Communications of the Association for Information Systems

Volume 12 Article 27

September 2003

Electronic Evidence and Computer Forensics

Linda Volonino
Canisius College, volonino@canisius.edu

Communications of the Association for Information Systems

ELECTRONIC EVIDENCE AND COMPUTER FORENSICS

Linda Volonino
Information Systems and Telecommunications
Canisius College
volonino@canisius.edu

ABSTRACT

Information and communication systems are now breeding grounds for electronic-evidence (e-evidence) in audits, investigations, or litigation. Increasingly organizations are being ordered by law or lawsuit to preserve, retrieve, and hand-over relevant electronic records (e-records) because "the courts are uniformly recognizing the discoverability of electronic communication and documents" [Nimsger and Lange, 2002]. This trend is an outgrowth of aggressive tactics by regulators to ensure corporate accountability and deter fraud.

In cases ranging from Securities and Exchange Commission probes of corporate malfeasance and insider trading to employment lawsuits, e-records are subpoenaed. Investigations conducted by the National Association of Security Dealers, Department of Justice, and Department of Homeland Security routinely require companies, their business partners, or third parties to preserve and disclose e-records, including internal e-mail and instant messages (IM). A high-profile example is the probe into alleged White House leaks of a covert CIA agent's identity in which White House employees received e-mail stating: "You must preserve all materials that might in any way be related to the department's investigation." E-mail, telephone logs, and other electronic documents were mentioned specifically.

Any communication or file storage device is subject to computer forensic searches to identify, examine, and preserve potential e-evidence—the electronic equivalent of a "smoking gun." Preserving e-records and then restoring them so that they can be searched can seriously disrupt IS and over-burden Information Systems staff. What's more, a preservation order might specify not only the type of e-records (data files or email), but also stipulate that processes that over-write data be suspended, or that backup tapes be retained for unspecified duration. These stipulations are very disruptive to IS operations. That disruption depends largely on whether the company had an e-record management (ERM) system to systemically review, retain, and destroy e-records received or created in the course of business.

This article presents an overview of e-evidence and computer forensics and their implications for Information Systems. It aims to encourage research into ERM and fully-indexed, searchable e-mail archives by providing compelling reasons for how these approaches mitigate e-evidence risks and cost. These research issues are important for several reasons. Rarely are IS

departments prepared for the challenges that evidentiary rules impose on active and archival data operations. Retaining unessential e-records increases costs and risks. Companies may need to justify their e-record retention and destruction policies as proof of compliance with their accounting, regulatory, or legal obligations. Courts impose severe sanctions on employers who claim they are unable to comply with e-record requests because of Information Systems design flaws or sloppy e-records management if it obstructs an investigation.

Keywords: electronic evidence, computer forensics, digital discovery, e-record retention and destruction, electronic records management, legal issues

I. INTRODUCTION

BUSINESSES' ELECTRONIC RECORDS CREATE RISK

It is common practice for businesses to retain electronically stored information because it is convenient and cost-effective to store records in electronic format and because regulations require companies to maintain certain business records. Less commonly known is that the numerous e-mail and Instant Messaging (IM) messages sent and received on company e-mail systems may also be considered business records by the courts. Judges and regulators view e-mail and IM messages as business records if communication via e-mail or IM is a standard business practice—or if those messages are created as part of operations [Sleek, 2000] (Appendix I.) Clearly, IM for business communications is the trend. IDC estimates that there will be more than 400 million IM accounts by 2004, with nearly half of them connecting businesses with their customers or clients [Smith, 2003].

The legal designation of e-mail and IM as business records is significant. Business records are subject to regulation and to pre-trial discovery, subpoena, or search warrant. Therefore, investigators use e-mail and IM records to create a "chain of evidence" proving illegal activity. With e-mail and IM sources of e-evidence, companies are exposed to risks of liability and litigation because:

Casual, private, or seemingly irrelevant e-mail messages or IM may be deemed business records, which even strongly worded disclaimers cannot repudiate.

