12-31-2007

Computer Forensics, E-Discovery, and Spoliation: Impact of the New Federal Rules

Burke Ward
Villanova University

Janice Sipior
Villanova University

Linda Volonino
Canisius College

Georgina Peterson

COMPUTER FORENSICS, E-DISCOVERY, AND SPOLIATION: IMPACT OF THE NEW FEDERAL RULES

Burke T. Ward, Marketing & Business Law, School of Business, Villanova University, USA burke.ward@villanova.edu
Janice C. Sipior, Decision & Information Technologies, School of Business, Villanova University, USA janice.sipior@villanova.edu
Linda Volonino, Information Systems, Richard J. Wehle School of Business, Canisius College, USA volonino@canisius.edu
Georgina R. Peterson, JPMorgan Chase & Co., Newark, Delaware, USA georgina.roselli@villanova.edu

Abstract

A challenge for organizations is to manage electronic information without exposing the organization to sanctions in a later lawsuit. Since organizations do not usually voluntarily disclose internal information, the recent amendments to the Federal Rules of Civil Procedure, applicable to the discovery process, can compel an organization to permit an examination of electronically stored information. Failure to comply can result in sanctions. This paper examines the legal discovery process, including e-discovery and spoliation, and proposes record retention policies and practices.

Keywords: computer forensics, e-discovery, spoliation.

Introduction

Organizations have been beset by civil and criminal litigation, with electronic business records used as evidence to indict managers. Internal organizational records, on seemingly harmless laptops, servers, jump drives, personal digital assistants (PDA) or backup tapes, may contain evidence of culpability, or other information damaging to a party in litigation. Ninety-three percent of all business documents are created electronically, and nearly one-third of all electronically stored data is never printed out (Oostenrijk 2005). Emails are "fertile ground for unearthing damaging documents" (Brownstone 2004), as are instant messages. Some lawyers even refer to email as "evidence mail" (Murphy 2005). In response to the ever increasing use of email and the digital preparation of most business records, computer forensics is increasingly important in records and information management (RIM).

This paper discusses computer forensics and its importance in litigation. The legal discovery process, including e-discovery, and spoliation, will be examined. The recent amendments to the Federal Rules of Civil Procedure, effective December 1, 2006, affecting discovery, e-discovery, and spoliation, and the implications for organizations will be discussed. Finally, we encourage organizations to formulate and implement a comprehensive Data Retention Policy which considers both traditional and electronic records, with proactive and reactive plans for the possibility of e-discovery proceedings.

Computer forensics

Computer forensics focuses on the preservation, identification, extraction, and documentation of computer information (Cavaliere 2001; Mercer 2004). In litigation, if the information taken from the system is to withstand judicial scrutiny, it is imperative that the work be done by a computer forensics expert, and that all irregularities in the data are documented. This includes any inconsistencies between the original hard drive and the mirror-image copy. If all proper safeguards and forensics methodologies are used, this should ensure that the digital evidence is preserved to allow admissibility at trial (Borck 2001). Further, electronic evidence is regarded as easier to obtain than traditional paper evidence, due to the convenience and ease of transferring and storage (Givens 2003). The total destruction of an electronic file is much more difficult; it cannot be as easily shredded, buried, or burned like its "physical copy-only" predecessors (Withers 2000).

Data contained on a computer hard drive needs to be carefully extricated. Since booting up or shutting down the computer risks losing or overwriting the memory and temporary files, extreme care must be used when extricating the files from the computer. It is imperative that a copy of the original is made using the least intrusive manner available. If any inadvertent changes occur to the original drive data during extrication, these would need to be documented (Bigler 2001). The duplicate image must produce the same output as the original. This means that the sixteen-character hexadecimal numeric value representing the data set of the original must match that of the mirror-image copy (Mercer 2004). This is similar to matching DNA in a criminal investigation. The original is never analyzed; instead the mirror-image copies are used for analysis. This is because booby traps and logic bombs may be present. Logic bombs can, for example, erase data if not properly dismantled (Dees 2004; Borck 2001; Kabay 2002).

