

**EIGHTEENTH ANNUAL  
NORTHEAST SURETY AND FIDELITY  
CLAIMS CONFERENCE**

**SEPTEMBER 27<sup>th</sup> and 28<sup>th</sup>, 2007**

**FUNDAMENTALS OF ELECTRONIC DISCOVERY  
AND THE NEW FEDERAL RULES**

**PRESENTED BY:**

**KIM McNAUGHTON, ESQUIRE  
LIBERTY BOND SERVICES  
MICHAEL A. STOVER, ESQUIRE  
WHITEFORD, TAYLOR & PRESTON, LLP  
7 Saint Paul Street, Suite 1900  
Baltimore, Maryland 21202**

**CURTIS E. FALANY, P.E.  
FORCON INTERNATIONAL  
1216 Oakfield Drive  
Brandon, Florida 33511**

**FUNDAMENTALS OF ELECTRONIC DISCOVERY**  
**AND THE NEW FEDERAL RULES**

By  
Michael A. Stover, Esquire  
Curtis E. Falany, P.E.  
Kim McNaughton, Esquire

**A. Introduction**

Discovery of electronically stored information has been an issue for decades, but there has been renewed interest in the topic of late due in large measure to the 2006 amendments to the Federal Rules of Civil Procedure which became effective on December 1, 2006. The issue has also risen in stature because of some recent high profile cases signaling the courts' willingness to tackle the issues and the general fact that electronic technology has become so fully integrated with how we live and work that discovery of electronic information has become a necessity instead of mere theory.

Studies have shown that since the advent of computers, the vast majority of all new information is created and stored in electronic format. Much of that information is never reduced to printed form. In the year 2006, an estimated 2 trillion e-mails were sent in the United States, and it is believed that approximately 2.7 trillion e-mails will be sent in the United States in 2007. A May 2007 survey revealed that the average employee sends and receives more than 135 e-mails per day. Thus, a company with 500 employees would generate nearly 17.5 million emails a year.<sup>1</sup> The amount of electronic data that can be stored in a small space is astounding. A compact disk can contain up to 325,000 pages of information, or about 125 banker boxes of material. One gigabyte, which is the standard unit of measure for most personal computers today, is equivalent to 500,000 typewritten pages. A typical desktop computer today has over 100 gigabytes of information, which represents the storage capacity of over 60,000,000 pages of paper documents – approximately 125,000 banker boxes of paper.

Not only is the vast majority of information created and stored electronically and such information comprises a huge volume of information, a recent study demonstrates that most organizations are not properly prepared to deal with this volume of information in a litigation context. According to a recent of 400 IT managers:

- 1 in 3 organizations surveyed are not familiar at all with the requirements of the newly amended federal rules;
- More than half of the survey respondents admit that they are “not prepared” to meet the new requirements under the federal rules;
- More than half of the organizations surveyed have not developed an e-discovery plan that has been prepared by counsel;

---

<sup>1</sup> Osterman Research, Inc., Survey of 400 IT managers and organizations, (May 2007).

- E-discovery requests are so painful that dealing with the IRS was the only activity respondents found more unpleasant;
- More than half of IT managers admit that they would rather have a cavity filled than respond to an e-discovery request.

Osterman Research, Inc., Survey of 400 IT Managers and Organizations (May 2007).

This paper will address where and how electronic information is created and stored and provide some insight on how networks operate, how the internet operates and a glossary of relevant terms. With that background in hand, the paper will next address the changes that have been made in the federal rules and the impact that those changes will have on how business is conducted and how law is practiced. Some of the key issues which will be discussed include: Reasonable Accessibility/Undue Burden and Cost; Routine operation/good faith exception; Duty to Preserve Information; Litigation Holds; Production Of Electronic Information – Who Bears The Costs; Production of Metadata and Spoliation Of Electronic Information. Finally, the paper will conclude with a few practical tips.

## **B. Understanding Electronic Information – What Is Out There And Where Is It?**

### 1. A Glossary of e-Discovery and electronic information terms

Before diving into the world of electronic bits and bytes it is helpful to set forth a glossary of the relevant terms and acronyms.

**ACTIVE DATA** Active data is information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without restoration or reconstruction.

**BACKUP DATA** Backup data is an exact copy of system data that serves as a source for recovery in the event of a system problem or disaster. Backup data is generally stored separately from active data on portable media.

**BIOS** Basic Input/Output System - the firmware programs written into memory and stored on the motherboard of a computer that control its basic operations.

**CD-ROM** Compact Disk - Read Only Memory - a method for using Compact Disks to store binary data for use with a computer.

**ENTROPY** The measure of disorder in a system. For our purposes, the information in a storage device is not permanent. The 2<sup>nd</sup> law of thermodynamics predicts that all stored information will eventually be lost.

ETHERNET	A local area network (LAN) protocol. A packet based protocol for delivering data inside a network (LAN.) Possible the most popular such protocol in use today.
ESI	Electronically Stored Information-
IMAP	Internet Mail Access Protocol - a mail protocol that provides for the management of received e-mail messages on a mail server.
IP	Internet Protocol - a packet based protocol for delivering data across networks.
IPv4	Internet Protocol version 4 - the current version. It allows for some 4 billion addresses. However for technical reasons, many of them cannot be used.
IPv6	Internet Protocol version 6 - the next version. It allows for virtually unlimited addresses. But then, they said that about IPv4.
INTERNET	A network of computer networks that operates worldwide.
LAN	Local Area Network - a computer network restricted in geographical area. LANs are often defined as a network sharing the same router.
LEGACY DATA	Legacy data is information that an organization has created or stored by the use of software and/or hardware that has become obsolete or which has been replaced by a different operating system and/or hardware.
MAN	Metropolitan Area Network - a computer network that covers a larger geographic area such as a city. A MAN can be comprised of many LANs.
MDA	Mail Delivery Agent - a mail server that accepts incoming e-mail messages and stores them for retrieval by recipients.
METADATA	Metadata is information about a particular data set or document that describes how, when and by whom it was collected, created, accessed, modified and how it is formatted.
MTA	Mail Transport Agent - a mail server that accepts e-mail messages for forwarding to another server.
MTU	Magnetic Tape Unit - a device for reading and writing electronic data on magnetic tapes.
NAS	Network Attached Storage - Hard Drives or Tape Drives designed to

attach directly to a network rather than through a server or host.

- NATIVE FORMAT** Electronic documents have an associated file structure defined by the original creating application. This file structure is the document's native format.
- PDF** Portable Document Format (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 like a picture of the document.
- POP3** Post Office Protocol 3 - a mail protocol that provides for the delivery of e-mail messages to a recipient's e-mail client
- RAID** Redundant Array of Inexpensive Disks - a means of logically storing data on arrays of multiple hard disk drives to improve performance and fault tolerance.
- RAM** Random Access Memory - a means of storing memory in such a way that all locations are equally accessible.
- ROUTER** A device for determining the routes digital information takes between networks.
- SAN** Storage Area Network - A network designed to attach storage devices such as hard disk drives and tape drives to a server.
- SMTP** Simple Mail Transport Protocol - a mail protocol that provides for the forwarding of e-mail messages between mail servers.
- TIFF** Tagged Image File Format (TIFF) is identified by its .tif extension. Images are stored in tagged fields and programs use the tags to accept or ignore fields, depending on the application.
- VLAN** Virtual Local Area Network - a technique that allows computers to behave as if they are on a single physical LAN even when they are widely separated physically.
- VPN** Virtual Private Network - a communications protocol that supports VLANs.
- VOLATILE** A volatile memory device requires a continuous source of electrical energy to retain stored data. An example would be the RAM memory in a desktop computer. A non-volatile memory will retain stored data indefinitely without such a source. An example would be a floppy disk

drive.

WAN Wide Area Network - A still larger network comprised of multiple LANs and MANs.

## 2. Where and How can Electronic Data be Stored

It is interesting to note that the industry does not yet have a standard definition of 'Electronic Stored Information' or ESI. An Internet search of Electronic Stored Information and Federal Government produces nearly 2 million hits. A simple definition of ESI might be: information that is stored in an electronic form. For the purposes of this paper, the definition will be: information that is stored, recovered, processed, or transmitted electronically. This is not a meaningless distinction. Consider the following examples of storage devices:

Thumb Drive or Flash Memory - information is stored electronically as an electric charge.

Hard or Floppy Disk - information is stored magnetically as changes in a magnetic field.

CD Rom - information is stored mechanically (or optically) as a series of microscopic holes or pits in an aluminum film.

The common thread is that all of these devices store information and none of it is directly legible to a human. All of these devices require electronics to read and to recover the stored information and to present it in a human legible format. Consider another storage device: Paper - information is stored mechanically (or optically) as change in reflectivity on a uniform background. Information stored on paper may be human legible, this writing for example. Other information on paper, bar codes for example, may not be human legible. Consider that all of the above noted storage devices are non-volatile and can be physically removed from a computer system. For the sake of the focus of this writing, we will not consider where these devices, and the ESI they contain, might be physically located when not connected to their respective computer systems.

### (a) Topology of a Network

There are several commonly used terms for computer networks. From the smallest to the largest, they are commonly called: LAN, MAN, WAN, and Internet. The LAN is typically comprised of computer workstations, servers, and auxiliary devices such as printers located in one geographical area and physically or logically separated from other networks by a router. In a typical operation, the LAN uses the ethernet protocol to pass data between the various computers, servers, printers, routers, and other devices on the LAN. In more recent times, both wired (copper wire or fiber optic based) LANs and wireless (radio based) LANs have become popular.