Communications made in confidence are not protected from disclosure if they fit the legal definition of business record.

E-mail or IM that did not meet the definition of business record when they were created might nevertheless be required as evidence in court. For example, an administrative e-mail notice of a company softball game could be used as evidence in a workers' compensation claim if an employee is injured during the game [Flynn and Kahn, 2003].

Shoddy e-records management (ERM) exacerbates the risk of civil or criminal liability for improper destruction of e-records. Penalties for improper e-record destruction can be severe, as evidenced in December 2002 when regulators fined five Wall Street brokerages $8.3 million for failing to preserve e-mail messages [Smith, 2003]. The content and preservation of e-records will be subject to greater litigation and investigations under new legislation, such as the Sarbanes-Oxley Act, to deter corporate corruption and fraud.

SARBANES-OXLEY ACT

The Sarbanes-Oxley Act (SOX) that was signed into law in 2002 represents an aggressive effort by the U.S. Congress to address the data retention and preservation issues arising from the Enron and Arthur Andersen fraud cases. SOX included the creation of the Public Company Accounting Oversight Board to address corporate responsibility issues [Patzakis, 2003]. This law also:

1. Mandates the retention of electronic documents.

2. Mandates that companies produce their electronic records and other documents when summoned by the new Oversight Board.
3. Imposes strict criminal penalties for altering or destroying records, including those kept in electronic form.

Section 802 of SOX imposes fines of up to $25 million and/or 20 years imprisonment against:

> *"whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence" any government investigation or official proceeding."*

In like manner, the National Association of Securities Dealers (NASD) and several government regulatory agencies issued new regulations and guidelines that expand existing e-record retention requirements. Public companies will need ERM procedures for prompt recovery of e-evidence in the course of the internal audits and investigations that these rules and regulations will inevitably generate.

FEDERAL RULES OF CIVIL PROCEDURE

In 1970, Rule 34 of the Federal Rules of Civil Procedure (Fed. R. Civ. P.) was amended to address changing technology and communication. Amended Rule 34 made electronically stored information subject to "subpoena and discovery" for use in legal proceedings [Rasin and Moan, 2001]. This rule is the one that made e-records and communications breeding grounds for evidence of company activities and conduct. And every computer-based activity—whether it is sending email, invoices, viruses, or hack attacks—leaves an electronic trace.

FEDERAL RULES OF DISCOVERY

According to Rule 26 of the Federal Rules of Discovery (Fed. R. D.), each company has the duty to preserve documents that may be relevant in a case [Scheindlin and Rabkin, 2002a]. This duty to preserve is fundamental to, and inseparable from, the duty of disclosure. When involved in a legal action, companies are bound by the duty of disclosure to turn over requested e-records in readable format by a specified date.

Fed. R. D. categorize e-records as:

1. Computer-stored records. This category includes active data, replicated data, residual data, backup data, and legacy data.
2. Computer-generated records. This category includes cache files, cookies, Web logs, and embedded data or metadata.

The company must be able to produce all e-records that may be relevant in the case as requested in the subpoena, court order, or discovery motion. Furthermore, the Fed. R. D. specifically require that electronic documents be produced, regardless of whether or not paper versions are produced.

II. POWER AND PREVALENCE OF E-EVIDENCE

E-EVIDENCE

Broadly defined, e-evidence is electronically-stored information on any type of computer device that can be used as evidence in a legal action. Since e-mail can provide especially devastating evidence, the use of e-evidence is increasing. In a survey of 1,100 U.S. companies conducted by the American Management Association and the ePolicy Institute, 14% of respondents said they were ordered by a court or regulator to produce employee e-mail in 2002, which was up from 9% in 2001 [Zaslow, 2003]. Garry Mathiason, whose law firm defends major corporations in employment cases, reported that almost every case his firm handles includes a "smoking e-mail"

component [Varchaver, 2003]. In 2000, e-mail was the most common type of e-evidence, and was dubbed "evidence-mail." In legal actions where evidence-mail or other e-evidence is used, it is as powerful as a smoking gun or DNA evidence, and as hard to deny or refute [Varchaver, 2003].