After original data is copied, files need to be properly identified. All historic descriptive information, known as metadata, including file characteristics such as the date of file creation, deletion, and the last time it was viewed must be noted (Borzych 2005). The metadata may contain relevant information (Beckman 2006). Furthermore, any additional removable media, which could contain data that is not available on the hard drive, needs to be identified and properly catalogued.

When analyzing data, there are many aspects to examine. Active data is the information readily accessible to users, including spreadsheets, text documents, databases, email, and address books. This data is available on the hard drive and is also present on backup tapes. Comparisons of computer backups to existing physical documents can show how and when a document was altered. Computer logs will track network usage, including when files were downloaded, copied, printed, or purged (Todd 2004). More important information may be found within the deleted data.

Deleted and residual data

Deleted and residual data are not included on backup tapes and need to be extracted from the hard drive. In Windows, when a file is deleted and the recycle bin is emptied, the data on the surface of the disk is marked as fit for overwriting with new information, but the old information has not been removed (Castelluccio 2002). Unless new data is written to every segment of the disk that contained the old file, fragments of the old file will remain. These fragments can be pieced together so that part, or all, of the original file can be reconstructed (Knight, 2004). It is an accepted proposition that deleted data, whether emails or documents, are considered by the court to be discoverable (Borzych 2005).

File slack

When a file is saved, it is assigned a particular number of clusters or bytes depending upon the file's size. The number of bytes is equal to or greater than the size of the actual file. Therefore, there is usually unused space at the end of the file on the hard drive. This space between the actual end of the file and the end of the allocated space is called slack. File slack may contain data from a previous file that the cluster held before being assigned to the current file (Bigler 2001). This slack could potentially contain valuable information.

Swap file

A Windows swap file is created when the computer, on which a project is being completed, does not have enough RAM to hold the work. Windows then moves a portion to the hard drive, creating additional virtual RAM. This additional RAM can actually be fairly substantial, and also hold untold secrets, similar to file slack. Ambient data, terminology coined by New Technologies, Inc., describes all the data stored in the file slack, Windows swap file, and unallocated disk space (Castelluccio 2002). This could potentially contain important information and needs to be thoroughly searched by the forensics specialists. Swap files are at risk of being inadvertently deleted if the computer is booted up (Schultz and Keena 2001), making it imperative that a mirror-image copy of the drive be created.

Integrity of forensics process

Software used in forensics automatically signs the disk before analysis begins and each time a change is made. Each investigator has a unique signature, ensuring a complete audit trail of the process. "For admissibility in court, the evidence should possess a chain of custody to show that no inadvertent or purposeful contamination occurred" (Mercer 2004).

Discovery

Discovery is the formal pre-trial process whereby litigating parties discover and obtain information. Subject to certain exceptions, such as privileged information, the scope of discovery is relevancy. Admissibility is not an issue in discovery. Rule 26 (b) (1) of the Federal Rules of Civil Procedure (FRCP) states that:

Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.

Discoverable items include hard-copy documents and any data stored in electronic format. Electronic discovery is the process of acquiring and presenting electronic information in the discovery phase of litigation. The process of acquiring electronic information includes forensics and retrieval of information. Presenting electronic information includes organization and indexing, presentation in a searchable format, enabling document production with the information, and packaging for presentations (Brown 2003). Digital information from any source, including primary files, copies, versions, metadata, system data, legacy data, and backup data, is discoverable if relevant and not privileged (Withers 2006).

Amendments to the Federal Rules of Civil Procedure

On December 1, 2006, amendments to the FRCP, relevant to e-discovery, became effective. These amendments to Rules 16, 26, 33, 34, 37, and 45 are intended to bring the discovery rules up-to-date in an information age (Finnegan and Wein 2006). The amendments to rules 26, 34, and 37 are most relevant to the scope of this paper.

Although extended by case law, amended Rule 34 (a) specifically extended the scope of discovery to electronically stored information. Rule 34 (a) states:

Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained — translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served;

Prior to the amendments, all discoverable information was treated the same, whether physical or electronic. The amendment to Rule 26 (b) creates a two-tier classification to electronically stored information. Rule 26 (b) (2) (B) states that:

(B) 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). The court may specify conditions for the discovery.

