

**COMPUTER FORENSICS:  
NON-ADVERSARIAL DISCOVERY<sup>SM</sup> OF  
FACTS**

**By: Donald Wochna, Esq.  
Chief Legal Officer**

**Vestige Ltd.  
46 Public Square  
Suite 220  
Medina, OH 44256  
330-721-1205**

## ABOUT VESTIGE LTD.

Vestige Ltd. is organized into Computer Analysis Teams, comprised of forensically trained attorneys and computer specialists using licensed forensic software, to locate data on electronic media that has evidentiary value, and to extract, preserve, and present that data in a manner consistent with our client's legal theories and strategies. VESTIGE's Computer Analysis Teams work with attorneys to execute search and production protocols that protect privilege and confidentiality, while extracting, parsing, and collating relevant evidentiary data. VESTIGE is a member of various law enforcement and computer forensic societies including the Northern Ohio Information & Technology Roundtable, Metropolitan Crime Clinic; National Institute of Standards and Testing, subgroup for Computer Forensic Tool Testing; and the Electronic Crime Investigation Group.

“The rules (of Civil Procedure) talk about the production of relevant information,  
so we seem to create the burden to seek e-data...**I can’t imagine how counsel  
who is responsible cannot seek relevant electronic information”**

Judge Loretta Preska  
U.S. District Court, S.D.N.Y.

“How a Judge Expects You To Handle Electronic Records in Discovery”

July, 2003

Metropolitan Opera Association, Inc. v. Local 100, 212 F.R.D.178 (S.D.N.Y., 2003)

**Lawyers who forsake electronic discovery on behalf of a client  
due to costs, come close to professional negligence.**

Magistrate Judge John M. Facciola  
U.S. District Court, D.Col.

author of McPeck vs. Ashcroft, 212 F.R.D.33 (D.D.C., January 9, 2003)

## **EXECUTIVE SUMMARY: COMPUTER FORENSICS IS CAUSING A PARADIGM SHIFT IN DISCOVERY TOWARD “NON-ADVERSARIAL DISCOVERY<sup>SM</sup>”**

This paper analyzes relevant case law and identifies a significant shift in the focus and manner in which facts are being discovered in litigation. Basically, the traditional use by an attorney of the rules of discovery to obtain relevant “documents” is being replaced with a process and protocol using computer forensic analysis to first create “clones” of the media on which resides “relevant data” and then search those clones electronically for all relevant information. In effect, a request for production of documents is being replaced by a request for production of things: to wit, the media on which is resident data relevant to the matter.

This shift is both a reaction to the pervasive use of computers to create, store, process, and archive information in an ever-increasing number of formats, and a response to the discoverable data left behind by the unique features of computer operating systems. By first obtaining access to all media containing relevant data, and then extracting from the media all relevant data in whatever format it may exist, attorneys are able to discover both the data that is visible to the operating system (traditional documents, etc.) as well as data that is invisible and had traditionally been ignored and left behind. Because the process and protocol recognized by federal and state courts is value neutral, attorneys are offered the possibility of conducting discovery of facts in a non-adversarial forum.

“**Non-Adversarial Discovery<sup>SM</sup>**” is the name Vestige has given its enhancement of the process and protocol recognized by federal and state courts to acquire all relevant data and evidence in any case or matter. Non-Adversarial discovery<sup>SM</sup> is based on computer forensic analysis: the use of specialized software and procedures to identify, extract, and present all data relevant to a case, including data that has been hidden, deleted, or otherwise rendered invisible. Using Non-Adversarial discovery<sup>SM</sup> protocols, an attorney can obtain from his client and from other party litigants all relevant data in one process very early in litigation. Once all relevant data has been extracted and protected for privilege, the data can be prepared for use in court using any type of organizational technique, including electronic discovery organization software such as Summation or Case Map.

### **TRADITIONAL DISCOVERY AND FEATURES OF COMPUTER SYSTEMS**

Traditionally, litigators obtained relevant documents from their opponent by issuing a Request for Production of Documents. Although the Rules of Civil Procedure mandate the disclosure of relevant, non-privileged documents<sup>1</sup>, it is a rare case in which an opponent copies all relevant documents and provides them in response to the first Request. Usually, counsel must make several phone calls, write letters, monitor the partial responses provided, and constantly work to obtain as complete a production of documents as possible. Additionally, counsel had to ensure that its definition of

---

<sup>1</sup> This assumes counsel has defined the term document properly.

“documents” was broad enough to include all forms and formats in which relevant information may have been stored by a litigant. Constantly expanding the definition of “documents” to capture all formats in which relevant data may be stored on computer systems used by clients and litigants is challenging in a society in which computer usage has exploded.

North American Businesses sent about 2.5 trillion email messages in 2001. The total number of electronic records produced in the world could, within the next ten years, double every sixty minutes. Sign of Times, Daily Journal Extra, October 28, 2002, Pamela Voich & Michele Lange. Email has become a treasure trove of “present-sense” impressions. In a case involving Phen-Fen drug, one email read: “Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem?” Dispensing with the Truth, St. Martin’s Press, Inc. Alicia Mundy (April, 2001).