MANs, WANs, and the Internet are progressively larger 'networks of networks (LANs) with the largest, the Internet, covering the entire world. In addition to LANs which are based on physical locations, there are virtual LANs (VLANs) where the LAN is based on something other than physical location, such as a business relationship. *VLANs can allow a computer in your office to treat a server or printer half-way around the world just as if it were in the office next to yours.*

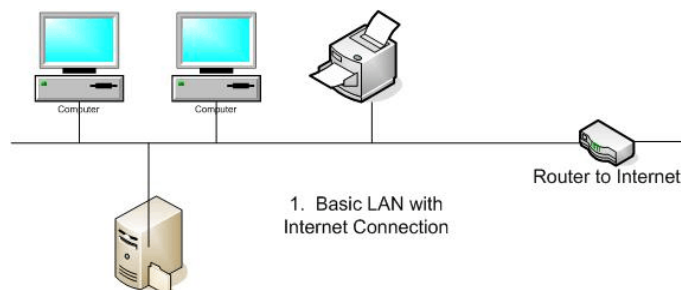
(b) Understanding the Internet

The Internet is controlled anarchy. It had its beginnings in a government project where resources needed to be shared across the country. It is managed by a number of boards and committees, some created by governments and some by the users themselves. Standards can be created by a committee, by one company or a group of companies, with technical might or marketing prowess, or by groups of users. All in all, the Internet works because the users are willing to cooperate to make it work.

Internet Protocol (IP) is the basic addressing system for the Internet. It is administered in the U.S. and North America by the American Registry of Internet Numbers. The present system, called IPv4 uses four octets of address space (32 bits) ranging in value from 000.000.000.000 to 255.255.255.255, but not every value in this range can be used. Certain address values are sacrificed to make the IP work and others are reserved as private. Private addresses are not recognized by the Internet and cannot therefore be routed. Even though this is an extremely large number, the world is rapidly running out of IP addresses. The Internet Systems Consortium report dated January 2007 showed 433,193,199 named computers in the Internet Domain Name System. The July 9, 2007 issue of Network World estimated 1.1 billion computers connected to the Internet world-wide. A new version of the Internet Protocol, IPv6, with greatly expanded address space is "in the works."

(i) A Simple LAN

To understand the Internet, we will start with the smallest division, the LAN. In this example, a Basic LAN with Internet Connection, there are two desktop computers, a file server, a printer, and a router which connects to the Internet.

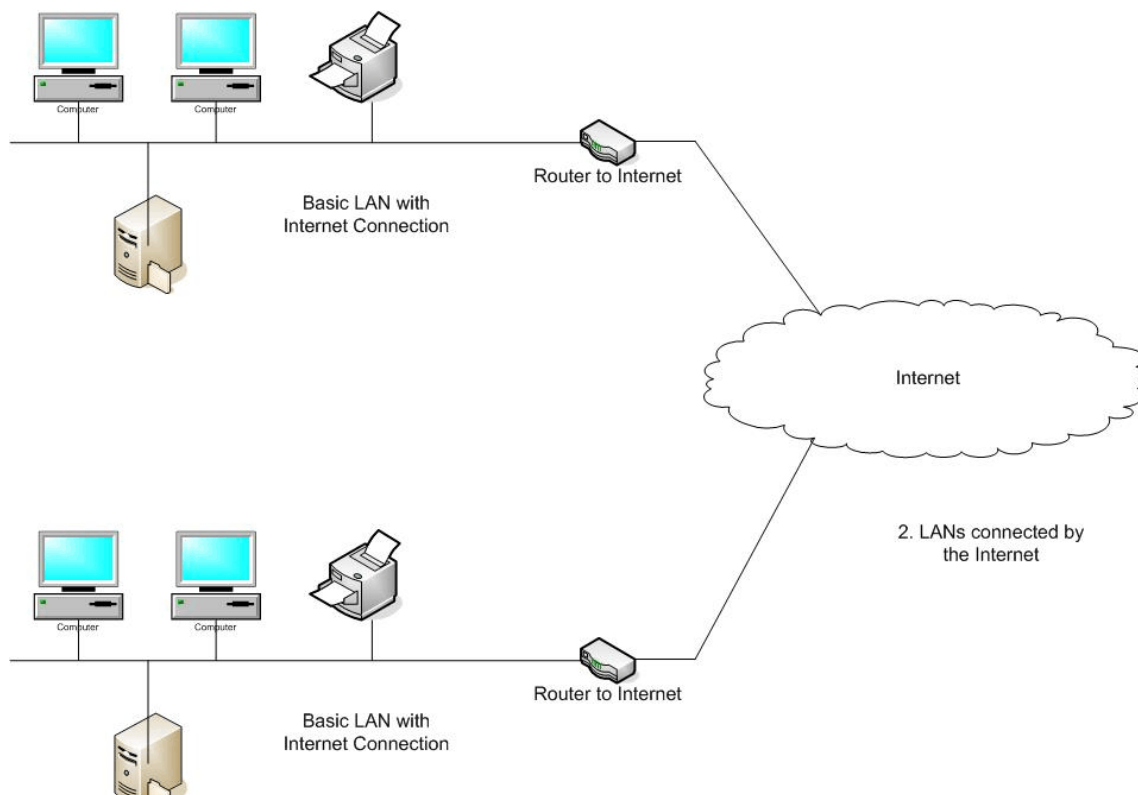


Internal to the LAN, data flows between the computers, printers, file server, and router using the ethernet protocol. Devices on the LAN are addressed in an IP address space called a netblock. The IP protocols are designed so

that the router knows which devices are connected to the LAN and which are not. If the router detects a data packet not addressed to the LAN, it searches for a path through the Internet to another router that can deliver the packet to its LAN. There are numerous other protocols and address schemes used on networks. However, the Internet runs on IP so for the sake of brevity, we will consider only IP and ethernet.

(ii) A Simple Internet

Using IP and ethernet protocols, a device on the LAN can determine that it is attempting to send a data packet to an IP addressed device that is not on its LAN. The IP device will then send its data packet to a gateway device, in this example an IP router, for delivery. The IP router then contacts its peers in the Internet to locate a path to the device with the desired address. Once that device, or another router with a path to the device, is located, the router forwards the packet through the Internet.



(iii) Complex Internet

Imagine, if you would, the Internet 'cloud' covering the entire earth. Then imagine the number of computer, servers, routers, home networks, office networks,

wireless networks, PDAs, refrigerators, cell phones, etc. connected to it. The sheer size of the Internet boggles the mind. And it is growing...

Using illustration #2, the Internet works in such a way that, in theory, every device can be connected to every other device. ESI (data) can be stored on any device connected to the Internet or connected to a LAN connected to the Internet. *It is important to note that not all networks are connected to the Internet.*

(c) Types of Physical Storage Devices and Media that Store Electronic Data

An Incomplete List of Physical Storage Devices

- Disk Drive (DD)
- Hard Disk Drive (HDD)
- Removable Disk Drive (RDD) - i.e. Zip disk
- Floppy Disk Drive (FDD)
- Compact Disk Drive (CDD or CD-ROM)
- Digital Video Disk (DVD)
- Optical Disk Drive - similar to the CDD except larger and often proprietary.
- Tape Drive (MTU)
- Flash Memory and Flash Drives (Thumb Drives, Travel Drives, BIOS)
- Random Access Memory (RAM)

An Incomplete List of Logical Storage Devices

- Redundant Array of Inexpensive Disks (RAID)
- Storage Area Network (SAN)
- Network Attached Storage (NAS)
- File Server

Other Potential Storage Locations

- Print Server
- Mail Client
- Personal Digital Assistant (PDA)
- Cell Phone
- Mail Server, including Mail Transport Agents and Mail Delivery Agents
- Exchange Server
- Hardware Buffer - Devices such as Fax Machines, Copiers, Scanners, and Printers have hardware buffers.
- Routers
- Firewalls
- Intrusion Detection Systems (IDS)
- Tape Libraries
- CD or DVD Libraries

## Removable Disk Libraries

### (d) Making Electronic Data Human Legible

Writings that were made and stored mechanically thousands of years ago are still human legible today. Such writings were made on rocks, clay tablets, papyrus scrolls, and copper plates. They can be found today on the walls of tombs in Egypt and in caves near the Dead Sea. Translations can be difficult and somewhat inaccurate but still, humans can read it.

### Legacy Data - Old and/or Obsolete Hardware

Data stored on a disk drive or tape drive 40 years ago can be another matter entirely. The necessary hardware and software to read the hard disk may not exist or may be difficult to obtain. The software may only run on a specific operating system that is obsolete. The computer hardware to run the operating system may no longer exist.

The barriers to recovering data written or stored with older hardware is one that can be solved by the application of large amounts of money and engineering time. As a rule, anything that was invented can be reinvented. As long as the basic information on the original recording and the playback techniques and equipment exists, the hardware system can be recreated and the data recovered.

### Legacy Data - Old and/or Obsolete Software

There can also be problems with recovering ESI. The ESI may have been encrypted and the original keys, or for that matter, the original decryption software may have been lost. The ESI may have been written in an unknown file structure or a database format or protocol that is unknown or no longer available.

### Encryption

Recovering encrypted ESI is also possible. However, the amount of computing power required and the time required to apply it, can be so great as to completely overwhelm any potential value of the ESI itself. For instance, several encryption methods in wide use today can be 'cracked' by the direct application of significant computing power for a time period of 100 years or so. Although such encryption is not perfect, it is very useful for ESI which will lose all value before it can be recovered. *Please note: The Federal Government, from time to time, attempts to legislate a mandatory escrow of all (public) encryption keys generated in the US. The present status of such efforts is unknown to this author.*

## A Mostly Fictitious Example of Barriers to ESI Recovery

World Wide Widgets, Inc. failed in business. On the day of its failure, the employees shut down the company file and mail servers as usual and left the building for the last time. Security guards confiscated all name badges, paperwork, storage media, etc. from the employees as they left the building.