Thus the amendment creates a distinction between electronically stored information that is reasonably accessible, and that which is "not reasonably accessible." What does this mean? Neither the Rule, nor the Advisory Committee report defines these terms. The Advisory committee gives as examples, of costly or burdensome retrieval, "deleted information, information

kept on some backup tape systems for disaster recovery purposes, and legacy remaining from systems no longer in use." (Beirne et al. 2006).

The Rule's standard is "not reasonably accessible because of undue burden or cost." Because of the Rule's vagueness, guidance will have to come from judicial precedent. The leading case on this issue is *Zubulake v. UBS Warburg* (2003). *Zubulake* was an employment discrimination case. One of the initial issues was the plaintiff's discovery demands for back emails. The defendant claimed that the requested information was inaccessible, in part because of cost. In deciding this issue, Judge Scheindlin looked to the type of media on which the information is stored, and the cost of its production. She created five categories, presented in Table 1.

Table 1. Categories of media to determine accessibility of electronically stored information

1**. Active, online data***:* "On-line storage is generally provided by magnetic disk. It is used in the very active stages of an electronic records [sic] life-when it is being created or received and processed, as well as when the access frequency is high and the required speed of access is very fast, i.e., milliseconds." Examples include hard drives.

2**. Near-line data***:* "This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records. Access speeds can range from as low as milliseconds if the media is already in a read device, up to 10-30 seconds for optical disk technology, and between 20-120 seconds for sequentially searched media, such as magnetic tape." Examples include optical disks.

3. **Offline storage/archives***:* "This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered 'archival' in that their likelihood of retrieval is minimal. Accessibility to off-line media involves manual intervention and is much slower than on-line or near-line storage. Access speed may be minutes, hours, or even days, depending on the access-effectiveness of the storage facility." The principled difference between nearline data and offline data is that offline data lacks "the coordinated control of an intelligent disk subsystem," and is, in the lingo, JBOD ("Just a Bunch Of Disks").

4. **Backup tapes***:* "A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. Their transfer speeds also vary considerably ... The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks." As a result, "[t]he data on a backup tape are not organized for retrieval of individual documents or files [because] ... the organization of the data mirrors the computer's structure, not the human records management structure." Backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression.

5. **Erased, fragmented or damaged data***:* "When a file is first created and saved, it is laid down on the [storage media] in contiguous clusters ... As files are erased; their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining contiguous free space. These files are then broken up and randomly placed throughout the disk." Such broken-up files are said to be "fragmented," and along with damaged and erased data can only be accessed after significant processing.

In the determination of whether electronically stored information is accessible for e-discovery, Judge Scheindlin stated,

Of these, the first three categories are typically identified as accessible, and the latter two as inaccessible. The difference between the two classes is easy to appreciate. Information deemed "accessible" is stored in a readily usable format. Although the time it takes to actually access the data ranges from milliseconds to days, the data does not need to be restored or otherwise manipulated to be usable. "Inaccessible" data, on the other hand, is not readily usable. Backup tapes must be restored using a process similar to that previously described, fragmented data must be de-fragmented, and erased data must be reconstructed, all before the data is usable. That makes such data inaccessible.

Backup technologies have improved since *Zubulake* in 2003. Today, more organizations are choosing backup and recovery services delivered over the internet or disk-based backups. These newer technologies do not have the sequential access problem of tape drives. Thus, the information should be in an accessible and readily useable format (Riedy and Beros 2006). Even if the information is accessible, the cost of production may be considered an "undue burden or cost."

Cost of e-discovery

The cost of discovery is usually borne by the producing party (*Sedona Guidelines* 2005). However, Rule 26(b) (2) (C) states that "[T]he frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues." Courts have used this provision to order a cost shifting, or cost sharing between the requesting and producing parties. This approach is essentially one of weighing and balancing.

The leading case on this issue is, again, *Zubulake v. UBS Warburg*. Zubulake wanted an extensive e-discovery order to be issued for backed up email. UBS Warburg argued that the expense was an undue burden, in part, because of cost. The Court eventually ordered cost-splitting. The Court evaluated the cost-splitting based upon a seven-factor test, developed by Judge Scheindlin. Each of the factors is weighed dependent upon its importance. The seven factors are:

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 cost and its incentive to do so
6. The importance of the issues at stake in the litigation
7. The relative benefits to the parties of obtaining the information

Ultimately, the plaintiff was required to bear 25% of the cost associated with the restoration of backup tapes; the defendant would bear the remaining 75% of restoration cost, plus all other costs relating to searching and reviewing the restored emails (Jones 2003).