The following is a partial sample of the types of information typically found on a computer system:

- i. Correspondence
- ii. Drafts of documents
- iii. Changes to documents created and never saved
- iv. Documents created but not saved
- v. Instant messages received and sent
- vi. Emails
- vii. Attachments to emails or instant messages, including jokes, love letters, strategy discussions, observations
- viii. Folder names and file structure
- ix. Presentations
- x. Audio and video files
- xi. Pictures, including all pictures displayed from every website visited
- xii. Websites visited, including all files necessary to completely reconstruct each website in the order they were visited, and files related to the amount of time spent viewing each website
- xiii. Pictures from websites that may not have been visited but which were loaded onto computer as “pop-under” or “pop-up”
- xiv. Spreadsheets, draft spreadsheets
- xv. Accounting and tax information
- xvi. Faxes sent and received
- xvii. Images and text scanned
- xviii. Everything that has been downloaded from any computer or the internet
- xix. Contact lists, phone numbers
- xx. Credit card numbers
- xxi. Search information for all searches conducted. For example, Google searches
- xxii. Business records

- xxiii. System and program artifacts related to the manner in which a system was used, including artifacts related to copying, printing, programs installed (whether or not currently present on the system), programs frequently run, networked connections and access to other computers.

Even if attorneys could constantly refine the definitional parameters of “documents”, the operational characteristics of computers limits their usefulness in obtaining documents.

**Operational Characteristics of Computer Systems.** The fundamental feature of computers is speed. In order to achieve maximum speed, engineers have developed techniques to achieve functionality as quickly as possible. These techniques, however, have consequences that impact attorneys.

For example, computer engineers developed techniques to “delete” information as quickly as possible. None of these techniques, however, destroys the information. When a user presses the “delete” key, the computer operating system takes a number of steps only to ultimately render the file “invisible” to the operating system. Because the computer was built for speed, it takes no time whatsoever to overwrite, shred, or otherwise destroy the information. Thus, although the information cannot be “seen” by the computer, it is nevertheless present on the hard drive.

Data can become “orphaned” on a computer system. Generally data is saved on a computer in a data file that must be opened and read with particular software. If the software program that created the data file is uninstalled, deleted, or cannot be launched (such as when it has become corrupted) the data file cannot be read by the computer and is “orphaned”. Similarly, software developers sometimes update software to new versions that cannot read information created with prior versions. This feature seems especially prevalent in accounting software. For example, a financial spreadsheet created with version 1.0 of an accounting program may not be readable using an updated version of the program. Although the financial spreadsheet created with version 1.0 is resident on the computer system, it is “invisible” because the computer cannot interpret the data any longer. In effect, the data file is “orphaned” because the computer system no longer has a program available to use the file.

Data can become “hidden” on a computer system. For example, a document file (with a “.doc” extension) can be saved with a different extension (such as with a “.jpg” extension). The document will not be readable by the computer in this situation. Thus, although the data is still on the computer, the data cannot be opened.

In addition to invisible data left on computer systems, the computer’s operating system and the software programs leave a tremendous amount of information behind as they perform their functions. This information, referred to as artifacts, can be used to reconstruct the manner in which a computer was used. For example, a corporate officer may copy proprietary customer information to removable media prior to leaving a corporation to work for a competitor. Removable media may include “travel drives”

shaped like wristwatches or pens that contain USB flash drives capable of storing over a gigabyte of information. Once removed from the premises, the only evidence of this type of unlawful activity will be artifacts left behind by the operating system. These artifacts can be extracted and when properly analyzed will document the unlawful copying of data to the removable media.

These characteristics of computer operating systems and software programs have legal consequences for attorneys relating primarily to the preservation and acquisition of the “invisible” data and artifacts.

### **Scope of Visible and Invisible Information on Computers.**

All the information on a computer will be either visible or invisible to the operating system. Visible information can, of course, be intentionally rendered invisible, such as by deletion or the removal of the software program necessary to read the information. Of course, experienced attorneys find that information that intentionally has been rendered invisible (by the client or opponent) is frequently the most damaging information. Additionally, parties to litigation and their counsel have a duty to preserve evidentiary information and avoid spoliation.

In order to understand the procedures that may be needed to preserve and acquire visible and invisible information from computer systems, attorneys must understand the threats to the integrity of visible and invisible information posed by computer operating systems.

### **Ongoing Use of Computer System as Ground for Forensic Process Create Clone**

Visible and invisible data on a computer system may be destroyed by several threats including, electrical shock, viruses, physical damage to the hard drives, and systemic and intentional overwriting. Of all the threats, systemic overwriting of invisible data occurs merely from the ongoing use of the computer system on which resides relevant information.

Systemic overwriting by the operating system occurs as a result of the engineering techniques used to make computer perform rapidly. As explained above, a computer’s operating system creates thousands of artifacts and file data as it is being used. Additionally, the operating system renders invisible all data “deleted” by the computer user. All the artifacts, file data, and invisible information is written to physical locations on the computers’ hard drives. All this information remains physically written on the hard drives until such time as the operating system “overwrites” some of the data by writing new artifacts, file data, and/or invisible information at the same physical locations.