Shortly after that event, the forensic investigators arrived to secure the company ESI. What they found on arrival was all doors, including the security doors to the server room, were standing open. Paper was strewn everywhere. Most of the computer hardware was still in the server room but all documentation, backup tapes and disks, logs, or any other items that weren't bolted to the floor or wall were gone or spread over the building. The investigators reviewed the items collected by the security and found little of use. The investigators interviewed the employees who testified that they followed normal procedures and locked the server room door as they left. The investigators decided to focus on the recovery of the company books. The hard disk drives were removed from the servers and image copied (twice.) The original servers, which were never powered up, were impounded by the Court. One image copy was set aside as evidence. The second was installed, in a read-only mode, in a host computer and inspected. The drive was found not to be encrypted. However, it contained a data base of unknown properties in a format compatible with Microsoft NT. Further inspection of file headers and legible (text) files contained in the data base, determined that the data base contained company financial records. Further, the files appeared to have been maintained in a proprietary data base, by a software package called Tricky Financial Software manufactured by TFS, LLC. No copies of installation software or licenses were ever discovered. There was some doubt that legal software licenses were ever obtained. After some effort, it was determined that TFS, LLC was previously located in Denver and was no longer in business. With luck and a lot of Internet searches, a successor company to TFS, LLC was found in Tampa, Florida. That successor company offered to convert the TFS software to be compatible with their latest financial package together with a license to use their software, for a fee of \$20,000. This information was passed to the Client and further efforts to recover the company records from the server were not funded.

### **C. The New Federal Rules**

As of December 1, 2006, the Federal Rules of Civil Procedure were amended to give greater guidance to courts and litigants in dealing with electronic discovery issues. There are four key areas of change to the Rules that address electronic discovery: early attention to e-discovery issues; the role of accessibility; the form of production; and sanctions. *W.E. Aubuchon Co., Inc., v. Benefirst, LLC*, 2007 U.S. Dist. LEXIS 44574 at \*7 (D.Mass. 2/6/2007).

## 1. Rule 26(a)(1)(B) – Initial Disclosures

Rule 26(a) sets forth the general provisions governing discovery and includes the requirements for initial disclosures. Unless a local opt-out rule or specific court order applies, the initial disclosures must be made even before a discovery request is presented and frequently occur at the very initial stages of a case filed in federal court. Amended Rule 26(a)(1)(B) requires that in the initial disclosures, a party must provide to the other parties a copy or description of “electronically stored information” that may be used to support its claims or defenses in the case. This change merely clarified what courts have held over the past decades, i.e. that documents subject to discovery include electronically stored documents. Requiring the disclosure at the outset of the case points out counsel’s corresponding obligation to investigate the client’s electronic information system to determine where and how potential information is created, stored and how such information is deleted. This is an obligation which courts are increasingly taking very seriously and which can have far reaching and potentially expensive and disastrous consequences for counsel and clients who choose to ignore the obligation.

## 2. Rule 26(b)(2)(B) – Reasonable Accessibility/Undue Burden and Cost

Federal Rule 26(b)(2)(B) was amended to provide:

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

Fed. R. Civ. P. 26(b)(2)(B).

The amendment was designed to address issues raised by difficulties in locating, retrieving, and providing discovery of some electronically stored information. Fed. R. Civ. P. 26(b)(2), advisory committee note (2006 amendments). Rule 26(b)(2) contemplates that a party will produce all electronic information that is relevant, not privileged and *reasonably accessible*. The producing party must then identify by category or type the sources containing potentially responsive information that it is neither searching nor producing. The advisory committee note states that “the identification should provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.” *Id.* Of course, the fact that a producing party may determine that information is not reasonably accessible, does not alter the fact that the producing party is still under the obligation to *preserve* such information as discussed later herein. If the parties cannot agree voluntarily on the production of information designated as “inaccessible,” a motion to compel or motion for protective

order is required. The party asserting inaccessibility has the burden of proving that the information is not reasonably accessible because of undue burden or cost. The party seeking production has the burden of proving that the need for the discovery outweighs the burden and cost of production.

In *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003)(*Zubulake I*), the court addressed the issue of accessibility of electronically stored information and found that the time and expense required to retrieve documents and electronic data depends primarily on the format and media on which the data is maintained. *Zubulake I* at 318. The *Zubulake I* Court broke down electronic data into the following five categories, listed in order of most accessible to least accessible: (1) active on-line data - hard drives, for example; (2) near-line data – typically, storage devices such as optical disks; (3) offline storage/archives - removable optical disks or magnetic tape media which can be labeled and stored in a shelf or rack; (4) backup tapes - devices like tape recorders that read data from and write it onto a tape; they are sequential access devices which are typically not organized for retrieval of individual documents or files; and (5) erased, fragmented or damaged data - such data can only be accessed after significant processing. *Id.* at 318-319.

Generally, the first three categories of data are considered "accessible" and the last two categories are considered "inaccessible." That the data is deemed "accessible" does not mean it is readily obtainable, the time it takes to actually access such data may range from milliseconds to days; however, the key to accessibility is that the data does not need to be restored or otherwise manipulated to be usable. *Id.*, at 320. The *Zubulake I* Court further observed that "inaccessible data," on the other hand, is not readily usable. Backup tapes must be restored ... fragmented data must be defragmented, and erased data must be reconstructed; such efforts make such data inaccessible. *Id.*

Courts grappling with the question of whether the information is reasonably accessible may require focused discovery on the issue and can order a sampling of the information to determine the burden, cost and importance of the information. Ultimately, Rule 26(b)(2)(B) permits the court to order production of electronically stored information even if it is not reasonably accessible upon the showing of good cause. The advisory committee note to amended Rule 26(b)(2)(B) identifies several specific factors that the court should take into account before it orders discovery from sources that are not reasonably accessible. It states:

The decision whether to require a responding party to search for and produce information that is not reasonably accessible depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified in the circumstances of the case. Appropriate considerations may include: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;

(4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

Fed. R. Civ. P. 26, advisory committee note (2006 amendments).

In *Disability Rights Council Of Greater Washington v. Washington Metropolitan Transit Authority*, 2007 U.S. Dist. LEXIS 39605 (D.D.C. 6/1/2007), the United States District Court for the District of Columbia applied new rule 26(b)(2)(B) in the context of a motion to compel the defendant, Washington Metropolitan Transit Authority (WMATA), to restore electronically stored data from backup tapes and produce the electronic information in TIF format. WMATA failed to implement a "litigation hold" and did not properly instruct its employees to retain potentially responsive electronic documents, even after the litigation was filed, and, as a result, nothing was done to stop WMATA's email system from automatically obliterating all emails after sixty days. The WMATA system also recycled the daily backup tapes every seven days and the weekly backup tapes every forty-five days, which resulted in the destruction of that backup data. There were, however, monthly backup tapes which contained a snapshot of the network system on the date of the backup and these tapes were retained.

Plaintiffs proposed that the backup tapes be restored so that, once rendered searchable, their contents could be searched by a keyword analysis to find the emails of several key persons. WMATA opposed the restoration process on the grounds of burden and expense, insisting that the backup tapes are not reasonably accessible and there is little reason to believe that they will produce relevant information. In addressing WMATA's argument, the Court noted that Rule 26(b)(2)(B) permits a court to order discovery from sources that are not reasonably accessible upon a showing of good cause and after considering the limitations of Rule 26(b)(2)(C). The Court applied the relevant factors noting that Plaintiffs were physically challenged citizens who need the access to public transportation; that access to public transportation by person with physical disabilities to work and enjoy their lives with their fellow citizens was a crucial concern of the community and that Plaintiffs had no substantial financial resources and the law firm representing them was proceeding pro bono. The Court also noted that the Plaintiff's request was specific and narrowly tailored and there was absolutely no other source from which the electronically stored information could be secured as a result of WMATA's failure to impose a litigation hold. Accordingly, the Court found sufficient cause to order the search of the backup tapes.

In *W.E. Aubuchon Co., Inc., supra.*, the Court held that even though the electronic information was stored on a server which was searchable and therefore accessible, the manner in which the data was stored made the data inaccessible for purposes of Rule 26. Over the relevant time period an estimated 550,000 to 600,000 claims were stored on the server; however, The search process for retrieving the claims was complicated by the fact that there was no index of images. The images were

stored on the server first, according to year of processing, then by claims examiner, then by the month of processing, and finally by the actual processing date. The system was not set up for the wholesale retrieval of claim images on a group by group basis. Although the Court expressed its misgivings about a system of storage that seemed designed to discourage searching, it nevertheless found that the retrieval of the records would be costly and unduly burdensome, thus making the data inaccessible. Ultimately, after applying the Rule 26 factors, the Court ordered the production of the data even though it was in an inaccessible format with the producing party to bear the costs.

Most authorities hold that backup tapes are not reasonably accessible for purposes of Rule 26. But the question of whether information contained on those backup tapes will be produced or not depends on the unique nature, facts and circumstances of each case. For a producing party to oppose production of such inaccessible data a strong and detailed showing of the costs and burdens of producing such data must be made. Courts will no longer permit a bald allegation of undue burden or cost to suffice. The producing party must explain the specific limitations it faces, whether it is dealing with data that was stored from an obsolete system or software that is no longer in use, whether the data is readily searchable or indexed, the impact restoring the inaccessible data will have on the ongoing operations of the party's business, the hours required to restore the data, the amount of data that is stored and the likelihood that the data is not relevant to the other party's search. The new rules and recent decisions provide courts with a framework from which to evaluate the issue and the parties need to be familiar with that framework in order to fully evaluate and respond.