Spoliation

Preservation letters should be sent to all parties and non-parties in possession of potentially relevant data at the onset of litigation. A preservation order should be tailored to the particular issues involved in the specific litigation to ensure a candid and expeditious discovery process (Marcus 2004). It is also important that the preservation letter contain a request for the computer to be taken out of service until the mirror image can be created (Borzych 2005). This is important since simply

turning on the computer can alter the data it contains (Shariati 2004). Regardless, a party's responsibility to preserve evidence does not begin when process is served; instead, it begins at the moment when litigation can be reasonably anticipated (Arent et al. 2002).

Spoliation is "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation," (Watson 2004). Spoliation can encompass four distinct torts (O'Hara and Gennaro 2004):

1. Intentional spoliation by a party to underlying litigation
2. Negligent spoliation by a party to underlying litigation
3. Intentional spoliation by a third party not a party to underlying litigation
4. Negligent spoliation by a third party not a party to underlying litigation

In most cases, the durability of electronic evidence stands in the way of spoliation (Givens 2003), yet some still find a way to commit it. The most common practices causing spoliation of evidence are the failure to discontinue document-destruction policies, the improper collection and imaging of the electronic data, and the modification of websites (Schultz and Keena 2002). People are more prone to deleting emails and documents from their systems as they have become more cognizant of the danger of archived files. "The fact of deletion can lead to a court's imposing serious sanctions for attempting to destroy relevant evidence" (Benson 2004) if relevant information was deleted from a computer during litigious proceedings, at a time when there is a legal obligation to preserve all evidence. Parties can be sanctioned for spoliation under Rule 37 in the FRCP or through a court's inherent power (Scheindlin and Wangkeo 2004). Rule 37 itself does not specifically authorize the imposition of sanctions for spoliation, but the court has relied on subsets (b) and (c) of Rule 37 when imposing such sanctions. This is because a party has "destroyed documents in violation of a court order or the destruction of documents has rendered a party unable to comply with its disclosure obligations under the Rules" (Scheindlin and Wangkeo 2004). Sanctions can range from adverse inferences or presumptions, preclusion of evidence, monetary sanctions, to dismissal or default. "Courts have found that a dismissal or default is justified when a party destroys evidence with the intent to subvert discovery. Thus courts can dismiss an action or render a default judgment when the spoliator's conduct was egregious, the prejudice to the non-spoliating party was great, and imposing a lesser sanction would be ineffective to cure the prejudice" (Shapiro and Kilpatrick 2004). At the federal level, criminal penalties apply to the obstruction of justice through destruction of evidence. Spoliation can also lead to a party being held in civil or criminal contempt.

A troublesome issue is the destruction of relevant information pursuant to a good-faith records and information management (RIM). The case law on spoliation sanctions for destruction pursuant to a RIM is very inconsistent. In response to this inconsistency, Rule 37 was amended. Amended Rule 37 (f) provides a safe harbor for organizations which establish and follow automated RIM systems operated in good faith. Amended Rule 37 (f) states:

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.

As discussed below, this safe harbor is narrow, not broad.

Retention policies

Organizations need a RIM policy, not only for every day operational purposes, but increasingly for compliance (Torres 2006). In addition to the discovery and spoliation issues discussed above, RIM policies are necessary for regulatory compliance. For example, the United States Internal Revenue Service has stated that willful failure to maintain tax-related digital records could lead to criminal penalties (IRS Rev Proc 98-25, Section 12). Similarly, the 2002 passage of the Sarbanes-Oxley Act stipulated that CEOs and CFOs can be fined and/or imprisoned for false certification of financial statements (Andolsen 2004). According to Forrester Research, the realization that RIM policies are necessary for compliance is driving enterprise content management technologies markets ("Catalyst of Cataclysm?" 2004).