Courts are recognizing that the ongoing use of the computer operating system destroys invisible information, including data that may be relevant to the claims or defenses in a case. Antioch v. Scrapbook, 210 F.R.D. 645, 2002 U.S. Dist. LEXIS 20811 (D.Ct. Minn., April 29, 2002). Indeed, this is a significant threat that can be ameliorated only by either

refraining from using the computers or by creating a forensic “snapshot” of the computers, which includes all visible and invisible information locked into a secure, authenticated clone of the relevant hard drives.

In Antioch, the United States District Court for the District of Minnesota was faced with the issue whether, at the initial stages of litigation, to grant Plaintiff’s Motion to Compel Discovery and Appoint a Neutral Expert in Computer Forensics. Plaintiff filed its motion prior to any conference required by Rule 26(f), Federal Rules of Civil Procedure, at a time therefore when discovery was prohibited. Additionally, no Scheduling Order was in force by the Court, no Pre-Trial Conference had been scheduled, and one of the defendants had not yet filed its Answer. Antioch at page 650-651. In its motion Plaintiff argued that that “data from a computer which has been deleted remains on the hard drive, but is constantly being overwritten, irretrievably, by the Defendants’ continued use of that equipment”. Antioch at 651.

The Minnesota District Court granted Plaintiff’s motion for expedited discovery and its motion to compel discovery on the ground “the Defendants may have relevant information on their computer equipment, which is being lost through normal use of the computer, and which might be relevant to the Plaintiff’s claims or the Defendant’s defenses. This information may be in the form of stored or deleted computer files, programs or emails, on the Defendants’ computer equipment”. Antioch at 652.

It is important to note that the District Court focused upon the features of the operating system as the ground upon which to compel the preservation of the data resident on the defendant’s computers. The Court specifically noted that the plaintiff provided an affidavit of a computer forensic expert attesting that “data which is deleted from a computer is retained on the hard drive, but is constantly being overwritten by the new data, through the normal use of the computer equipment”. Antioch at 651.

This case supports the technologically accurate legal argument that relevant data is being destroyed by the continued operation of the computer systems used to create, process, archive, or delete data. This technological argument ought to be sufficient to compel the forensic imaging of relevant computers as the only viable method of preventing the loss of relevant data.

Antioch implicitly raises the issue whether the discovering party must first prove that the producing party has engaged in deletion of information as a condition precedent to creating forensic images of relevant computers. It seems apparent that where the discovering party grounds its need to create a forensic image on the overwriting characteristics of the computer’s operating system, or where the discovering party has focused upon the discovery of residual data left behind by the operating system, the producing party must create a forensic image. The producing party cannot comply with such a request using the normal operating system.

Whether a party has a duty to create forensic images of relevant computers to prevent spoliation of evidence has received some attention from an ad-hoc group of attorneys and large corporations. See discussion of Sedonna Principles below.

Finally, requiring counsel to prove deletion as a condition of obtaining an Order granting a Motion to Compel may not have much practical significance. It is hard to imagine a party successfully arguing that it has never used the delete function of its computers, or that it has never deleted any information relevant to the dispute at bar. In any event, counsel can conduct a Rule 30(B) deposition of the party to establish the existence and use of the delete function in the normal course of business. Where deletion is known to have occurred in the normal course of business, courts have uniformly held that the deleted data is discoverable.

### **DELETED DATA IS DISCOVERABLE. DELETION DOES NOT PLACE DATA OUTSIDE THE SCOPE OF DISCOVERY**

It is generally understood that deleting data does not remove it from the scope of discovery. See Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) (“[I]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable”); Rowe Entm’t, Inc. v. The William Morris Agency, Inc., 205 F.R.D. 421, 427-431 (S.D.N.Y. 2002) (stating that “[e]lectronic documents are no less subject to disclosure than paper records,” and only questioning which party should bear the cost of such discovery, especially for backup tapes or deleted e-mails); McPeck v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001) (stating that, “[d]uring discovery, the producing party has an obligation to search available electronic systems for information demanded,” and ordering a limited backup restoration of e-mails); Kleiner v. Burns, 48 Fed. R. Serv. 3d 644, 2000 WL 1909470 (D. Kan. Dec. 15, 2000) (noting that Rule 26(a)(1)(B) requires description and categorization of computerized data, including deleted e-mails, and stating that “[t]he disclosing party shall take reasonable steps to ensure that it discloses any backup copies of files or archival tapes that will provide information about any ‘deleted’ electronic data”); Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000) (“First, computer records, including records that have been ‘deleted,’ are documents discoverable under Fed. R. Civ. P. 34.” Citing Crown Life Insurance Co. v. Craig, 995 F.2d 1376 (7<sup>th</sup> Cir. 1993); Illinois Tool Works, Inc. v. Metro Mark Products Ltd, 43 F.Supp.2d 951 (N.D. Ill. 1999)); Playboy Enter. v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) (“Plaintiff needs to access the hard drive of Defendant’s computer only because Defendant’s actions in deleting those e-mails made it currently impossible to produce the information as a ‘document.’”). Anti-Monopoly, Inc. v. Hasbro, Inc. WL 649934 (S.D.N.Y., Nov. 3, 1995); Seattle Audubon Society v. Lyons, 871 F. Supp. 1291 (W.D. Wash. 1994); Linnen v. A.H.Robins, Co. WL 462015 (Mass. Super., June 16, 1999). Deleting data on a hard drive does not remove the data from the scope of discovery. Dodge, Warren & Peters Ins. Servs. v. Riely WL 245586 (Cal. Ct. App. Feb. 5, 2003); Simon Property Group v. mySimon, Inc. 194 F.R.D. 639, 2000 U.S. Dist. LEXIS 8950 (S.D. Ind. 2000).