Stricter regulatory compliance, primarily SOX in the financial sector and the Health Insurance Portability and Accountability Act (HIPAA) in health care, is also intensifying the demand for e-evidence. One of the first electronic document destruction cases under the SOX began in February 2002 when Ernst & Young (E&Y) received a subpoena from federal banking regulators. A former E&Y partner, Thomas C. Trauger, had been arrested and charged with fraudulent alteration of audit documents for NextCard Inc. Trauger allegedly altered portions of E&Y's electronic working papers for NextCard's 2000 audit to improve NextCard's financial condition. [*United States v. Trauger,* 2003].

COMPUTER FORENSICS AND E-EVIDENCE

Computer forensics is the search of computer and communication devices for existing or deleted e-evidence.

> *"Computer forensics is a mandatory process whenever the results of a computer investigation may ultimately be presented in a legal or administrative proceeding" Patzakis [2003].*

Computer forensics is typically a two-stage process:

1. The discovery, recovery, preservation and control of electronic data or documents.
2. The analysis, verification and presentation of e-evidence in court or investigations.

Federal and state investigations of fraud, negligence, antitrust, discrimination, intellectual property theft, viruses, and sabotage include computer forensic searches. The outcome of many corporate cases turns on evidence obtained through computer forensics, most prominently Enron, Chase, Imclone, and Microsoft. Computer forensics investigations also revealed deliberate attempts to obstruct justice by destroying evidence, which is a criminal offense.

Computer forensics can be used to detect, trace, or prove a diverse range of crimes or cause of action (Appendix III):

- fraud, negligence, malpractice
- theft of trade secrets, intellectual property
- violations of non-compete agreements
- safer design of a defective product
- privacy invasion, identity theft
- child pornography, violent crime
- money laundering, terrorist activity
- hacker activity, malware
- workplace harassment, discrimination, defamation

The following cases illustrate the use of computer forensics to find electronic proof of an illegal activity:

- In June 2002, supported by evidence from computer forensics investigations, a jury found Arthur Andersen LLP guilty of "wholesale destruction of documents." It was because of their document destruction—and not fraudulent accounting practices—that Judge Harmon imposed the maximum fine of $500,000 and five years probation on Andersen, which collapsed following its conviction [Eoannou, 2003].

- In the case against American Home Products, manufacturers and distributors of Fen-Phen, internal e-mail was subpoenaed and over 33 million emails were searched. Plaintiffs' computer forensics experts uncovered e-mail stating:

  > *"Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem?"* [Keena, 2002].

  American Home Products was charged with reckless indifference to human life, and settled the case for a record $3.75 billion.

- During the 2003 investigation of SoBig.F, the FBI subpoenaed an Arizona Internet service provider (ISP) to identify the criminal(s) responsible for the e-mail worm that the DHS believed originated from a posting on an Internet site [CNN Money, 2003].

- In September 2003, state and federal prosecutors for the first time searched IM records of licensed brokers and dealers investigating securities fraud [Smith, 2003]. Using evidence from the bank's IM archive, a former Bank of America broker was charged with grand larceny and securities fraud.[1]

- In October 2003, prosecutors confronted former Credit Suisse First Boston (CSFB) executive Frank Quattrone, charged with federal obstruction of justice, with copies of his e-mail in which he warned CSFB employees to clean out and destroy files amid investigations of the bank [Neumeister, 2003].

A computer forensics examination may help mitigate permanent data loss and indicate faulty e-record retention practices. Andersen's demise illustrates the importance of conducting a computer forensics investigation to locate and preserve e-evidence, or recover deleted information. In the Andersen case, the firm could neither convince federal officials nor the jury that the destruction of e-records was the unauthorized action of a few rogue employees and managers [Patzakis, 2003]. They also failed to prove that upper management did not tacitly endorsed the destruction.