### 3. Rule 26(b)(5)(B) – Privilege Procedure

Amended Rule 26(b)(5)(B) provides:

Information Produced. If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

Fed. R. Civ. P. 26(b)(5)(B).

This amendment to the Rule was added in response to repeated concerns raised by litigants and counsel that the risk of privilege waiver and the work necessary to avoid it significantly adds to the costs and delay of discovery. The costs and delays are

particularly burdensome when the review is of electronically stored information because of the sheer volume and the difficulty in ensuring that all information to be produced has in fact been reviewed. While the procedure has been added to the Rule, the advisory committee cautions that the amendment does not address whether the privilege or protection that is asserted after production has or has not been waived by the production. The courts have developed principles to determine whether, and under what circumstances, waiver results from inadvertent production of privileged or protected information. Fed. R. Civ. P. 26, advisory committee note (2006 amendments).

Rule 26(b)(5)(B) provides a procedure for presenting and addressing the privilege and waiver issues. The Rule is designed to work together with Rule 26(f), which is amended to direct the parties to discuss privilege issues in preparing their discovery plan. By the plain terms of the Rule, a party asserting a claim of privilege or protection after production must give notice to the receiving party. The notice contemplated by the Rule should be in writing unless the circumstances preclude it, such as during a deposition. The notice should be as specific as possible in identifying the information and stating the basis for the claim so that the receiving party can determine whether to challenge the claim and may sequester the information and submit it to the court for a ruling.

#### 4. Rule 26 (f) – Discovery Planning

Rule 26(f) is amended to direct the parties to discuss discovery of electronically stored information during the discovery-planning conference. The rule focuses on "issues relating to disclosure or discovery of electronically stored information"; the discussion is not required in cases not involving electronic discovery. When a case involves discovery of electronically stored information, the issues to be addressed during the Rule 26(f) conference depend on the nature and extent of the contemplated discovery and of the parties' information systems. Indeed, the rule envisions that one of the topics of discussion might be the electronic storage systems employed by each party so that the discovery plan takes into account the capabilities and limitations of the various systems. This Rule again points out the necessity of counsel's becoming familiar with those systems early in the case.

The particular issues regarding electronically stored information that deserve attention during the discovery planning stage depend on the specifics of the given case but generally may include: the identity of the various sources of electronically stored information within a party's control that should be searched and whether the information is reasonably accessible to the party that has it, including the burden or cost of retrieving and reviewing the information. Rule 26(f)(3) explicitly directs the parties to discuss the form or forms in which electronically stored information might be produced, which ties into the Rule 34(b) amendments to permit a requesting party to specify the form or forms in which it wants electronically stored information produced. Rule 26(f) is amended to direct the parties to discuss any issues regarding preservation of discoverable information during their conference as they develop a discovery plan. Rule 26(f) is also amended to provide that the parties should discuss any issues relating

to assertions of privilege or of protection as trial-preparation materials, including whether the parties can facilitate discovery by agreeing on procedures for asserting claims of privilege or protection after production and whether to ask the court to enter an order that includes any agreement the parties reach. Parties may attempt to minimize costs associated with privilege protection by agreeing to protocols designed to minimize the risk of waiver. Specifically, the parties may agree that the responding party will provide certain requested materials for initial examination without waiving any privilege or protection -- sometimes known as a "quick peek." The requesting party then designates the documents it wishes to have actually produced. The parties may enter an agreement -- sometimes called a "clawback agreement," in which production is made without intent to waive any privilege or protection so long as the responding party identifies the documents mistakenly produced. Under such an agreement, the inadvertently produced documents are to be returned.

#### 5. Rule 33(d) – Option to Produce Electronic Information

Under the amendment to Rule 33(d), explicit language in the Rule ensures that where an answer to an interrogatory may be derived from business records, electronically stored information is included under business records. Rule 33(d) is designed to parallel Rule 34(a) by "recognizing the importance of electronically stored information."

Special difficulties may arise in using electronically stored information, either due to its form or because it is dependent on a particular computer system. Rule 33(d) allows a responding party to substitute access to documents or electronically stored information for an answer only if the burden of deriving the answer will be substantially the same for either party. Rule 33(d) states that a party electing to respond to an interrogatory by providing electronically stored information must ensure that the interrogating party can locate and identify it "as readily as can the party served," and that the responding party must give the interrogating party a "reasonable opportunity to examine, audit, or inspect" the information. Depending on the circumstances, satisfying these provisions with regard to electronically stored information may require the responding party to provide some combination of technical support, information on application software, or other assistance. The key question is whether such support enables the interrogating party to derive or ascertain the answer from the electronically stored information as readily as the responding party. A party that wishes to invoke Rule 33(d) by specifying electronically stored information may be required to provide direct access to its electronic information system, but only if that is necessary to afford the requesting party an adequate opportunity to derive or ascertain the answer to the interrogatory. In that situation, the responding party's need to protect sensitive interests of confidentiality or privacy may mean that it must derive or ascertain and provide the answer itself rather than invoke Rule 33(d).

#### 6. Rule 34 – Production of Documents

Rule 34(a) is amended to reference electronically stored information to confirm that discovery of electronically stored information stands on equal footing with discovery

of paper documents. The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. A Rule 34 request for production of "documents" should be understood to encompass, and the response should include, electronically stored information. Fed. R. Civ. P. 34, advisory committee note (2006 amendments).

Discoverable information often exists in both paper and electronic form, and the same or similar information might exist in both. The items listed in Rule 34(a) show different ways in which information may be recorded or stored. Images, for example, might be hard-copy documents or electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments. Rule 34(a) requires that, if necessary, a party producing electronically stored information translate it into reasonably usable form. Rule 34(a)(1) was also amended to make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying. That opportunity may be important for electronically stored information.

The amendment to Rule 34(b) permits the requesting party to designate the form or forms in which it wants electronically stored information produced. Specification of the desired form or forms may facilitate the orderly, efficient, and cost-effective discovery of electronically stored information. The rule recognizes that different forms of production may be appropriate for different types of electronically stored information - word processing documents, e-mail messages, electronic spreadsheets, different image or sound files, and material from databases. The rule does not require that the requesting party choose a form or forms of production. The responding party also is involved in determining the form of production. In the written response to the production request that Rule 34 requires, the responding party must state the form it intends to use for producing electronically stored information if the requesting party does not specify a form or if the responding party objects to a form that the requesting party specifies. A party that responds to a discovery request by simply producing electronically stored information in a form of its choice, without identifying that form in advance of the production in the response required by Rule 34(b), runs a risk that the requesting party can show that the produced form is not reasonably usable and that it is entitled to production of some or all of the information in an additional form. If the requesting party is not satisfied with the form stated by the responding party, or if the responding party has objected to the form specified by the requesting party, the parties must meet and confer under Rule 37(a)(2)(B) in an effort to resolve the matter before the requesting party can file a motion to compel.

If the form of production is not specified by party agreement or court order, the responding party must produce electronically stored information either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable. Rule 34(a) requires that, if necessary, a responding party "translate" information it produces into a "reasonably usable" form. Under some circumstances,

the responding party may need to provide some reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information. The rule does not require a party to produce electronically stored information in the form in which it is ordinarily maintained, as long as it is produced in a reasonably usable form. But the option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation.

Some electronically stored information may be ordinarily maintained in a form that is not reasonably usable by any party. One example is "legacy" data that can be used only by obsolete systems. The question of whether a producing party should be required to convert such information to a more usable form, or should be required to produce it at all, should be addressed under Rule 26(b)(2)(B) and the analysis applicable to inaccessible data.

## 7. Rule 37 – Sanctions

The 2006 amendments to Rule 37 adds new section (f) which provides:

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

Fed. R. Civ. P. 37(f).

The amendment was designed in recognition of the fact that, “many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. As a result of the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part.” Fed. R. Civ. P. 37, advisory committee note (2006 amendments). The advisory committee defines “routine operation” as, “the ways in which such systems are generally designed, programmed, and implemented to meet the party’s technical and business needs,” which may involve the “alteration and overwriting of information, often without the operator’s specific direction or awareness, . . .” Id.

### (a) Routine operation/good faith exception

While the 2006 amendment to Rule 37 indicates that a court may not impose sanctions, absent “exceptional circumstances,” where electronically stored information was lost due to the routine, good-faith operation of an electronic information system, it is clear that this Rule does not exempt a party who fails to affirmatively intervene to stop

the operation of a system that is obliterating information that may be discoverable in litigation. The advisory committee note to Rule 37 states:

[Rule 37(e)] applies to information lost due to the routine operation of an information system only if the operation was in good faith. Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case. The good faith requirement of [Rule 37(e)] means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold."

Fed. R. Civ. P. 37, advisory committee note (2006 amendments).

Thus, in order to take advantage of the good faith exception, a party needs to act affirmatively to prevent the system from destroying or altering information, even if such destruction would occur in the regular course of business. In *Doe v. Norwalk Community College*, 2007 U.S. Dist. LEXIS 51084 (D.Conn. 7/16/07), the Court held that because the defendants failed to suspend the document retention policies which resulted in destruction of relevant data the defendants could not take advantage of Rule 37(f)'s good faith exception. The *Norwalk* Court also observed that, Rule 37(f) only applies to information lost due to the routine operation of an electronic information system and defendants failed to establish that they had such a system in place. Indeed, testimony revealed that the defendants did not appear to have one consistent, "routine" system in place, and they did not consistently follow the policies that did exist.