It seems well settled that discovery is not limited to only those files that are “visible” to the computer system; discovery includes files that cannot be seen by the operating system, including deleted files. In reaction to this case law, an ad-hoc group has suggested that discovery ought to be limited only to the “visible” files on a computer: i.e. those files and information purposefully stored on a computer system. Sedona Principle No. 8, “The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production”, March 2003, [www.thesedonaconference.org](http://www.thesedonaconference.org). This group has suggested that discovery ought to exclude disaster recovery backup tapes and other sources of data and documents other than the active files. *Id.* This group also suggests that, absent special need and relevance, a party responding to discovery ought not to be required to preserve, review, or produce deleted, shadowed, fragmented or residual data or documents. Even metadata (such as the dates a file was created, modified, or accessed) ought to be excluded as a rule. *Id.*

Comparing and contrasting the Sedonna principles with case law granting discovery requests for electronic data highlights the tension in the law created by the features and characteristics of computer operating systems that create significant, invisible, relevant information on the hard drives. On the one hand, this valuable information ought to be treated like any other relevant information. The fact that it is invisible to the operating system ought to be analogous to paper documents that have been torn to shreds but recovered from a waste basket. On the other hand, invisible computer data has traditionally been expensive to preserve and extract. It is understandable that defendants would object to the burden and expense of preserving this data when it is not used in the ordinary course of their business. Thus, while courts continue to grant motions to discover invisible data, the Sedonna principles argue that this data ought to be excluded.

Absent specific circumstances, preservation obligations should not extend to deleted data or residual data. While most computer systems will have a plethora of data that could be “mined”, there should not be routine authorization for such forensic recovery. If, as is typically the case, deleted data and residual data are not accessed by employees in the ordinary course of business, there is no reason to require the routine preservation of such data. The relevance of the data to the matters in question will be marginal at best in most cases, while the burdens involved will be great. In exceptional cases, however, there may be good cause for targeted preservation of deleted and residual data.

Sedonna Principles Comment 9.b. “Deleted Data and Residual Data”.

Although the principles seem clear, it is not difficult to imagine a case in which the Sedonna proponents, as plaintiffs, will reject these principles and find deleted data to be very relevant. In several years of practicing law and conducting forensic examinations, this author has found that deleted and residual data is usually very relevant. For example, in many sexual harassment and wrongful termination cases, corporations frequently use deleted email, instant messages, notes, jokes, love letters, etc. to establish an irrefutable factual basis authorizing the corporation’s actions. Similarly, many corporations are very pleased to extract, and anxious to aggressively use, evidence of wrongful copying of

customer lists, trade secrets and proprietary information to obtain injunctive relief against former sales personnel.

If the Sedonna proponents have a legitimate concern about extracting invisible data, it appears to be based on the cost and burden associated with computer forensic analysis. The Sedonna principles suggest that invisible data resident on computer systems ought not to be discovered where the cost and burden is extraordinary.

The proper subject of discovery is electronic data and documents that are relevant to the claims and defenses in the case, and a requesting party should not be permitted to discover electronic data and documents that do not meet this standard regardless of how technically feasible access may be. Accordingly, forensic data collection should not be required unless exceptional circumstances warrant the extraordinary cost and burden of this approach. See *McPeck v. Ashcroft*, 212 F.R.D. 33, 365 (D.D.C. 2003) (declining to order searches of backup tapes where the burden on defendant in searching those tapes would be great and plaintiff had not demonstrated a likelihood of obtaining relevant information). Making image backups of computers is only the first step of an expensive, complex, and difficult process of data analysis that can divert litigation into side issues involving the interpretation of ambiguous forensic evidence.

#### Sedonna Principle Comment 8.b. “Forensic Data Collection”

This concern can be, and as a matter of fact, has been rendered moot by advances in computer forensic technology. Today, computer forensic analysis is very cost effective, especially because it captures all relevant data: visible and invisible in one streamlined process. In the final analysis, the Sedonna conference is a traditional response to the existence of evidence: the acceptance of computer forensic analysis by counsel and clients depends ultimately on whether the evidence extracted from the computer systems is helpful to the client’s cause or the attorney’s legal theories and strategies. In this regard, it is no different than traditional paper discovery.