Without doubt, the discovery of e-evidence assumed enormous importance in litigation. As regulatory agencies intensify investigation of corporate malfeasance and computer crimes, the obligations imposed on companies and their IS staff increases correspondingly. An overview of obligation and rights in legal actions is presented next.

III. E-EVIDENCE IN LEGAL ACTIONS

PRE-TRIAL DISCOVERY

In preparation for trial or other legal action, each party has the right to learn about, or discover, as much as possible about the opponent's case. This pre-trial process is called discovery. A discovery request is an official request for access to any type of information that may be considered evidence [Arent et al., 2002]. Information is discoverable (i.e., subject to discovery) if it is relevant to the facts that lead to the lawsuit or litigation, often regardless of whether or not it was personal or private [Gleim, et al. 1992].

As discussed in Section I, under discovery rules, litigants can be required to produce e-records by a specific date. Therefore, if an opposing party submits a discovery request for a company's e-mails or other e-records, the company is required by law to retrieve and produce those records in readable format. Generally, courts view the failure to disclose information as an attempt to hide guilt and obstruct justice. For example, a court fined Prudential Insurance Co. $1 million for not turning over electronic data because failure to disclose that data harmed a plaintiff's ability to

[1] U.S. companies are preserving IM archives to meet stricter regulatory and supervisory requirements.

establish legal claims against the company [Sleek, 2000]. The legal duty to preserve e-evidence is further complicated by the requirement that organizations that might be involved in legal action must take steps to preserve e-evidence even before being ordered to do so.

E-MAIL IN DISCOVERY

The types of electronic data typically sought in discovery are internally produced e-records and internal and external communications, primarily email. Flynn and Kahn [2003] report that discovery of e-mail occurs in nearly 100% of federal civil and criminal litigation cases and major employment disputes. They identified four reasons why e-mailis targeted, each of which directly relate to the management of IS and end-users.

1. People tend to be candid in e-mail messages, even if they are discussing confidential, incriminating, or criminal matters. E-mail records are notorious as sources of careless remarks that can cause devastating consequences in the courtroom.
2. Most organizations lack e-mail management, which increases the chance that damaging messages lurk somewhere in the e-mail system, servers, laptops, hand-helds, or backup tapes.
3. Producing e-mail, particularly if its unmanaged, can be too costly or inconvenient for a company. Faced with the costs or inability to respond to an e-mail discovery request within allotted time, a company may be forced to agree to huge settlements.
4. Despite the potential to waste millions of dollars or thousands of hours searching archived or deleted e-mail and other e-records, the courts ruled that e-mail searching is not "unduly burdensome."

Many companies are trying to determine how to organize their e-records systems for the eventuality of litigation, given that plaintiffs aggressively pursue them in discovery [Prywes 2002],. Prywes stressed that planning for e-records discovery is especially important for companies that make and sell products used by the public. These companies face almost certain litigation or product liability suits, including class action suits.

LANDMARK CASE ABOUT THE DISCOVERY OF E-EVIDENCE

In August 2003, U.S. District Judge Shira A. Scheindlin set forth a revised test for determining how electronic discovery costs should be allocated. Her decision in *Zubulake v. UBS Warburg,* [S.D.N.Y. May 13, 2003] is considered to be a landmark case setting precedent as to which party pays for discovery of e-evidence. When addressing the burden and expense issues associated with electronic discovery, the courts recognize five categories of stored data. These categories are:

1. *Active, online data*. This data is in an "active" stage in its life and is available for access as it is created and processed. Storage examples include hard drives or active network servers.
2. *Near-line data*. This data is typically housed on removable media, with multiple read/write devices used to store and retrieve records. Storage examples include optical disks or magnetic tape.
3. *Offline storage/archives*. This category represents data that is offline on tape or other removable computer storage medium. Offline storage of electronic records is traditionally used for disaster recovery or for records considered "archival" in that their likelihood of retrieval is minimal.
4. *Backup tapes*. Data stored on backup tapes is 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. Data stored on backup tapes is also

typically compressed, allowing storage of greater volumes of data, but also making restoration more time-consuming and expensive.