(b) Duty to Preserve Information

Identifying the boundaries of the duty to preserve involves two related inquiries; first, *when* does the duty to preserve attach, and second, *what* evidence must be preserved? *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 ("Zubulake IV"). As Judge Scheindlin summarized in *Zubulake IV*, "[t]he scope of a party's preservation obligation can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Id.* at 218.

(i) When The Duty To Preserve Attaches

The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when the party should have known that the evidence

may be relevant to future litigation. *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998); *Fujitsu Ltd. v. Fed. Express Corp.*, 247 F.3d 423, 436 (2d Cir.), cert. denied, 534 U.S. 891, 122 S.Ct. 206, 151 L.Ed.2d 146 (2001); *Jordan F. Miller Corp. v. Mid-Continent Aircraft Serv.*, 139 F.3d 912 (10<sup>th</sup> Cir. 1998), *Silvestri v. General Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001) and *Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988). Clearly, when a demand letter<sup>2</sup> is received, suit is filed or a discovery request is received a party is on notice to preserve relevant information. The question of when a party “should have known” involves the application of an objective standard that will be heavily dependent on the facts and circumstances of each case. The Court in *Zubulake IV* observed that, “merely because one or two employees contemplate the possibility that a fellow employee may sue does not generally impose a firm-wide duty to preserve.” *Zubulake IV* at 217. Similarly, in *Cache LaPoudre Feeds, LLC v. Land O’Lakes, Inc.*, 2007 U.S. Dist. LEXIS 15277 (D.Colo. 3/2/2007), the Court noted that while some employees of the defendant may have been aware of plaintiff’s trademark at the time an alleged trademark infringement began, such knowledge alone is not sufficient to place a company on notice of impending litigation. *Id.* at \*22 n.6. Of course, it is an undeniable reality that litigation “is an ever-present possibility” in our society. *National Union Fire Insurance Co. v. Murray Sheet Metal Co., Inc.*, 967 F.2d 980, 984 (4th Cir. 1992). Accordingly, the *Cache LaPoudre* Court observed that, “[W]hile a party should not be permitted to destroy potential evidence after receiving unequivocal notice of impending litigation, the duty to preserve relevant documents should require more than a mere possibility of litigation.” *Id.* at \*24, citing *Hynix Semiconductor Inc. v. Rambus, Inc.*, 2006 U.S. Dist. LEXIS 30690, 2006 WL 565893, \*21 (N.D. Cal. 2006).

The test will be would the information, facts and circumstances available at the time to the relevant decision-makers persuade a reasonable person to anticipate that litigation is likely to occur. In *Norwalk Community College, supra.*, the Court examined the question of when the duty to preserve electronic information arose in the context of a Title IX suit. The defendants argued that the duty to preserve did not arise until after the lawsuit was filed. The Court rejected this argument and instead looked back prior to the filing of suit at several events. The first event which the Court considered significant toward triggering the duty to preserve was a demand letter sent by plaintiff’s counsel which clearly indicated an intention to sue. The Court next looked to an early internal meeting that was held between officials of the defendant regarding the operative

---

<sup>2</sup> See *Washington Alder LLC v. Weyerhaeuser Co.*, 2004 U.S. Dist. LEXIS 8756 (D. Or. 2004) (finding that a letter from Washington Alder threatening to sue for antitrust violations put Weyerhaeuser on notice of possible litigation and triggered a duty to preserve documents), compare *Indiana Mills & Manufacturing, Inc. v. Dorel Industries, Inc.*, 2006 U.S. Dist. LEXIS 45637 (S.D. Ind. 2006) (concluding that defendant could not reasonably anticipate litigation after receiving a letter from the patent holder which referred to infringement and the possibility of a negotiated resolution, but made no further threat of a lawsuit); *Claude P. Bamberger International, Inc. v. Rohm and Haas Co.*, 1997 U.S. Dist. LEXIS 22770 (D.N.J. 1997) (in concluding that defendant had not anticipated litigation, noted that plaintiff’s pre-filing correspondence had not threatened litigation, but rather sought a business remedy for perceived business wrongdoing).

incident from which the Court concluded the defendants should have known then that litigation was reasonably likely.

Courts have held that “a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy.” *E\*Trade Secs., LLC v. Deutsche Bank AG*, 2005 U.S. Dist. LEXIS 3021 at \*14 (D.Minn. 2/17/05). Companies have an obligation to evaluate readily available information, facts and circumstances to determine if future litigation is likely and if so, the duty to preserve relevant information will be deemed to have arisen whether the company exercised its obligation or not. A company cannot bury its head in the sand and expect to be protected from the duty to preserve.

Judge Scheindlin, the presiding judge in the influential *Zubulake* decisions, recently observed that some questions that courts may wish to focus on when considering the question of when the duty to preserve information arises include:

1. Did an organization create a process for evaluating the threat of litigation;
2. Was a response team created to assess the threat and report to a responsible decision-maker;
3. Did the decision-maker evaluate the threat in light of prior experience with similar facts and circumstances;
4. Was the threat made by a known or unknown person or entity;
5. Did the threat arise from a regulatory action or criminal proceeding;
6. Did the threat arise from a respected attorney sending a notice to preserve;
7. Did the threat arise from an event such as a plane crash, explosion or accident;
8. Did responsible media coverage alert the company of similar actions involving similar products or issues.<sup>3</sup>

In the context of the surety, there are several events which might potentially serve as a trigger for the duty to preserve information, depending of course on the surrounding facts. Certainly, notice of default of a principal, termination of a principal, demand letters from obligees and/or payment bond claimants would serve to place a surety on notice of potential future litigation. Responses to status letters sent from the surety to an obligee might also act as a trigger. Audits, account reviews and/or updates might reveal information that could arguably give rise to an anticipation of litigation. A request for financing from the indemnitor may also place the surety on notice of potential future litigation depending on the circumstances surrounding the request. Criminal investigations and/or regulatory actions against the principal and/or indemnitors could also signal the potential for future litigation. If the surety decides to

---

<sup>3</sup> Judge S. Scheindlin, S.D.N.Y., *The Ten Most FAQ's in the Post-December 1, 2006 World of E-Discovery*, Federal Judges Association Newsletter, In Camera (Nov. 2006) – FAQ No. 1.

retain outside counsel and/or consultants to investigate a strong argument can be made that the duty to preserve information has arisen.

(ii) What Electronic Information Should Be Preserved

Once the duty to preserve information has arisen, the question becomes, what information must be preserved? "Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, "no." Such a rule would cripple large corporations, . . . As a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation." *Zubulake IV* at 218, *citing Concord Boat Corp. v. Brunswick Corp.*, 1997 U.S. Dist. LEXIS 24068 (E.D. Ark. 8/29/97) and *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery*, cmt 6(h)(Sedona Conference Working Group Series 2003)("Absent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes."). "A party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter." *Zubulake IV* at 218; *see also, e.g., Quinby v. WestLB AG*, 04 Civ. 7406, 2006 U.S. Dist. LEXIS 64531, 2006 WL 2597900 at \*9 (S.D.N.Y. Sept. 5, 2006), *amended on other grounds*, 2007 U.S. Dist. LEXIS 2955, 2007 WL 38230 (S.D.N.Y. Jan. 4, 2007). The duty to preserve extends to any documents or tangible things, as defined by Rule 34(a), including electronically stored information, that were created by individuals "likely to have discoverable information that the disclosing party may use to support its claims or defenses." *Zubulake IV* at 217-18 (fn. omitted) and *Quinby, supra.* at \* 9. Additionally, the duty also includes documents prepared for those individuals, to the extent those documents can be readily identified (e.g., from the 'to' field in e-mails). The duty extends to information that is relevant to the claims or defenses of any party, or which is relevant to the subject matter involved in the action. Thus, the duty to preserve extends to those employees likely to have relevant information -- the so-called 'key players' in the case. *Zubulake IV* at 218 (fns. omitted).

Once the duty to preserve has been triggered, the potential party must not destroy unique, relevant evidence that might be useful to an adversary. While a litigant is under no duty to keep or retain every document in its possession, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request. *See Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 72 (S.D.N.Y. 1991), *quoting William T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443, 1445 (C.D.Cal. 1984).

In recognition of the fact that there are many ways to manage electronic data, litigants are free to choose how the task of preserving data is accomplished. For example, a litigant could choose to retain all then-existing backup tapes for the relevant personnel (if such tapes store data by individual or the contents can be identified in

good faith and through reasonable effort), and to catalog any later-created documents in a separate electronic file. That, along with a mirror-image of the computer system taken at the time the duty to preserve attaches (to preserve documents in the state they existed at that time), creates a complete set of relevant documents. Presumably there are a multitude of other ways to achieve the same result.

It is important to note that the duty to preserve information extends beyond information that the party possesses to information that the party has custody or control over. See *In Re NTL, Inc. Securities Litigation (Gordon Partners v. Blumenthal)*, 2007 U.S. Dist. LEXIS 6198 (S.D.N.Y. 1/30/2007). Under Rule 34(a), parties may request from their adversaries documents, including electronically stored documents, "which are in the possession, custody or control of the party upon whom the request is served." The concept of "control" for purposes of the federal rules has been construed broadly by the courts. See *In re Flag Telecom Holdings, Ltd. Sec. Litig.*, 236 F.R.D. 177, 180 (S.D.N.Y. 2006); *M.L.C., Inc. v. N. Am. Philips Corp.*, 109 F.R.D. 134, 136 (S.D.N.Y. 1986). Under Rule 34, "control" does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action." *Bank of New York v. Meridien Biao Bank Tanzania Ltd.*, 171 F.R.D. 135, 146-47 (S.D.N.Y. 1997) and *Exp.-Imp. Bank of the United States v. Asia Pulp & Paper Co.*, 233 F.R.D. 338, 341 (S.D.N.Y. 2005).