### THE COMPUTER FORENSIC PROCESS

Although the computer’s operating system cannot view the “invisible” data resident on the computer’s hard drives, special forensic software can read, extract, and process all data on hard drives, including “invisible” data in a non-disruptive, economical manner. The procedure used by computer forensic analysts to identify and extract all relevant data from a computer hard drive begins with the creation of a forensic mirror-image clone or copy of the relevant hard drives. *Playboy Enterprises, Inc. v. Welles* 60 F. Supp.2d 1050 (S.D. Cal. 1999). *State v. Cook* 149 Ohio App.3d 422 (2<sup>nd</sup> Dist. Mont. County, 2002)

The choice of forensic software is important. Encase software has been recognized by Ohio Courts as a reliable, precise, and accurate method of preserving electronic data.<sup>2</sup>

---

<sup>2</sup> Each forensic image contains embedded data that guarantees the integrity of the image at the time of its creation, and for all times thereafter. No change to the forensic image can occur undetected

See State. v. Cook, supra. Encase is easily the most widely accepted and used forensic software, currently being used by over 9,000 law enforcement agencies worldwide.

Creating a mirror image forensic clone of a relevant hard drive requires that the computer forensic specialist have access to the relevant computers and the hard drives contained therein for an average of two to five hours.<sup>3</sup> During this period of time, the computer forensic analyst will open the relevant computer cases, remove and attach a write-blocking device to the hard drive (to prevent any change to any of the data on any of the relevant hard drives), and create an exact forensic mirror image of each relevant hard drive. Each forensic mirror image is written to a hard drive supplied by the forensic examiner. After the process is completed, the relevant computer's hard drives are placed back into the computer case from which they were removed.

## **OBJECTIONS TO REQUEST TO PRODUCE RELEVANT COMPUTER HARD DRIVES**

### **A. DISRUPTION**

Regardless of the number of relevant computers, the imaging process can be accomplished very quickly because all relevant computers can be imaged simultaneously. To further minimize any inconvenience to the producing party, forensic images of all relevant computer hard drives can be scheduled during convenient times including evenings, after business hours, Saturdays or Sundays. Imaging can occur on-site, or at any convenient location, including the offices of counsel. Indeed, the producing party can even remove the relevant hard drives and ship them to the computer forensic analyst if the producing party does not want anyone on-site.

This forensic process is not disruptive. In fact, this process is very efficient, allowing the identification and extraction of relevant data to be accomplished electronically.

### **B. COST**

It is generally accepted law that, absent unusual circumstances, the producing party bears the cost of the identification, extraction, and production of relevant computer data. Linnen v. A.H.Robins Co., Inc. No. 97-2307, 1999 WL 462015 (Mass. Super.Ct. June 16, 1999); Bills v. Kennecott Corp., 108 F.R.D. 459 (D.Utah, 1985). The basis of this rule is that a party choosing to enjoy the tremendous business advantages of using computers to process data, cannot shield themselves from the costs attendant to the extraction of relevant data in litigation. In re Brand Name Prescription Drugs Antitrust Litigation, 1995 U.S.Dist. LEXIS 8521, 1995 WL 360526 (N.D.Ill. June 15, 1995).

Parties, however, are entitled to be protected from undue expense or burden in producing data in litigation. Southern Diagnostic Assoc. V. Bencosme WL 31422863 (Fla. Dist. Ct.

---

<sup>3</sup> This is an average time. Many cases can be completed in less than two hours. Sometimes, the imaging process takes longer depending on the condition of the relevant hard drives, the speed at which they operate, and other factors.

App., Oct. 30, 2002); Strasser v. Yalamanchi, 669 So.2d 1142 (Fla. Dist. Ct. App. 1996); In re Brand Name Prescription Drugs Antitrust Litigation WL 360526 (N.D. Ill. June 15, 1995).

Traditionally, courts looked to several factors to determine when the costs of producing data ought to be borne by the requesting party. Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 51 Fed. R. Serv. 3d 1106 (S.D.N.Y. 2002). (Defendants argued that costs of recovering email would range from \$84,000 to \$403,000. Trial Court held "it is not enough to say that because a party retained electronic information, it should necessarily bear the cost of producing it." Court used a multi-factor test to determine when to shift the cost of production:

1. the specificity of the request,
2. the likelihood of finding relevant information,
3. the availability of such information from other sources,
4. the purposes for which the data was retained,
5. the possibility that the responding party might benefit from the production,
6. the total cost of production,
7. the relative ability of the parties to control costs and the incentives to do so, and
8. the resources of each party.

Medtronic Sofamor Danek, Inc. v. Sofamor Danek Holding, Inc., 2003 U.S. Dist. LEXIS 8587 (W.D. Tenn. May 13, 2003)(The defendant sought information contained in 2,000 GB of data stored on 515 backup tapes and in 210 GB of electronic files from plaintiff's individual employees. The plaintiff asserted that there were 993 backup tapes with over 61 TERABYTES of data and the individuals' files contained over 300 GB of data. The court analyzed the factors in Rowe to determine whether an expense is "undue." As to total cost of production factor, the Court considered:

1. Cost of restoring backup tapes;
2. Cost of designing and conducting a search;
3. Cost of privilege review;
4. Cost of physical production; and
5. Production cost summary.

The Court set forth a detailed Protocol that included the use of a computer expert).