5. *Erased, fragmented, or damaged data*. This data was tagged for deletion by a computer user, but may still exist somewhere on the free space of the computer until it is overwritten by new data. Significant efforts are required to access this data.

For data in accessible format, the usual rules of discovery apply, which means that the responding party is required to pay for production. When inaccessible data is at issue (categories 4 and 5), the judge can consider shifting costs to the requesting party

IV. IMPACT OF DISCOVERY AND ORDERS TO PRESERVE E-EVIDENCE ON INFORMATION SYSTEMS

DISRUPTION OF INFORMATION SYSTEMS

As discussed in Sections I and II, a court or investigator may issue an evidence preservation order for a company's e-records, including active data, data archives, metadata, network logs, cookies, web usage logs, email, and IM. Almost without exception, this order will disrupt Information Systems. To ensure e-evidence preservation, backup or maintenance operations that might alter requested data or e-records must be prevented from doing so.

A company can be charged with an order that is even more disruptive to Information Systems than an order to preserve. A court may specifically order a company to freeze their backup tapes and "to create and retain new backup tapes on an ongoing basis after the litigation is under way" [Shear, 2003]. This freeze order impairs or complicates IS operations. An order to freeze backup tapes can generate significant costs if backup systems and schedules need to be reconfigured. For legal cases that span several years, the number of backup tapes that need to be managed and the risk of data corruption increase significantly.

COST AND COMPLEXITY OF RESPONDING TO DISCOVERY

Responding to a discovery request for a corporation's internal e-mail may seem simple and straightforward to the courts or lawyers. However, a company served with a request to produce e-mail messages faces time consuming and expensive processes. The cost and complexity depends on the volume of e-records, how they are organized, and their accessibility. The cost of responding to a discovery request can be in the millions of dollars if several years' worth of archived e-mail and files must be located, restored, sorted through, and cleansed to remove non-relevant confidential material [Sleek, 2000]. Those costs are often in the millions of dollars. At the extreme, Chief of Staff John Podesta estimated the cost of the effort to reconstruct, retrieve and analyze e-mail related to the Monica Lewinsky case to be $11.7 million [Streza, 2003].

Extensive spin-off costs may be associated with discovery. Searching through massive amounts of carelessly stored emails, server logs, or e-records can tie up a company' IS staff for days or weeks. Indiscriminately retaining or destroying information exposes companies to risks that are rarely considered. Streza describes those risks.

> *The e-mail may pull otherwise unknowledgeable witnesses into the litigation. They may add little, if anything, to the merits of the claims or defenses, yet they are corralled, interrogated and distracted from otherwise productive duties. Instead of uncovering truly relevant facts, producing e-mail prolongs and sidetrack the search for truth, and sometimes may even develop untruth. Some written communications found in e-mail just are not accurate*. [Streza 2003]

RESEARCH POSSIBLITIES

These risks to Information Systems show the importance of research in ERM and compliance monitoring methods to ensure that employees retain necessary e-records. New methods for

sorting, categorizing, retaining, and deleting e-mail and other electronic business documents are needed. In addition, while developments in storing and scanning technology increased the ease of storage, the volume and variety of e-records are expanding rapidly. For practical reasons, businesses must develop rules and procedures for deciding what they can discard and what they must retain [Scheindlin and Rabkin, 2002b]. Boeing, the world's largest aircraft manufacturer, illustrated how disruptive a discovery request can be when no ERM or searchable e-mail archive is in place.

CASE ON POINT: BOEING'S DISCOVERY REQUEST

In October 1997, Boeing announced a $1.6 billion write-off because of production problems earlier that year. When this news was released to the public, the value of the company's shares dropped so sharply that a class-action lawsuit for securities fraud was filed against Boeing [Melnitzer, 2003].

During the pre-trial investigation, the attorney for the plaintiffs (the party that is suing) learned that Boeing stored 14,000 e-mail backup tapes in a warehouse in Washington, D.C. The attorney filed a discovery request for all Boeing's e-mail related to their production problems. Company officials were required to produce those computer tapes for use as evidence. Boeing faced serious problems because the Information Systems staff could not figure out whose emails were on which tapes without restoring and searching all 14,000 of them.