(iii) Litigation Holds

Once the duty to preserve electronic information arises, the potential party and its counsel must take affirmative steps to ensure that the relevant information is in fact preserved. One common technique is to issue a "litigation hold" communication to the key employees of the potential party instructing them to preserve and protect potentially relevant information. It is critical to keep in mind that one of the key employees should be the person in charge of the electronic information system. A litigation hold is essentially the action taken to prevent the destruction of documents once litigation has commenced. The concept is not new, but its utility has become ever more important in the electronic age where, for example, an individual computer may be programmed in the ordinary course to destroy information after a period of time or where, for example, persons using a computer network, who are unaware of the litigation, destroy electronically stored discoverable information. Preventing that destruction requires a litigation hold -- i.e., disabling the automatic deletion feature or communicating to all persons who have the potential to destroy the discoverable information and informing them not to do so.

The litigation hold can come from inside counsel, human resources, management or outside counsel. The American Bar Association Civil Discovery Standards (August 1999), Standard No. 10 "Preservation of Documents" states that, "[w]hen 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 possible consequences for failing to do so." *Id.* Opposing counsel may also send a "preservation letter" to a potential party advising the party to preserve information and courts are also capable of issuing preservation orders. While a litigant certainly may request that an adversary agree to preserve electronic records during the pendency of a case, or even seek a court order directing that this happen, such actions by a party are not required, and a failure to do so does not vitiate the independent obligation of an adverse party to preserve such information.

In *Zubulake IV*, the court noted that once litigation is commenced or a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. In furtherance of the "litigation hold," counsel must affirmatively: become fully aware of the client's document retention policies and data retention architecture; counsel must communicate with "the key players" in the litigation in order to understand how they stored information; counsel must take reasonable steps to monitor compliance with the "litigation hold" so that all sources of discoverable information are identified and searched; and, having identified all sources of potentially relevant information, a party and its counsel are under a duty to retain that information and produce information responsive to the opposing party's requests.

While an attorney is entitled to rely on the assertions of the client, that reliance must be predicated on an investigation undertaken by the attorney and the reasonable conclusions drawn therefrom under the circumstances. Advisory Committee Notes to the 1983 Amendments to Fed.R.Civ.P. 26(g). In *Metropolitan Opera Ass'n, Inc. v. Local 100 Hotel Employees and Restaurant Employees International Union*, 212 F.R.D. 178, 221-224 (S.D.N.Y. 2003) the Court held that defense counsel failed to comply with Rule 26(g) by never adequately instructing defendant as to its overall discovery obligations, by failing to inquire about the client's document storage procedures and capabilities, by failing to implement a systematic procedure for document production or retention, and by failing to ask important witnesses for documents.

While instituting a litigation hold may be an important first step in the discovery process, the obligation to conduct a reasonable search for responsive documents continues throughout the litigation. See Fed.R.Civ.P. 26(e)(2) (a party is under a duty seasonably to amend discovery responses "if the party learns that the response is in some material respect incomplete or incorrect and if the additional or corrective information has not otherwise been made known to the other parties during the discovery process or in writing"). A litigation hold, without more, will not suffice to satisfy the "reasonable inquiry" requirement in Rule 26(g)(2). *Cache LaPoudre Feeds, supra.* at \*55-56. Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents. *School-Link Technologies, Inc. v. Applied Resources, Inc.*, 2007 U.S. Dist. LEXIS 14723 (D.Kan. 2/28/2007). Proper communication between a party and its lawyer will ensure (1) that all sources of relevant information is discovered, (2) that relevant information is retained on a continuing basis; and (3) that relevant non-privileged material is produced to the

opposing party. *Id.* While counsel has a continuing obligation with respect to litigation holds, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data. *The Sedona Conference, Best Practices Recommendations & Principles for Addressing Electronic Document Production*, 44 (2004 Annotated Version) and *Miller v. Holzman*, 2007 U.S. Dist. LEXIS 2987 (D.D.C. 1/17/2007).

At a minimum a litigation hold letter should include the following:

1. A recitation of the corporate commitment to preservation of evidence and reasonable cooperation with judicial/governmental requests (keep in mind that the litigation hold letter will be discoverable and will be viewed by the opposing counsel, the judge and potentially the jury);
2. Reference to the current version of the corporate retention policy;
3. Contact information for designated authorities handling the matter;
4. An explanation of the legal matter at hand;
5. The criteria for identifying potentially relevant information; and
6. Statement that all reasonable efforts must be made to identify and preserve potential evidence, including advising that:
  - a. Electronic information that is subject to the hold cannot be deleted, modified or altered;
  - b. Loading of new software that could materially impact the electronic information subject to a hold should be prohibited;
  - c. Metadata and data that has been deleted but not purged or overwritten must be located and preserved;
  - d. All file and system maintenance procedures which could have an impact on information subject to a hold must be suspended until the data is protected;
  - e. Any hardware that has been removed from active use that may contain relevant information subject to the hold must be protected; and
  - f. Portable or removable electronic storage media with relevant information must be preserved.
7. A detailed, non-exclusive, list of potential media-types or locations in which potential evidence might exist;
8. An explanation of the potential consequences of failure to comply; and
9. The procedure for preserving in place or delivering information to a central repository

The letter should have some return receipt mechanism through which the recipients can acknowledge that they received and intend to comply with the preservation efforts. In considering the contents of a litigation hold letter it should become clear that significant efforts must be made by counsel to understand the client's electronic storage system in advance of issuing such a letter. Courts recognize this fact and are increasingly holding counsel responsible for failing to do so.

(8) Rule 45 – Subpoenas

The Amendment to Rule 45 merely conforms the Rule for subpoenas to the changes in the other discovery rules, related to discovery of electronically stored information. Additionally, the Rule provides greater detail for the production of electronically stored information. In short, the Rule makes clear that the electronically stored information also can be obtained by subpoena.

**D. Production Of Electronic Information – Who Bears The Costs**

Ordinarily, the presumption is that the producing party should bear the cost of responding to properly initiated discovery requests. *Oppenheimer Fund Inc. v. Sanders*, 437 U.S. 340, 358, 57 L. Ed. 2d 253, 98 S. Ct. 2380 (1978); *Murphy Oil USA v. Fluor Daniel*, 2002 U.S. Dist. LEXIS 3196, 2002 WL 246439 (E.D. La. February 19, 2002). However, because of the potentially enormous and costly task of searching for all relevant and unprivileged electronic records associated with broad discovery of electronic records and the minimal threshold requirements of Rule 26(b)(1) for the discoverability of information (a requesting party is entitled to seek discovery of non-privileged information "relevant" to the claims and defenses raised in the pleadings) courts have attempted to fashion reasonable limits that will serve the legitimate needs of the requesting party for information, without unfair burden or expense to the producing party. The precise formulas used by the Courts have varied.

In *McPeck v. Ashcroft*, 202 F.R.D. 31, (D.D.C. 2001), the court adopted a "marginal utility" analysis to determine which party was required to pay the cost of expansive discovery of electronic records. Under this approach, the court must assess the likelihood that the source to be searched will produce information that is relevant to a claim or defense. The greater the likelihood that it will produce relevant information, the fairer it is to require the producing party to bear the expense and *vice versa*. In *Rowe Entertainment v. The William Morris Agency, Inc.* 205 F.R.D. 421 (S.D.N.Y. 2002), the court adopted an eight-factor test to accomplish the task of performing the cost/benefit analysis. The eight factors established in *Rowe* are as follows:

- (1) The specificity of the discovery requests;
- (2) The likelihood of discovering critical information;
- (3) The availability of such information from other sources;
- (4) The purposes for which the responding party maintains the requested data;
- (5) The relative benefit to the parties of obtaining the information;
- (6) The total cost associated with production;
- (7) The relative ability of each party to control cost and its incentive to do so; and
- (8) The resources available to each party.

*Rowe, supra.* 205 F.R.D. at 429.

Not all courts agreed with the approach used in *Rowe* because it has been perceived as permitting too easily the shifting of the expense of production from the producing party to the requesting party. Thus, in *Zubulake v. UBS Warburg, LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) ("*Zubulake III*"), the court crafted a more refined approach. In *Zubulake III*, the Court set forth an analytical framework for determining whether it is appropriate to shift the costs of electronic discovery. The plaintiff in *Zubulake* was a highly-paid investment banker who accused her employer of gender discrimination and illegal retaliation. *Zubulake* claimed that key evidence supporting her claim was located in e-mails that were contained only in backup tapes and sought an order compelling the defendant, UBS Warburg LLC ("UBS"), to produce the e-mails at its own expense. *Zubulake I, supra*, 217 F.R.D. at 311-12. After UBS was ordered to produce the e-mails, the court considered whether cost-shifting was merited.

As a threshold matter, the *Zubulake I* Court stated that "cost-shifting should be considered only when electronic discovery imposes an 'undue burden or expense' on the responding party." *Id.* at 318 (emphasis omitted), *quoting* Fed.R.Civ.P. 26(c). "[W]hether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of production)." *Id.* Data that is "accessible" is stored in a readily usable format that does not need to be restored or otherwise manipulated to be usable. *Id.* at 320. Conversely, data that is "inaccessible" is not readily useable and must be restored to an accessible state before the data is usable. *Id.* Backup tapes are considered an inaccessible format, and, thus, shifting the costs of producing data from backup tapes may be considered. *Id.*

If the responding party is producing data from inaccessible sources, the *Zubulake I* court identified seven factors to be considered in determining whether shifting the cost of production is appropriate:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total costs of production, compared to the amount in controversy;
4. The total costs of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.

