operations of an electronic information system; provided the operations are done in good faith.

The drafters of the amendment took into consideration the fact that the routine operation of computer systems involves data alteration and the overwriting of information, without operator awareness or intent.[32] The drafters also understood that these features are essential to the operation of modern IT systems. Although acknowledging these facts, Rule 37(f) is not intended to work as a shield for parties that intentionally destroy information in the contexts of litigation. Thus, under Rule 37(f), absent exceptional circumstances, sanctions will not be imposed for the loss of electronically stored information resulting from the routine, good-faith operation of an electronic information system.

8. Rule 45. Subpoena

The amendments to Rule 45 track and/or conform to the amendments we have described in the other rules. I will attempt to go through and parallel the most important amendments found in Rule 45.

1. Subsection 45(a)(1)(B), like Rule 34(a), addresses testing and sampling, with the former allowing for the issuance of a subpoena for such purposes including inspection and copying.

2. Subsection 45(a)(1)(C), like Rule 34(b), is amended so that the party, in this instance issuing a subpoena, can designate the form or forms of producing electronic data.

[32] *Digital Forensics in Civil Litigation*, Pennsylvania Bar Institute, authors Leonard Deutchman, Esquire, and Brian T. Wolfinger, September 2005, pg. 110.

3. Subsection 45(c)(2), like Rule 34(b), preserves a party's right to object to the requested form or forms, demanded by the subpoena.

4. Subsection 45(d)(1)(B), similar to Rule 34(b), provides a default that if a subpoena does not specify the form or forms for electronically stored information, the person served must produce the electronic data in a form or forms which it is usually maintained or in a form or forms that are reasonably usable.

5. Subsection 45(d)(1)(C) is a totally new amendment that provides that the producing party, of electronically stored information, should not be required to produce the same information in more than one form, unless ordered by the court for good cause.

6. Subsection 45(d)(1)(D), like Rule 26(b)(2)(C), provides that a responding party need not produce electronically stored information from sources a party identifies as not reasonably accessible. For good cause shown, however, a court can order its production.

7. Subsection 45(d)(2), like 26(b)(5), adds a procedure for the assertion of privilege or of protection as trial-preparation materials after production. In both instances, the receiving party may submit the information to the court for resolution of the privilege claim.

There are other minor amendments to Rule 45 that conform to the other rule changes. However, I have provided a parallel of those changes that I believe are significant enough to warrant your immediate consideration, the other minor amendments, while important, should be consulted by the reader before December 1, 2006.

VI.

Lessons from the case of Zubulake v. UBS Warburg

The precautions suggested by the Committee regarding the need to understand the client's electronically stored data and data system are not better exemplified than in the case, Zubulake v. UBS

Warburg.[33] The underlying facts of the case involved a gender discrimination suit by Laura Zubulake against her former employer, UBS Warburg. In a discovery request, Zubulake requested emails that existed only on back-up tapes. An additional request sought e-mails between Zubulake and several key people. An agreement was reached between the parties wherein UBS Warburg agreed to produce emails of the relevant key people.

UBS Warburg produced 100 pages of emails and Zubulake produced 450 pages. No additional emails were produced by UBS Warburg and the company took the position that the agreement did not cover a search for emails on back-up tapes. Zubulake took the opposite position and demanded all emails. A deposition of UBS Warburg's IT designee revealed that an indexing program revealed that there were seventy-seven back-up tapes containing the emails at issue. Further, since they were archived, the emails were easily searchable using search terms.

The court then ruled that the discovery request of Zubulake was proper and ordered production of the emails.

In Zubulake III, the court reviewed the results yielded from restoration of the five back-up tapes. It was determined that it cost $19,000 for the restoration of the five tapes and it would cost and estimated $273,649 to restore the remaining seventy-two back-up tapes. The court after weighing all the factors order Zubulake to bear 25% of the cost of producing the back-up tapes.

In Zubulake IV, the plaintiff was able to show that UBS was unable to produce back-up tapes containing emails of four central figures in the case. Zubulake was further able to demonstrate that some of the emails had been intentionally deleted. Despite a request of the court to award sanctions and give an adverse inference instruction to the jury, the court only ordered UBS to pay for the cost of re-deposing several witnesses whose emails were disclosed after the initial depositions and as a result of the discovery litigation.