Tapes are rarely configured so that they can be easily searched. They are the most common backup media, but are designed primarily for disaster recovery where the entire tape is reloaded. Regardless of how difficult or expensive it is to retrieve files from backup tapes, companies must comply with discovery requests and produce the emails or records that are requested [Varchaver, 2003]. Boeing’s only choice was to restore all tapes, which took thousands of hours of employee time. In addition to the huge cost of responding to the discovery request, the e-mails that Boeing produced for the plaintiffs' attorney contained so much damaging evidence that the company paid $92.5 million to settle the class-action case.

V. ERM

ERM (defined earlier as an acronym for Electronic Records Management) is used for "systemic review, retention, and destruction of documents received or created in the course of business" [Scheindlin ad Rabkin, 2002b]. It consists of a broad range of policies, procedures, classification schemes, and retention and destruction schedules for electronic records.

ERM POLICY CONSIDERATIONS

E-record retention and destruction policies can reduce costs and disruptions significantly. ERM reduces costs when requested information can be found promptly, preserved, and protected against accidental deletion. Disruptions are avoided because normal backup and overwriting procedures can continue to go on without bringing company information systems to a halt [Editor, 2002]. Scheindlin and Rabkin [2002b] recommend using separate servers for business documents to expedite the identification of privileged material in case of a discovery request. A study of record retention at DuPont validates this recommendation. The DuPont study revealed that more than 50% of documents the company collected for discovery requests between 1992 and 1994 should never have been retained [Melnitzer, 2003]. Because of poor ERM, DuPont estimated that it cost the company between $10 million and $12 million over those three years in unnecessary retention and production costs.

An ERM policy should incorporate several general considerations.

- The policy should address each type of data and where it is stored.
- A policy should also provide for emergency recovery of inadvertently destroyed data.
- User training, compliance, and enforcement must be considered.

The impacts of the failure to manage e-mail as part of an ERM program are shown in numerous litigation cases.

VI. CONCLUDING REMARKS

Since the 1990s, in the amount of electronic material that is discoverable for use as e-evidence increased significantly. in The number of cases that involve the discovery of electronic material also increased. By 2000, it was standard practice for lawyers who were engaged in discovery to request electronic information that was created, stored, transmitted, discarded, or deleted.

E-evidence, its preservation, and retrieval are issues that urgently need to be researched by those in Information Systems. IS researches may have avoided these challenging issues because they require legal knowledge. Regardless of reason, these research challenges cannot be ignored given that e-mail and other e-records are the primary source of evidence in many controversies and legal matters. When companies fail to manage their e-records, they face severe sanctions by the courts, disruption of computer operations, and considerable costs.

Once litigation begins, it is too late for planning. Companies expose themselves to financial risk and criminal charges if their policy for retaining and destroying of e-records is not sound and comprehensive. The pervasive and haphazard use of e-mail and IM make them the greatest source of risk, expense, or embarrassment for companies. Proper ERM procedures based on duties to preserve and disclose e-records are needed to reduce a company's exposure to IS disruption and obstruction charges.

Editor's Note: This paper is based on a tutorial originally presented by the author in August 2003 at the AMCIS meeting in Tampa Fl. The manuscript was received on October 13, 2003 and was published on October 24, 2003.

REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Arent, L. M., R. D. Brownstone, and W.A. Fenwick. (2002) "E-Discovery: Preserving, Requesting and Producing Electronic Information," *Santa Clara Computer and High Technology Law Journal*. 19 (131) December.

CNN Money. (2003) "FBI subpoenas ISP Over SoBig," (current August 23, 2003). http://cnnfn.com/2003/08/23/technology/sobig_subpoena.reut/index.htm

Editor interview of Michael Prounis (2002). "Plan For Electronic Discovery Now—And Avoid "Bet The Company" Mistakes." *The Metropolitan Corporate Counsel*. August. p. 24.