*Id.* at 322. The factors were weighed by the Court in descending order, the first factor being the most important consideration and the seventh factor the least important. To determine whether cost-shifting was appropriate in *Zubulake I*, the Court looked to a sample in which UBS restored data from 5 out of 72 backup tapes which contained the e-mails from *Zubulake's* immediate supervisor, the alleged principal perpetrator of the discrimination, over a five-month period. *Zubulake III, supra*, 216 F.R.D. at 282. The

restoration yielded a total of 8,344 e-mails including duplicates. Searching the e-mails for the terms "Laura," "Zubulake" and "LZ" yielded 1,075 non-duplicate e-mails of which UBS determined 600 were responsive to Zubulake's document request. *Zubulake III, supra*, 216 F.R.D. at 282. In applying the analysis set forth above, the Zubulake Court found that UBS was entitled to shift to plaintiff 25% of the costs of producing the e-mails. *Id.* at 289.

In addition to the tests fashioned by the courts in *McPeck*, *Rowe* and *Zubulake I*, it has also been argued that the Rule 26(b)(2) balancing factors are all that is needed to allow a court to reach a fair result when considering the scope of discovery of electronic records. *Thompson v. U.S. Dept. of Housing and Urban Development*, 219 F.R.D. 93 (D.Md. 2003). Rule 26(b)(2) requires a court, *sua sponte*, or upon receipt of a Rule 26(c) motion to evaluate the costs and benefits associated with a potentially burdensome discovery request. The rule identifies the following factors to be considered: whether the discovery sought is unreasonably cumulative or duplicative; whether the information sought is obtainable from some other more convenient, less burdensome or inexpensive source; whether the party seeking the information already has had adequate opportunity to obtain the information; and whether the burden or expense of the proposed discovery outweighs its likely benefit, taking into consideration the following: the needs of the case, the amount in controversy, the resources of the parties, the importance of the issues at stake in the litigation and of the discovery sought to the resolution of the issues.

Regardless of which test is used, the most important ingredient for the analytical process to produce a fair result is a particularization of the facts to support any challenge to discovery of electronic records. *Thompson, supra*. Conclusory or factually unsupported assertions by counsel that the discovery of electronic materials should be denied because of burden or expense can be expected to fail. See, e.g., *St. Paul Reinsurance Co., Ltd. v. Commercial Financial Corp.*, 198 F.R.D. 508, 511-12 (N.D. Iowa 2000) (citing numerous cases that hold that a party resisting discovery bears the burden of demonstrating lack of relevance, burden or excessive expense, and that generalized or conclusory allegations are insufficient. Instead, a particularized showing, by affidavit or similar submission is required to present facts supporting the challenge); *Marens v. Carrabba's Italian Grill, Inc.*, 196 F.R.D. 35, 38 (D. Md. 2000) (a party that objects to discovery requests on the grounds of burden or expense has an affirmative duty to particularize the basis of the objections, failing to do so waives the objection); *Coker v. Duke & Co.*, 177 F.R.D. 682, 686 (M.D. Ala. 1998); *Jackson v. Montgomery Ward & Co.*, 173 F.R.D. 524, 528-29 (D. Nev. 1997); *Kelling v. Bridgestone/Firestone, Inc.*, 157 F.R.D. 496, 497 (D. Kan. 1994); *Eureka Fin. Corp. v. Hartford Accident and Indemnity Co.*, 136 F.R.D. 179, 182-83 (E.D. Ca. 1991). Further, it should be noted that the responding party typically has the burden of proof on a motion for cost-shifting. See *Zubulake III, supra*, at 283; see also *Wiginton v. CB Richard Ellis, Inc.*, 229 F.R.D. 568, 573 (N.D. Ill. 2004).

## E. Production of Metadata

The term “metadata” essentially refers to the data that is created about the data that is stored electronically. It is the “electronic equivalent of DNA, ballistics and fingerprint evidence.”<sup>4</sup> Virtually all electronically stored information contains data about the data stored. The metadata varies depending upon the software that created the particular file. Metadata can include information regarding the author of a particular document, the identity of any editors of the document, the identity of anyone who prints the document; the dates and times that the document was accessed or edited; internal information on the cataloguing of the file and other information. Depending on the nature of the case and the issues involved, the metadata regarding specific documents could be critical.

When a document is printed into a hard format, the metadata is not included. Metadata may not even be visible or accessible to different users on the party’s network. If the file is converted from its “native format” to an image file (.tiff, .pdf, .bmp, .jpeg, etc.) the metadata will not become part of the image. Metadata can be removed or “scrubbed” from a file by software or data manipulations designed for that purpose. Because of the potentially valuable nature of metadata, courts typically require that electronically stored information be produced in the native format in which it is kept in the normal course of the business so that the metadata is preserved. Further, courts have generally frowned on any efforts to “scrub” metadata and/or to change the file formats of electronically stored data to prevent the production of metadata.

In *Hagenbuch v. 3136 Sistemi Elettronici Industriali S.R.L.*, No. 04 C 3109, 2006 WL 665005 (N.D. Ill. Mar. 8, 2006), the court addressed a dispute between the parties regarding production of electronic data in its native format with metadata attached. Plaintiff inspected defendant's electronically stored information at defendant’s office and designated numerous documents and electronic media for copying. Defendant offered to print out and deliver hard copies of all the documents identified, but Plaintiff refused that offer and requested identical electronic copies of the electronic media. Defendant converted the information on the original electronic media into Tagged Image File Format (.tiff) documents and downloaded the documents onto CD's.

Plaintiff argued that the .tiff documents created by defendant are "fundamentally different from the original documents and are not documents produced as they are kept in the usual course of business." In opposition, defendant argued that "the .tiff documents are reasonably usable forms of the designated electronic media that satisfy Fed. R. Civ. P. 34's requirements."

The court found that .tiff documents do not contain all of the relevant, non-privileged information that would be provided if the documents were in the designated electronic media such as: (1) the creation and modification dates of a document; (2) e-mail attachments and recipients; or (3) metadata. Further, the court was persuaded that

---

<sup>4</sup> *The Ten Most FAQ's in the Post-December 1, 2006 World of E-Discovery*, *supra*. – FAQ No. 8.

this information is relevant to plaintiff's case as it will allow plaintiff "to piece together the chronology of events and figure out who received what information and when."

In *Williams v. Sprint/United Management Co.*, 230 F.R.D. 640 (D. Kan. 2005), plaintiff filed suit asserting that her age was a determining factor in defendant's decision to terminate her employment. Defendant produced spreadsheets in electronic format; however, defendant scrubbed the spreadsheet files to remove the metadata and locked certain cells and data on the spreadsheets. Defendant argued that the spreadsheet's metadata is irrelevant, contains privileged information and that plaintiffs never requested the metadata. In addressing the dispute, the court explained that the production of electronic documents as they are maintained in the ordinary course of business includes the production of the metadata associated with the documents. The court stated that all metadata ordinarily visible to the user of the Excel spreadsheet should presumptively be treated as part of the document and should be discoverable. Ultimately, the court held that when a party is ordered to produce electronically stored information as it is maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order. Finally, the court held that the initial burden with regard to the disclosure of the metadata is on the party directed to produce the documents.

However, in *Kentucky Speedway, LLC v. NASCAR, Inc.*, 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. 12/18/06), the Court stated that "in the rapidly evolving world of electronic discovery, the holding of the *Williams* case is not persuasive. Having the benefit of the newly amended rules, advisory notes, and commentary of scholars, I respectfully disagree with its conclusion that a producing party "should produce the electronic documents with their metadata intact, unless that party timely objects ..., the parties agree that the metadata should not be produced, or the producing party requests a protective order." *Id.* at \*22. Similarly, in *Wyeth v. Impax Laboratories, Inc.*, 2006 U.S. Dist. LEXIS 79761 (D. Del. 2006), the Court stated, "[e]merging standards of electronic discovery appear to articulate a general presumption against the production of metadata." Clearly metadata will be critical in certain cases and in other cases it will be irrelevant, whether its production will be required will depend on the facts and circumstances of each case.

## **F. Spoliation Of Electronic Information**

Spoliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. *Teague v. Target Corporation*, 2007 U.S. Dist. LEXIS 25368 (D.W.N.C. 2007), quoting *Silvestri v. General Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001); *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999); *Allstate Ins. Co. v. Hamilton Beach/Proctor Silex, Inc.*, 473 F.3d 450 (2d Cir. 2007); *Byrnie v. Town of Cromwell*, 243 F.3d 93, 107 (2d Cir. 2001). As noted above, parties have an affirmative duty to preserve material evidence long before the filing of an initial pleading

in litigation. The determination of an appropriate sanction for spoliation, if any, is within the sound discretion of the trial judge, and is assessed on a case-by-case basis. *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001). The authority to sanction litigants for spoliation arises jointly under the Federal Rules of Civil Procedure and the court's own inherent powers. See *Turner, supra. at 72, citing* Fed. R. Civ. P. 37 and *Shepherd v. American Broadcasting Companies*, 62 F.3d 1469, 1474-1475 (D.C. 1995). Where a party violates a court order - either by destroying evidence when specifically directed to preserve it or by failing to produce information when directed to do so because the relevant data have been destroyed – Federal Rule 37(b) provides that the court may impose a range of sanctions, including dismissal or judgment by default, preclusion of evidence, imposition of an adverse inference, or assessment of attorneys' fees and costs. *Chan v. Triple 8 Palace, Inc.*, 2005 U.S. Dist. LEXIS 16520. Even though a party may have destroyed evidence prior to issuance of a discovery order and thus may be unable to obey, sanctions are still appropriate under Rule 37(b) because the inability to obey was self-inflicted. *Id.*

While courts have broad discretion to sanction a party for spoliation, the applicable sanction should be tailored to serve the threefold purposes of deterring parties from engaging in spoliation, placing the risk of an erroneous judgment on the party who wrongfully created the risk, and restoring the prejudiced party to the position it would have been in had the misconduct not occurred. *Phoenix Four, Inc. v. Strategic Res. Corp.*, 2006 U.S. Dist. LEXIS 34268; *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999). However, utilizing a sanction of dismissal for spoliation is generally not authorized absent bad faith conduct in exceptional circumstances. *Cole v. Keller Industries, Inc.*, 132 F.3d 1044, 1047 (4th Cir. 1998).

