Computer Forensics In the Age of Electronically Stored Data
By Joel H. Mirman

Where's that Selectric® typewriter when we need it?

It doesn't seem so long ago that people communicated by writing letters or memos created on Selectric® typewriters. When they tore up the originals, the carbons and the carbon paper, there was no trail to follow. Today there are 10 billion e-mails generated daily. It takes only eleven days of e-mail to equal the 107 billion pieces of first class mail delivered in the United States in 1998. In an organization of 100 employees, each generating an average of 10-15 e-mail messages per day, there will be 240,000 to 360,000 e-mail messages per year, even before factoring in backups and copies.

Over 99% of all new information created today is stored electronically. Less than one third of electronically created data is ever produced in hard copy. And the information is decentralized. In other words, it could have been created at the office on a desktop computer, on a laptop, on a home computer, on a Palm Pilot®, Blackberry® or a similar device. It could have been printed, saved on a hard drive or a floppy disk, a Zip® disk or a Jaz® cartridge, on a tape backup, or on a CD. It could have been e-mailed to countless recipients.

And written words are not the only form of communication that is stored electronically. In many cases, voice-mails are converted to electronic WAVE files and are preserved. Telephone systems, including land-based, cellular and digital systems, as well as pagers, Palm Pilots® and Blackberrys® maintain call records that can be retrieved by a qualified forensic expert.

The impact of electronic data storage on the operation of businesses is enormous. Most companies generate their information electronically, but spend little or no time making sure that the information is secure. At most, the typical small company makes some form of backup to enable data restoration. Few have document retrieval programs that allow for the orderly retrieval of discreet pieces of information.

Because less than one third of all electronic data created is reduced to paper, just looking through a patient file, a personnel file, a correspondence file, etc. should give no comfort that one is seeing everything that has been said or written.

E-mails are a treasure trove of information. One of the problems with e-mail is its ease of use. It is impersonal — there is no one staring the author in the face when it is created. People say things in e-mails that they would *never* say in person. And unlike the careless statement made in person, the e-mail message is preserved for posterity – often in multiple copies and in multiple locations – locations that may not be known to the author or the owner of the system where they were generated.

The forensic computer expert often deals with the following scenario. Someone sends an inappropriate e-mail. A supervisor learns of it and suggests that it be deleted immediately. The sender deletes it from his "sent" folder and the recipient deletes it as well. This is far from the end of the story. The expert will search to see who else received copies and who received copies

of the copies. Are there different versions on the system? Is the information backed up somewhere? Did anyone make a hard copy? Did anyone save it on another medium? Can it be retrieved from a server? Can a search of the ISP – the Internet Service Provider – prove fruitful?

And even if it has been deleted from all systems, "deleted" does not mean destroyed. When a file is deleted, the computer makes the space occupied by that file available for new data. Reference to the deleted file is removed from directory listings and from the file allocation table, but the bits and bytes that make up the file remain on the hard drive until they are overwritten by new data, unless they are successfully wiped by use of utility software.

When computer storage was expensive, hard drives were small, and it did not take long for data to be overwritten. Now that it is common to have even home computers with 40 or more gigabytes of storage, it is much less likely that deleted data will be quickly written over. This means that a file that appears to have been deleted is probably still recoverable.

Litigants should insist on full access to electronic document creation and storage devices. These electronic versions have imbedded data – called meta data – that will allow a forensic person to find when they were created and by whom, when they were edited and by whom, what those edits were, and who received a copy.

Important. These documents can be electronically searched – so the expert can conduct Boolean searches much like those on Westlaw® or Lexis®. Instead of manually sifting through thousands – if not millions – of pages looking for that needle in a haystack, the investigator can have the system search for it electronically.

Little protection for employee e-mails

Many courts have found no reasonable expectation of privacy in company emails, particularly where the employer has given appropriate notice to its employees.

Chat rooms are another source of information. In a suit brought by Northwest Airlines, forty-three people were ordered to turn over their home computers.

Keeping everything forever is generally a bad idea. Keeping too much can make retrieval a bigger problem than it needs to be. This can actually be used as an offensive weapon by some. In some cases, the company's records were so voluminous that it would rather pay a settlement than go through the production process.

Just because you *can* keep something a long time, doesn't mean you should. Some organizations simply box up old files and store them away without any attempt to cull out what should not be kept. Now that electronic document storage is so inexpensive, the easy decision may seem to be that everything should be electronically stored. Most organizations should not retain documents longer than they are needed; yet, most do retain them in one form or another.

How long should documents be retained? Perhaps 75% of all documents created have no legally required retention period. For the other 25%, there are retention periods in statutes or regulation periods, statutes of limitations, or other factors requiring their retention.

And how will they be retained? Tapes are fragile. Humidity and heat affect microfilm. And will the medium you use be readable when you need it? Do you remember CP/M, an early operating system? Or 5¼ inch floppy disks? Will the Word® document you save today be readable in 10 years? Should it be saved in a static form such as PDF or TIFF?

The decision regarding how long to keep documents should be a combined management/legal decision. Certain documents are not legally required to be maintained, but may be helpful for historical purposes. After all, people die, retire, quit or even have honest differences in their recollections of what took place. Management needs to decide what makes sense for the organization.

Whose cost is it?