Electronic data is often recycled or overwritten as part of routine business practices (Scheindlin and Wangkeo 2004) because businesses simply cannot retain volumes of outdated information due to finite physical space and budgets. Moreover, records that have ceased to have operational or legal value, and that are retained unnecessarily, are subject to potential discovery (Launchbaugh 2004). Therefore, it is important for a company to have a comprehensive Data Retention Policy that coordinates retention of both electronic and traditional documents (Shapiro and Kilpatrick 2004). This policy should be enacted in good faith before there is a pending litigation. Built into the records management policy should also be a discovery response plan that contains policies and procedures for responding to discovery in a timely, responsible manner (Launchbaugh 2004).

According to Kahn (2005), 80% of organizations have recently made or are planning to make changes in the way they manage information. A thorough Data Retention Policy should meet the following criteria (Kiel et al. 2005):

1. comply with statutory or regulatory obligations that govern different types of documents retained.
2. specify the length of time that each type of document is retained.
3. establish a method of destruction and a destruction schedule.
4. provide a detailed protocol for halting routine destruction in the event of anticipated or actual litigation

In an age where email is often a primary source of legal discovery, a survey fund that 59% of organizations do not have a formal email retention policy (Winkler 2005). It is imperative that email usage and content rules be established. The organization's records retention schedule should also be applied to email records management (Murphy 2005).

As discussed previously, new rule 37(f) creates a safe harbor for "electronically stored information lost as a result of the routine, good-faith operation of an electronic system." "System" is not defined, but seems to apply only to automated procedures. This rule lessens the likelihood that an organization will be subjected to judicial sanctions for routine automated

recycling of electronic data, as long as the company did not intentionally destroy any discoverable information in defiance of a preservation order, or with knowledge of pending litigation (Moore 2007).

Conclusion

A challenge for organizations is to manage information and document retention without exposing the organization to sanctions in a later lawsuit. Courts have struggled with the demands of electronic discovery, and the issue of sanctions for intentional or unintentional failure to comply. The recent amendments to the FRCP are an attempt by the U.S. legal system to address the issues of electronic record retention as information technology continues to advance. Organizations must respond to the necessity to address RIM by developing and implementing a comprehensive Data Retention Policy for compliance and litigation purposes. The policy is not absolute protection from sanctions, but at a minimum creates a credible defense. Further, if such a policy is automated, the recent amendments to the FRCP afford a higher level of protection from sanctions

References

Andolsen, A. A. "RIM & RIO: Investing wisely for the future," *Information Management Journal* (38:5), 2004, pp. 47-54.

Arent, L. M., Brownstone, R. D., and Fenwick, W. A. "Ediscovery: Preserving, requesting, and producing electronic information," *Santa Clara Computer and High Technology Law Journal* (19:131), 2002.

Beckman, B. "Production, Preservation, and Disclosure of Metadata," *Colum. Sci. & Tech. L. Rev*. (7:1), 2006.

Beirne, M. D., Pluchinsky, D. A., and Murr, G. B. "Federal Rule of Civil Procedure 26(B)(2)(B) and the 2006 Amendments," *Andrews Product Liability Litigation Reporter* (17:11), December 14, 2006, 7 pp.

Benson, R. J. "The Increasing Significance of Computer Forensics in Litigation," *Intellectual Property & Technology Law Journal* (16:11), 2004, pp. 1-4.

Bigler, M. "Computer Forensics Gear," *Internal Auditor* (58:4), 2001, p. 27.

Borck, J. R. "Leave the cybersleuthing to the experts," *InfoWorld* (23:25), 2001, p. 54.

Borzych, M. E. "Avoiding Electronic Discovery Disputes," *Arizona Attorney* (41:36), 2005.

Brown, T. "Electronic Discovery Basics," *Rhode Island Bar Journal* (52:71), 2003.

Brownstone, R. D. "Collaborative Navigation of the Stormy E-discovery seas," *Richmond Journal of Law & Technology* (10:53), 2004.

Castelluccio, M. "Computer Forensics – A cheat sheet," *Strategic Finance* (84:2), 2002, pp. 59-60.

"Catalyst or Cataclysm?" *Information Management Journal* (38:5), 2004, pp. 4-7.

Cavaliere, F. J. "The Web-wise Lawyer," *Practical Lawyer* (47:4), 2001, pp. 9-10, 60.