One of the most often utilized sanctions for spoliation is the issuance of jury instructions permitting the jurors to draw an *adverse inference* from a party's destruction of evidence. *Thompson v. U.S. Dept. Of Housing and Urban Dev.*, 219 F.R.D. 93, 100-01 (D.Md. 2003). An adverse inference instruction is a severe sanction that often has the effect of ending litigation because it can be too difficult for the spoliator to overcome the adverse inference. Accordingly, most courts recognize that such a sanction should not be given lightly. *Phoenix Four, Inc. v. Strategic Res. Corp.*, 2006 U.S. Dist. LEXIS 34268 (citation omitted) *quoting Zubulake IV*, 220 F.R.D. at 219-20; see also, e.g., *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999).

Courts have held that three elements should be shown to warrant an adverse inference instruction for spoliation: (1) the party having control over the evidence had an obligation to preserve it when it was destroyed;<sup>5</sup> (2) the destruction or loss was accompanied by a "culpable state of mind;" and (3) the evidence that was destroyed was relevant to the claims or defenses of the party that sought discovery of the spoliated evidence, to the extent that a reasonable fact finder could conclude that the lost evidence would have supported the claims or defenses of the party that sought it.

---

<sup>5</sup> The obligation to preserve evidence was discussed earlier, see Section C(7)(b) at p. 19.

*Residential Funding Corp. v. Degeorge Financial Corp.*, 306 F.3d 99, 107-108 (2d Cir. 2002).

With respect to the element of “culpable state of mind,” courts have recognized that evidence of bad faith or fraudulent intent is not required to obtain the adverse inference instruction. See *Vodusek v. Bayliner Marine Co.*, 71 F.3d 148, 156 (4th Cir. 1995). Of course a finding of bad faith, intentional or willful destruction of evidence will satisfy the element. The “culpable state of mind” requirement has been held to include gross negligence and ordinary negligence. *Residential Funding Corp.*, *supra.* at 108; *Byrnie*, *supra.* at 107-112; *Zubulake IV*, *supra.* at 220. In *Chan v. Triple 8 Palace, Inc.*, 2005 U.S. Dist. LEXIS 16520 (S.D.N.Y. Aug. 11, 2005), the failure to establish any form of litigation hold at the outset of litigation was held to be grossly negligent because the defendants continued to systematically destroy evidence having never been informed of their obligation to suspend normal document destruction policies.

With respect to the element of “relevance,” the moving party must show that the lost information would have been favorable to it. *Chan*, *supra.* “Relevant” in this context means something more than sufficiently probative to satisfy Rule 401 of the Federal Rules of Evidence. Rather, the party seeking an adverse inference must adduce sufficient evidence from which a reasonable trier of fact could infer that the destroyed or unavailable evidence would have been of the nature alleged by the party affected by its destruction. *Residential Funding Corp.*, *supra.* at 108-09. However, courts must take care not to hold the prejudiced party to too strict a standard of proof regarding the likely contents of the destroyed or unavailable evidence, because doing so would subvert the purposes of the adverse inference, and would allow parties who have destroyed evidence to profit from that destruction. *Id.*

Where a party destroys evidence in bad faith, that bad faith alone is sufficient circumstantial evidence from which a reasonable fact finder could conclude that the missing evidence was unfavorable to that party. *Id.* at 109. Similarly, a showing of gross negligence in the destruction of evidence will in some circumstances suffice, standing alone, to support a finding that the evidence was unfavorable to the grossly negligent party. *Id.* Accordingly, where a party seeking an adverse inference adduces evidence that its opponent destroyed potential evidence in bad faith or through gross negligence, satisfying the ‘culpable state of mind’ factor, that same evidence will frequently also be sufficient to permit a jury to conclude that the missing evidence is favorable to the party satisfying the “relevance” factor. *Id.* In the absence of bad faith or gross negligence by the alleged spoliator, the relevance element can be established if the moving party submits extrinsic evidence tending to demonstrate that the missing evidence would have been favorable to it. *Chan v. Triple 8 Palace, Inc.*, *supra.*

## **G. Practical Points and Tips**

### **1. Implement, Update and Enforce Records Management Policies in Light of e-Discovery Rules**

In light of the changes made to the federal rules and the obligations and burdens placed on litigants and counsel by the courts and recent decisions, if you do not have a document management plan or policy currently in-place, one must be created and implemented immediately. The plan should be created with reference to the many obligations that may be imposed if litigation should occur; it should not be created in a vacuum and cost should not be the only guiding factor. As the litigants who have lost some of the recent e-discovery battles would tell you, it is far cheaper to plan and prepare in advance than to suffer the consequences of failing to plan later. If you have a document management plan, but it is more than a few years old, it must be updated to address any changes that have been made to your electronic systems and to ensure conformance with the new requirements as noted herein. Finally, if you have a plan and it has been updated recently, perform an audit to determine if the plan is being followed and implemented properly. Don't wait for litigation to check to see if the document management plan was followed, by then it may be too late.

### **2. Review/Revise Computer Use Policies**

In addition to a document management plan, all organizations should implement and enforce computer use policies. Every organization should require its employees to save data in the same manner and to maintain that data in the same manner. Employees should not routinely retain data or information on personal computers, home computers or mobile devices. If the organization has a network, data should be saved to the network not to internal hard drives. Employees should not use the organization electronic systems for personal use and all must be reminded that in the event of litigation or regulatory action e-mails may likely be produced.

### **3. Educate the Users**

All who use the e-mail system must be periodically reminded that such communications are not necessarily private, personal or confidential and could be produced in response to discovery requests. Many treat e-mail communications as informal discussions and may include information that is off-color, unprofessional or worse without realizing or intending that such information would be produced often years later. The business systems should be used only for business and should be used in a professional manner. Users should also be educated so that they are aware that simply deleting an e-mail or document does not actually obliterate the document. In most cases, hitting the delete button only marks the file and it may remain for an indefinite period of time or may be stored in a deleted file folder. Users should know that metadata is being compiled and stored with most electronically created documents and that information can be produced in response to discovery requests. Users should

be made aware of the document management policy and be made familiar with how documents are stored and maintained, when they are backed-up, what is stored and for how long.

#### 4. Get to Know Your IT systems

Before litigation hits, counsel and organizations need to become fully familiar with the IT systems. Not only is such knowledge now required under the federal rules for purposes of the initial Rule 26 conferences, but such knowledge is also required to properly implement a litigation hold in the event that litigation becomes reasonably probable.

#### 5. Enforce “Litigation Holds”

Courts have uniformly expressed their dismay and displeasure with counsel and parties who fail to enforce litigation holds. It is not enough to implement a litigation hold at the outset, counsel and the parties must continue to enforce that litigation hold throughout the litigation and should undertake periodic review to determine whether the litigation hold is being observed and followed.

#### 6. Check state rules and laws regarding e-discovery

With the implementation of the new federal rules, it will only be matter of time before state courts start amending the rules in local jurisdictions to address e-discovery. When creating and implementing a document management program care must be taken to determine if the jurisdiction in which you are located or do business have specific requirements that might impact how, what and for how long information must be maintained.

### **H. Conclusion**

Whether you like it or not, whether you understand it or not, e-discovery is here and it will be here going forward for the foreseeable future. It is a fact of life and rapidly becoming a part of life just as computers, e-mail and the internet have become part of life. Many have looked at the issue as one of those, “oh, that doesn’t apply to me” types of situations. With the changes to the federal rules and the recent case law pre-dating the changes and post-change, e-discovery will rapidly become an issue in every case. Because of the costs and burdens as well as the potential benefits of catching an opposing party “asleep at the wheel,” e-discovery presents a significant opportunity for the “little guy” to inflict some serious pain and cost on the “big guy.” In many recent decisions, the “big guy” has failed to properly implement a litigation hold, failed to preserve information or failed to enforce a litigation hold once it had been implemented and the courts have issued adverse inference instructions which have led to extreme verdicts in favor of the “little guy.” These verdicts appear to have more to do with failures to preserve and manage electronic information than with the facts or merits of

the case. It is time to embrace the changes and to integrate those changes into the fabric of how business is done and how law is practiced.

## **BIOGRAPHY**

**Michael A. Stover** is a partner with the law firm of Whiteford, Taylor & Preston, LLP. He practices in the field of surety and construction law. He regularly represents surety companies in all aspects of performance and payment bond losses and claims including financing, takeover and workouts, as well as litigation on behalf of the surety defending and prosecuting claims and pursuing/protecting rights against indemnitors. Mr. Stover obtained his B.S. degree from the University of Maryland, College Park and his Juris Doctor from the University Of Maryland School Of Law with honors. Mr. Stover is admitted to the Bars of the State of Maryland, the United States District Court for the District of Maryland, the United States Courts of Appeals for the Fourth Circuit and for the Third Circuit and the United States Court of Federal Claims. Mr. Stover is a member of the American Bar Association Forum on the Construction Industry, the Fidelity and Surety Law Committee of the Tort Trial and Insurance Practice Section and the Public Contract Law Section of the American Bar Association and the Maryland State Bar Association. Mr. Stover has lectured on numerous occasions on surety and construction law issues.