In Zubulake V, despite a preservation order being in place, UBS employees deleted emails and in some instances never produced information to counsel. Thus, after two years from the date of the initial discovery demand, additional emails had been recently

[33] There are four decisions which demonstrate the advisory points raised in this article: Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003) (Zubulake I); Zubulake v. UBS Warburg, 216 F.R.D. 280 (S.D.N.Y. 2003) (Zubulake III); Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003)(Zubulake IV); and Zubulake v. UBS Warburg, 2004 U.S. Dist. LEXIS 13574, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) (Zubulake V).

discovered and it was determined that many other emails were irretrievably lost. The latter events happened because counsel failed to 1) retain information given by one employee; 2) instruct another employee about the litigation hold; 3) communication to UBS employees, sufficiently, email retention; 4) safeguard the back-up tapes that contained the lost e-mails. The court found "clear" proof that UBS employees had ignored the litigation hold.

Further it was noted; that UBS had withheld several relevant emails that were easily accessible, and did not divulge them until after a significant number of depositions had been take. Some of the emails subsequently discovered strongly supported Zubulake's contention that she was fired in retaliation for filing her EEOC complaint.

The court went beyond just criticizing UBS for their failure to produce and preserve discovery to criticizing UBS's counsel for their failure to supervise properly the retention and production of discovery. It ordered that the jury be instructed to draw an "adverse inference" from UBS's deletion of emails. The court further ordered UBS to pay the costs of any depositions or re-depositions as well as the costs of the instant discovery motion. Many important lessons can be learned from this case.

Lesson 1: Counsel must educate himself and become fully apprised of the client's electronic data and the capabilities of the systems in order to adequately advise the client as to what it must do.

Lesson 2: Counsel must understand fully his duty to identify all relevant discovery materials. Don't take at face value what "key players" say about emails and/or electronic documents that have been destroyed. Subsequent discovery of "deleted" or "destroyed" emails or documents can contradict what a witness may say under oath.

Lesson 3: There's no preparing a witness whose credibility has already been destroyed.

Lesson 4: Do not under estimate what your opponent already knows.

Lesson 5: Do not let discovery become <u>The Issues</u>, the defendant, in those instances, will most certainly always lose. With an adverse inference instruction being given, the defendant

has distracted the jury from the central issue and assured him or herself of a verdict in favor of the plaintiff.

Lesson 6: Spoliation is ***not*** about destroying evidence; rather it's about ***possible*** adverse evidence. In such instances one will never know if evidence is harmful or not. However, with an inference that question is answered; it was harmful and therefore destroyed.

CONCLUSION

The importances of the rules to federal litigation are obvious. State court systems that follow the federal rules on matters of discovery will like wise feel the impact of the amendments. However, what is anticipated is that without fan fare or articles alerting businesses and practitioners alike, the alarm will not be heard until well after the rules have become effective. As noted, the major problem with electronically stored data is the unknown quantity of data that is being electronically stored. Industry practices, the lack of a good electronic data file retention policy and the lack of enforcement of retention policies only exacerbates the problems. The inability of a company to properly evaluate the importance of their electronic data, and to critically discern what should be preserved, will lead to more decision like that of Zubulake v. UBS Warburg.

The warning bell tolls not only for the owners of uncontrollable amounts of electronically stored data, but, practitioners alike must also consider the warnings and realties of practicing in this electronically developed world where IT knowledge must be acquired. As noted in Zubulake the court's terse words went beyond admonishing the client and directed some strong advice to the counsels as well. As practitioners we must be on guard to not only educate ourselves about the rules but also about the system which operates and stores our client's electronically stored data. Before we can communication effectively the importance of "preserving" electronic discovery when a litigation hold order is in place, we must understand the quantity of data, the operation of the system and the capabilities of retrieving electronic data. Without a full appreciation and understanding of these basic facts and principles, more case will suffer the fate of Rule 37 sanctions.

It is hoped that this article will resonate with the reader regarding the importance of understanding the impact of the rules and their use in litigation. More importantly, it is hoped that business and legal professionals alike appreciate the very real impact that these

rules will have on how businesses store and have access to electronically stored data. Companies that haven't reviewed their current practices and polices and procedures applying to electronically stored data will, post December 1, 2006, be operating on borrowed time. The risks, as exemplified in Zubulake, are too great and companies should begin placing this topic at the top of a corporate policy list.

The author, Nathaniel V. Thompkins, Esquire, has his own law practice with offices in Pennsylvania and New Mexico. The Firm specializes in Corporate Law, Trust Law and Commercial Litigation. Contact information is located on the Firm's website at http://www.nm-ny-pa-law.net.

.