Recent case law has suggested that a balancing approach be used to determine when, and to what degree, the costs of extracting relevant data ought to be borne by the producing and requesting parties. "Cost shifting ought to be considered only when electronic discovery imposes an 'undue burden or expense' on the responding party. Zubulake v. UBS Warburg, 2003 U.S. Dist. LEXIS 7939 (S.D.N.Y. May 13, 2003).

Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved. This makes no sense. Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for

privilege checks, and the production can be made in electronic form obviating the need for mass photocopying.

*Id.* at \*27-\*28.

The Zubulake court created a “Seven-Factor Test.”

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 cost of production, compared to the amount in controversy;
4. The total cost 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.

It is important to note, however, that many of the cases addressing the allocation of cost involve forensic software more than four years old or involve back up tape technology. Changes in forensic software within the last four years have dramatically reduced the cost of imaging, identifying and extracting relevant data, and in many cases, the requesting party pays the cost to avoid any argument about cost shifting. This strategy is especially prevalent where the cost of imaging and analyzing multiple computer systems will cost less than \$7,000.00

To further reduce the cost of discovery on the parties, courts are appointing computer forensic experts as a neutral party expert to image and extract relevant data from all Relevant Computers. “Judges are getting the message. It makes more sense to look to one neutral expert, with the appropriate protocols, rather than relying on the parties to do it and duplicate their expense and effort.” Playboy Enterprises, Inc. v. Welles, 60 F.Supp.2d 1050 (S.D. Cal. 1999). Simon Property Group v. mySimon, Inc. 194 F.R.D. 639 (S.D.Ind. 2000).

### “FISHING EXPEDITION”

After the computer forensic expert creates images of all relevant hard drives, he will simultaneously mount all images on a lab computer, and electronically search and analyze the images for relevant data. Search strategies will be created jointly by the computer forensic expert and attorneys that reflect the legal theories and strategies in the case. “Unlocking” all data on an image, conducting keyword searches, combined with analysis of metadata and system artifacts, comprise the usual tools used to complete a forensic analysis.

Electronic searching for relevant data is the only practical means of identifying relevant data resident on a hard drive. An average size hard drive can have millions of pieces of data resident thereon, and it is impossible to search for relevant data by randomly viewing folders or files. No computer forensic expert will “browse” through the images of relevant hard drives seeking to stumble across relevant data. Nor does anyone simply open files to view their contents. All searching for relevant data is conducted electronically. As a result, non-relevant data is never identified, extracted, or viewed.

In some cases, counsel for the producing party argues that he should be given the right to approve of the search and analysis strategy used by the computer forensic expert, including the right to veto the use of search terms or analysis of system artifacts. In some cases, this argument is an attempt to prevent the discovery of relevant data.

This strategy is rendered moot by the protocol followed in state and federal cases that require counsel for the producing party receive the Initial Report of Relevant Data and redact it for privilege before the Report is produced.

### **REDACT FOR PRIVILEGE BEFORE REPORT IS PRODUCED.**

Computer forensic analysis is a tool that allows specialists to view all data on a hard drive, including all the data not seen by the operating system. Computer forensic analysis is not a tool to circumvent the law related to privileged communications. To satisfy the requirements of discovery, while allowing the producing party to review data for privilege, a standard protocol has evolved. See for example the decisions of Simon Properties, Playboy vs. Welles, Antioch vs. Scrapbook, cited herein. This protocol requires the computer forensic expert to identify and extract all relevant data, prepare an Initial Report, present its Initial Report of relevant data (which may include attorney-client data) to counsel for the producing party, while filing a copy of the Report of Relevant Data, under seal, with the Court. The computer forensic expert will also file with the Court and serve on all parties a Summary of its Report of Relevant Data, containing the following information:

- (1) Number of pages in Report, Number of tables, appendices, or exhibits
- (2) All search terms and the number of “hits” for each term
- (3) A statement of the Search and Analysis Strategy, Acquisition data related to the creation of the forensic images, and the table of contents for the report.

The computer forensic expert will copy its Report of Relevant Data onto a cdrom as a Word document or webpage. Counsel for the producing party will be able to redact the report for privileged communications as follows:

- (1) open the Report on counsel’s computer;
- (2) read the Report, and using the cursor, highlight any text for which counsel wishes to claim privilege;
- (3) “cut” the text out of the Report, and “paste” the text into a new document created on counsel’s computer;

- (4) identify the text in a privilege log;
- (5) Save the Report as Redacted;
- (6) produce to Plaintiff on cdrom a copy of the Report as Redacted and a copy of the privilege log.

This protocol is so efficient that Courts frequently order counsel for the producing party to produce a redacted report within ten days of receiving the Initial Report of Relevant Data. Moreover, this protocol completely satisfies concerns related to privileged communications, while permitting the parties to efficiently acquire all relevant data from all relevant computers.