Enneking, N. E. (1998) "Managing E-mail: Working Toward an Effective Solution." *Records Management Quarterly*. 32(3), July. p. 24.

Eoannou, C. L. (2003) "Briefs Filed in High-Profile Fifth Circuit 'Case about Document Destruction'," *Digital Discovery and e-Evidence* 3(7) July. pp. 1-2.

Flynn, J. P. and S. M. Finkelstein. (2002) "Tactic: A Primer on E-VIDE-N.C.E." *American Bar Association Litigation* (34). Winter.

Flynn, N. and R. Kahn. (2003) *E-Mail Rules*. New York: AMACOM. p.108.

Gleim, I N., J. B. Ray, and E. P. O'Connor. (1992) *Business Law/Legal Studies*. Gainsville, FL: Gleim Publications, Inc.

Gordon, M. (2002) "WorldCom Stock Drops to 6 Cents," AP Wire Story. July 1. 12:58 p.m.

Grimaldi, James V. (Mar. 16, 1999) "The Gates Deposition: 684 Pages of Conflict," *Seattle Times*, p. A1.

Keena, J. R. (2002) "E-Discovery: Unearthing Documents Byte by Byte," *Bench & Bar of Minnesota,* Mar. 2. http://www2.mnbar.org/benchandbar/2002/_mar02/_ediscovery.htm (current August 2003).

Melnitzer, J. (2003) "Keeping Track of the Invisible Paper Trail: What Legal Departments Can Learn From Boeing's Experience," *Corporate Legal Times*. February p. 15.

Neumeister, Larry (Oct. 12. 2003) "Prosecutors Use E-Mails Against Banker," *Associated Press*.

Nimsger, Kristin M. and Michele C.S. Lange. (2002) "Computer Forensics Experts Play Crucial Role." *The Lawyers Weekly*. 22(2) May 10.

Patzakis, J. (2003). "New Accounting Reform Laws Push For Technology-Based Document Retention Practices," *International Journal of Digital Evidence* 2(1) Spring.

Prywes D. I. (2002) "Discovery of Electronic Records: Preparing for the Inevitable," *The Brief*., 31(33). Summer

Scheindlin, S. A. and J. Rabkin. (2002a) "Outside Counsel Retaining, Destroying and Producing E-Data: Part 1," *New York Law Journal.* (227) May 8.

Scheindlin, S. A. and J. Rabkin. (2002b) "Outside Counsel Retaining, Destroying and Producing E-Data: Part 2," *New York Law Journal*. (227) May 9.

Shear, K. R. (2003) "Orders Freezing Backups—An Approach that Should Leave Courts Cold," *Digital Discovery and e-Evidence*, (3)7, July. pp. 3-5.

Sidor, G. and S. Rogers. (2002) "Electronic Evidence is Superior to Paper Evidence," *The Lawyers Weekly*. 21(44). March 29.

Sleek, S. (2000) "Good e-Recordkeeping Saves You Money, Protects Your from Liability," *Digital Discovery and e-Evidence*, (1)1, Dec. pp. 1, 4-5.

Smith, E. B. (Sept. 23. 2003) "Wall St. Bloodhounds Track IMs for Clues," *USA Today*.

Streza, R. (2003) "Discovery Unplugged: Should Internal E-mails be Privileged Confidential Communications?" *Defense Counsel Journal*, 70(1), January 1. pp. 36-41.

Tambe, J. W. and J. M. Redgrave. (2002) "Electronic Discovery Emerges as Key Corporate Compliance Issue, *The Metropolitan Corporate Counsel*. Oct. p. 6.

United States v. Trauger, N.D.California (2003), Cr. No. 3-03-30371, Sept. 24.

Varchaver, N. (2003) "The Perils of E-Mail," *Fortune*. Feb. 3, 2003.

Withers, K. J. (2000) "Killing the Vampire: Computer Users, Facing Discovery, Attempt to Make the 'Delete' Key Stick. Part I." *Federal Discovery News*. Feb. 15.