Dees, T. "New Computer Forensics Tools," *Law & Order* (52:6), 2004, pp. 24-25.

Federal Rules of Civil Procedure, http://www.law.cornell.edu/rules/frcp/

Finnegan, J. S. and Wein, A. "Coping with New Rules for E-discovery" *Product Liability Law and Strategy* November 16, 2006.

Givens, J. S. "The Admissibility of electronic evidence at trial," *Cumberland Law Review* (34:95), 2003.

Jones, N. A. "Who Should Pay for Electronic Pre-trial Discovery?" *Daily Record* 6 August, 2003.

Kabay, M. E. "Logic Bombs, Part 1," *Network World Security Newsletter* August 21, 2002.

Kahn, R. A. "Stand and Deliver," *Information Management Journal* (39:3), 2005, pp. 26-33.

Kiel, D. W., Helmer, K. D., and Henderson, T. E. "What clients can do to prepare for e-discovery," *New Jersey Law Journal* April 25, 2005.

Knight, W. "Chasing the elusive shadows of e-crime," *New Scientist* (182:2446), 2004, pp. 26+.

Launchbaugh, C. "E-records Management: A sad state of affairs or golden opportunity?" *Information Management Journal* (38:3), 2004, pp. 20-24.

Marcus, R. "Only Yesterday: Reflections of rulemaking responses to e-discovery," *Fordham Law Review* (73:1), 2004.

Mercer, L. D. "Characteristics and Preservation of Digital Evidence," *FBI Law Enforcement Bulletin* (73:3), 2004, pp. 28+.

Moore, L. "Document Retention Policies Under New E-Discovery Rules" *Virginia Lawyers Weekly* January 29, 2007.

Murphy, B. "Preventing Mistakes in E-mail Records Management," *The CPA Journal* (75:7), 2005, p. 14.

O'Hara, J. and Gennaro, M. I. "The Duty if Corporate Counsel to Preserve Evidence," *Connelly Foley CF* 14 September, 2004, p. 26.

Oostenrijk, L. S. "Comment: Paper or Plastic?: Electronic Discovery and Spoliation in the Digital Age," *Houston Law Review* (42:1163), 2005, 36 pp.

Scheindlin, S. A. and Wangkeo, K. "Electronic Discovery Sanctions in the Twenty-First Century," *Michigan Telecommunications and Technology Law Review* (11:71), 2004.

Schultz, D. H. and Keena, J. R. "Navigating the Perils of Discovery in the Electronic Information Age," *Michigan Bar Journal* (81:54), 2002.

Schultz, D. H. and Keena, J. R. "Put the byte on – Advancements in technology have complicated the discovery process, but Rule 16 provides some guidance," *Verdicts & Settlements* Sept. 26, 2001.

Sedona Conference "The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age," September 2005.

Shapiro, G. M. and Kilpatrick, B. A. "E-mail discovery and privilege," *The Corporate Counsel Review* (23:201), 2004.

Shariati, B. "Zubulake v. UBS Warburg: Evidence that the Federal Rules of Civil Procedure provide the means for determining cost allocation in electronic discovery disputes?" *Villanova Law Review* (49:393), 2004.

Todd, K. J. "Using Digital Evidence to Ferret out the Dishonest Employee," *Employee Relations Law Journal* (30:2), 2004, pp. 13+.

Torres, T. "Creating a Process-Focused retention Schedule" *The Information Management Journal*: September/October 2006.

Watson, L. M. "Anticipating electronic discovery in commercial cases," *Michigan Bar Journal* (83:31), 2004.

Winkler, D. "E-mail Management: Compliance, control, consolidation," *Computer Technology Review* (25:2), 2005, pp. 11-12.

Withers, K. J. "Electronically Stored Information: The December 2006 Amendments to the Federal rules of Civil Procedure," *4 Nw. J. Tech. & Intell. Prop. 171*, Spring 2006.

Withers, K. J. "Computer-based discovery in federal civil litigation," *Federal Courts Law Review* (2), 2000.

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003); 220 F.R.D. 212 (S.D.N.Y. 2003); 382 F. Supp. 2d 536 (S.D.N.Y. 2005).