## SANCTIONS

Parties to litigation have a duty to preserve evidence beginning at the time when a party knows or reasonably should know that the evidence may be relevant to pending or anticipated litigation. Mathias v. Jacobs, 197 F.R.D.29 (S.D.N.Y. 2000); Melendez v. Illinois Bell Telephone, 79 F.3d 661 (7<sup>th</sup> Cir. 1996). The duty to preserve data relevant to anticipated or existing litigation extends to data resident on computer hard drives and other electronically recorded data. Kleiner v Burns, WL 1909470 (D Kan., Dec. 15, 2000); Danis v. USN Communications, WL 1694325 (N.D.Ill. Oct. 23, 2000). Minnesota Mining & Manufacturing Co (“3M”) v Pribl, 259 F.3d 587 (Wis. 2001), 2001 WL 832749 (July 25, 2001). (Seventh Circuit Court of Appeals upheld the decision of the Trial Court to give a jury a negative inference charge on the ground that the defendant’s explanation that his child unintentionally downloaded six gigabytes of music on the day before the computer was produced was properly rejected by the Trial Court).

The first rule of preservation is to do no harm to the data to be preserved. Computer data is volatile and is destroyed by the mere operation of the computer’s operating system. Antioch v. Scrapbook, 210 F.R.D. 645, 2002 U.S.Dist.LEXIS 20811 (D.Ct. Minn., April 29, 2002). Log files are changed whenever a system is started. The start process (boot-up) changes the dates and information kept in thousands of files. Housekeeping programs that format disks (Defrag), purge files after a time period, recycle back-up tapes or media must be identified and stopped as soon as possible. The obligation to preserve documents rests with senior corporate officials, who must contact information technology personnel and insure that the company’s document retention programs are modified so as not to destroy relevant data. Danis v. USN Communications, Inc. 2000 WL 1694325 (N.D.Ill. October 23, 2000). Companies cannot use a corporate retention policy to “shield” their destruction of evidence, even where the destruction occurred before litigation was initiated. Rambus v. Infineon, 220 F.R.D. 264, 2004 U.S.Dist.LEXIS 4577 (E.D.Va. March 17, 2004).

Because the normal operation of a computer system threatens to destroy the “invisible” evidence located thereon, spoliation issues can be unique. Preventing spoliation from the ongoing use of the computers has been the ground for granting expedited discovery and compelling the forensic imaging of relevant computers. Antioch v. Scrapbook, Id. Where data destruction occurs after a complaint is filed and is deliberate, sanctions can

be imposed. William T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443 (C.D. Cal. 1984). “GNC was on notice from the inception of litigation that the [erased] records...were relevant to the litigation or at least were reasonably calculated to lead to the discovery of admissible evidence...GNC’s senior management know or should have known at the inception of this litigation that the records...were relevant to the matters in issue...and likely to be requested by Thompson during the litigation...[T]he Special Master ordered GNC to preserve all...records maintained by GNC in the ordinary course of its business at its headquarters...GNC employees were not instructed ... to preserve...records as required by the ...Order. GNC’s president ... issued a memorandum...to all GNC personnel advising them that the Order ‘should not require us to change our standard document retention or destruction policies or practices’. This instruction on its face appears to instruct GNC employees to conduct their destruction procedures as they had done in the past and it was so interpreted by the GNC employees.” The court struck GNC’s answer, entered default judgment against it, dismissed its complaint in a related case. The Court specifically rejected lesser sanctions. See also RKI, Inc. v. Grimes, 177 F.Supp.2d 859 (N.D. Ill. 2001) (Court determined that Defendant defragmented his home computer attempting to hide from plaintiff that defendant had deleted confidential information and software. The court sanctioned Defendant \$100,000 in compensatory and \$150,000 in punitive damages, attorneys’ fees, and court costs); Trigon Ins. Co. v. United States, 204 F.R.D. 277 (E.D.Va. 2001). (Willful destruction of documents results in adverse inference, expenses and attorneys fees in the amount of \$179,725.70).

Data does not necessarily have to be destroyed to result in sanction. Sanctions have been issued in cases in which data was withheld (DeLoach v. Philip Morris Co., 206 F.R.D. 568 (M.D.N.C. 2002). Plaintiffs given opportunity to respond to Defendant’s expert report, and Defendants denied opportunity to reply where Defendant failed to produce to Plaintiff certain database data on which Defendant’s expert relied); Sheppard v. River Valley Fitness One, 203 F.R.D. 56 (D.N.H. 2001) Court sanctioned attorney for lack of diligence in obtaining and producing computer records; GTFM, Inc., v. Wal-Mart Stores, 2000 U.S. Dist. LEXIS 16244 (S.D.N.Y. Nov. 8, 2000) Defendant must pay costs incurred by plaintiff from defendant’s failure to disclose the capabilities of the defendant’s computer system.

The powerful impact that computer forensics can have upon a case is perhaps best illustrated in Metropolitan Opera Assoc., Inc. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003). In this case, counsel for Local 100 tried very hard to avoid producing data on relevant computers. The District Court for the Southern District of New York reviewed the history of counsel’s efforts as follows:

[C]ounsel (1) never gave adequate instructions to their clients about the clients' overall discovery obligations, what constitutes a 'document'...; (2) knew the Union to have no document retention or filing systems and yet never implemented a systematic procedure for document production or for retention of documents, including electronic documents; (3) delegated document production to a layperson who (at least until July 2001) did not even understand himself (and was not

instructed by counsel) that a document included a draft or other non-identical copy, a computer file and an e-mail; (4) never went back to the layperson designated to assure that he had 'establish[ed] a coherent and effective system to faithfully and effectively respond to discovery requests,'...and (5) in the face of the Met's persistent questioning and showings that the production was faulty and incomplete, ridiculed the inquiries, failed to take any action to remedy the situation or supplement the demonstrably false responses, failed to ask important witnesses for documents until the night before their depositions and, instead, made repeated, baseless representations that all documents had been produced.