Zaslow, J. (May 28, 2003) "To Fight E-mail Sharing, Firms Try New Rules, Software," *Wall Street Journal*, http://online.wsj.com/article/ 0,,SB105405850262272400,00.html (current August 2003).

APPENDIX I. E-MAILDEFINED BY AS A BUSINESS RECORD BY FEDERAL RULES

E-mail is not simply communication, but may also be considered a business record under U.S. Federal Rule of Evidence 803(6). E-mail qualifies as a business record if all five conditions are met. Those five conditions as stated in Federal Rule of Evidence 803(6) are:

- The record must be kept in the course of a regularly conducted business activity.
- The particular record at issue must be one that is regularly kept.
- The record must be made by, or from, information transmitted by a person with knowledge of the source.
- The record must be made contemporaneously. (That is, the document or file must be created at the same time as the business activity).
- The record must be accompanied by foundation testimony. (Someone must be able to validate that the record was made at the time of the activity.

APPENDIX II: AMENDED FEDERAL RULE 26

Under amended Federal Rule 26(a)(1)(A), the responding party is required to disclose the name, address, and telephone number of "each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment." With e-evidence, this rule applies to IS managers since they oversee discoverable information.

Under amended Rule 26(a)(1)(B), the responding party must produce, or describe and state the location of, "all documents, data compilations, and tangible things in (their) possession, custody, or control…"

The 1970 amendment to Rule 34 and Rule 26(a) of the Fed. R. Civ. P. require that lists of all relevant paper and electronic documents be transferred from one party to another early in the process of litigation in a useable form [Enneking, 1998]. If an organization fails to produce e-records in a timely manner, the court may give the plaintiff physical control of the equipment upon which the relevant information is stored to see if they are able to extract the relevant records for themselves.

APPENDIX III: PARTIES TO CIVIL LITIGATION

The party who initiates a civil lawsuit is the *plaintiff*. The party who is sued is the *defendant.* The plaintiff initiates a lawsuit by filing with the court a statement, which is called the complaint, setting forth the cause of action. The complaint must contain sufficient facts to inform the court and the defendant of the nature of the plaintiff's cause of action.

LIST OF ACRONYMS

CSFB	Credit Suisse First Boston
DHS	Department of Homeland Security
DOJ	Department of Justice
ERM	Electronic Records Management
E&Y	Cap Gemini, Ernst and Young
Fed. R. Civ. P.	Federal Rule of Civil Procedure
Fed. R. D.	Federal Rule of Discovery
HIPAA	Health Insurance Portability and Accountability Act
IM	Instant Messaging
ISP	Internet Service Provider
NASD	National Association of Securities Dealers
SEC	Securities and Exchange Commission
SOX	Sarbanes Oxley Act of 2002

ELECTRONIC APPENDICES AND HYPERLINKS

SEC Press Release #2002-179. "SEC, NY Attorney General, NASD, NASAA, NYSE and State Regulators Announce Historic Agreement To Reform Investment Practices: $1.4 Billion Global Settlement Includes Penalties and Funds for Investors." http://www.sec.gov/news/press/2002-179.htm

DOJ's Computer Crime and Intellectual Property Section (CCIPS) "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (Jan. 2001). http://www.cybercrime.gov/searchmanual.htm

E-mail Recovery Options Increase: For Some Companies, Maintaining e-Mail Communications Means Going a Step Beyond Traditional Disaster Recovery.
http://computerworld.com/newsletter/0,4902,84891,00.html?nlid=FIN

ABOUT THE AUTHOR

Linda Volonino is Professor of IS and Director of the Graduate Program in Telecommunications Management at Canisius College. She is co-author of the textbook, "Principles and Practice of Information Security: Protecting Computers from Hackers and Lawyers" (Prentice-Hall, 2004). Linda is a computer forensics consultant to law firms, insurance agencies, and the DOJ. Website: http://telecom.canisius.edu.

Communications of the Association for Information Systems

ISSN: 1529-3181