Based upon these actions, the Court ordered a computer forensic expert to assist Local 100. Rather than submit to any forensic examination, Local 100 disposed of all relevant computers. When advised that the Local had simply thrown relevant computers away, the Court sanctioned the Union, granting judgment against the Union on the merits of the case, and ordering the Union to pay Plaintiff's attorney fees related to discovery. The Court rejected less severe sanctions including adverse inference and preclusion on ground **“ it is impossible to know what the Met would have found if the Union and its counsel had complied with their discovery obligations from the commencement of the action.”**

Traditionally, sanctions were applied to the intentional destruction of evidence. It is significant to note that at least one court has held that mere **negligence** in preserving or promptly producing electronic information is sanctionable. Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. 2002). This is an important case, because the parties agreed that the email eventually produced during trial did not contain any relevant information. Nevertheless, the District Court vacated the trial court's order denying sanctions (adverse inference instruction) and held that pursuant to Rule 37(b)2, Federal Rules of Civil Procedure, the trial court has power to “make such orders in regard to the failure [to obey an order to provide or permit discovery] as are just.” The Court also reasoned that Rule 37(c)(1), amended Dec. 2000, provides that failure to supplement discovery results in exclusion of the evidence and permits the Court to “impose other appropriate sanctions ... and may include informing the jury of the failure to make the disclosure... The sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence.” Id. at 108.

To obtain an adverse inference instruction, the movant must present sufficient evidence from which a reasonable trier of fact could infer that the evidence destroyed or not produced "would have been of the nature alleged by the party affected by its destruction" or non-production. The burden of proof on the movant, however, should not be “too strict a standard of proof” so as not to “subvert the ... purposes of the adverse inference” Id. at 108-09. Significantly, the Second Circuit Court noted that where a party fails to hire an expert to assist with electronic production as soon as the party determines that it cannot retrieve the data, and the continued reliance upon an expert that cannot produce results, may create an inference of a “culpable state of mind” supporting a determination that the party is acting in bad faith. Id. at 111.

Not all courts grant sanctions based solely upon the destruction of evidence. Where the data destroyed bears no possible relationship to the matters being litigated, courts have denied sanctions. Hildreth Manufacturing, L.L.C. v. Semco, Inc., 151 Ohio App.3d 693 (3<sup>rd</sup> Dist. App. Ct. Marion Cty) (Third District Appellate Court, Marion County, affirms the decision of the Marion County Common Pleas Court, denying Semco's Motion for Contempt against Hildreth for spoliation of evidence on the ground that the Trial Court properly determined that there was no reasonable possibility that the missing hard drives contained evidence of the theft of trade secrets. Semco had argued that sanctions were proper under Rule 37(B)(2)(e), Ohio Rules of Civil Procedure and pursuant to case law in Bright v. Ford Motor Co. 63 Ohio App.3d 256, 578 N.E.2d 547 (1990). Bright Court held that sanctions against a plaintiff for the willful destruction of evidence in violation of a protective order, required that plaintiff be given an opportunity to overcome a presumption that the defendant had been prejudiced. "A sanction which in effect puts a party out of court must be based on demonstrable prejudice to the opposing party...A workable formulation of prejudice for purposes of this case is: a reasonable possibility, based on concrete evidence, that access to the unaltered (requested evidence) would have produced evidence favorable to the (defendants), which was not otherwise obtainable." Bright at 259. Rule 37(B)(2)(e) provides "If any party...fails to obey an order to provide or permit discover,...the court in which the action is pending may make such orders in regard to the failure as are just, and among others the following:...An order...rendering a judgment by default against the disobedient party." Appellate Court reasoned that Hildreth adequately rebutted the presumption of prejudice by showing that a reasonable possibility did not exist that hard drives used by a CNC machine in the normal course of the operation of that equipment, contained evidence of customer lists or other intellectual property.

## CONCLUSION

Federal and state courts are quickly recognizing the unique challenges and advantages of discovering data relevant to a matter that resides on electronic media. The challenges are to preserve the data from destruction by forces including the computer's operating system, and to protect privileged data. The advantages are that the data can be identified and extracted using a computer forensic protocol that is non-disruptive, economical, and very powerful. Computer forensic analysis is replacing production of documents as the standard means of discovery, and offering attorneys a value-neutral mechanism to quickly determine all the facts in any case.

"Judges are getting the message. It makes more sense to look to one neutral expert, with the appropriate protocols, rather than relying on the parties to do it and duplicate their expense and effort." Playboy Enterprises, Inc. v. Welles, 60 F.Supp.2d 1050 (S.D. Cal. 1999). Simon Property Group v. mySimon, Inc. 194 F.R.D. 639 (S.D.Ind. 2000).