While the responding party normally bears the cost of gathering responsive documents, Federal Rules 34 and 26(c) allow courts to shift the cost of document production upon a showing of "undue burden and expense." In some cases, courts require some sort of expense sharing, or may require the requesting party to pay the entire cost.

An example of the reasoning employed by some courts can be found in *Rowe Entertainment, Inc., et al. v. The William Morris Agency, Inc., et al*., in which eight cost shifting factors were considered: (1) specificity of the discovery requests; (2) likelihood of a successful search; (3) availability from other sources; (4) purposes of retention; (5) benefit to the parties; (6) total costs; (7) ability of each party to control costs; and (8) the parties' resources.

Why keep it at all?

Given the grief involved in document retention, companies may ask why they should retain anything. Obviously, the documents may be needed for the company's own defense. There may be a statutory or common law duty to retain the records in their original form. And the company will have the best chance of defeating a spoliation claim if it has a "reasonable" records management policy that is consistently enforced.

A finding of spoliation can be very costly. Even in jurisdictions where there is no independent tort of spoliation, courts have given juries an instruction on "spoliation of evidence" which essentially say that if a party destroyed it, you can assume that it was harmful to that party.

What other systems keep records?

If you are in a secure environment where employees must gain access electronically, there may well be a running record of where employees traveled throughout the course of a day.

The computer system tracks how long employees were on the system, how much time they spent on various documents, and where they went on the system.

Modern telephone systems keep records of calls. How long are these records retained? And is voice-mail retained as a WAVE file discoverable?

The Need For A Document Retention Policy

For security purposes and for business protection, all businesses should have a well thought out document retention policy, which should include management of electronic

documents. It does no good to shred paper documents when the electronic versions may still exist.

Many companies operate without any kind of formal document retention policy. Paper files are closed and stored, and little or no attention is paid to the electronic counterparts of what is in those files. And the electronic versions will likely contain much more information than their paper siblings.

One of the problems in this area is that there are at least two distinct reasons for retaining documents. One is for disaster backup. It gives the company the ability to restore data in the event of some sort of computer crash. This is quite different from electronic record keeping, which allows the user to manage documents so that they can be retrieved, if necessary, in some sort of cost efficient manner.

Even a good written document retention policy needs to be audited to make sure it is in compliance. Having such a policy and testing compliance has several benefits:

- Volume can be controlled;
- The type of documents retained can be managed;
- Documents can be organized to allow for later retrieval in a reasonable time and at a reasonable cost; and
- A good faith defense can be maintained in the event that certain documents cannot be located.

A good document retention policy cannot be accomplished in a vacuum. It requires that the Information Systems ("IS") people are aware of the legal reasons for document retention and that the management team understands the technical limits of the IS department.

What To Do When The Lawsuit Comes

Whatever document retention system you had before litigation, or investigation, it goes out the window when you are on notice that one or the other is coming. NOTHING should be destroyed under these circumstances:

- When litigation is imminent;
- When litigation has been filed; and
- When the company knows or *should know that documents may eventually become* relevant in litigation.

A policy that is haphazardly followed may be as bad or worse than no policy at all. For example, in *In re Prudential Ins. Co. of America Sales Prac. Litig.*, uncoordinated implementation of the Prudential document retention was held to have denied its opponents relevant evidence, and resulted in substantial sanctions. There was no evidence presented that Prudential had acted maliciously.

And in another case, a default judgment was entered against a defendant who purposely destroyed records that might be detrimental to it in litigation.

The Arthur Andersen fiasco reminds us how important the records retention issue can be. An Arthur Andersen partner admitted, "I obstructed justice. I instructed people on the (Enron project) to follow the document retention policy, which I knew would result in the destruction of documents."

When the law firm of Vinson & Elkins was sued in the Enron class action litigation, it was reported that it took the cautious but expensive step of trading out all its hard drives and preserving the old ones—at an estimated cost of $800,000.

How Long Is Long?

Keeping everything forever is generally a bad idea. Keeping too much can make retrieval a bigger problem than it needs to be. This can actually be used as an offensive weapon by some. There are stories of a website instructing people to sue a certain company and ask for certain kinds of documents. People were told that the company's records were so voluminous that it would rather pay a settlement than go through the production process.

Just because you "can" keep something a long time, doesn't mean you "should." Some organizations simply box up old files and store them away without any attempt to cull out what should not be kept. Now that electronic document storage is so inexpensive, the "easy" decision may seem to be that everything should be electronically stored. Generally speaking, that is a mistake. Most organizations should not retain documents longer than they are needed; yet most do retain them in one form or another.

How long should documents be retained? Perhaps 75% of all documents created have no legally required retention period. For the other 25%, there are retention periods in statutes or regulation periods, statutes of limitations, or other factors requiring their retention.

And how will they be retained? Tapes are fragile. Humidity and heat affect microfilm. And will the medium you use be readable when you need it? Do you remember CP/M, an early operating system? Or 5¼ inch floppy disks? Will the Word® document you save today be readable in 10 years? Should it be saved in a static form such as PDF or TIFF?

The decision regarding how long to keep documents should be a combined management/legal decision. Certain documents are not legally required to be maintained, but may be helpful for historical purposes. After all, people die, retire, quit, or even have honest differences in their recollections of what took place. Management needs to decide what makes sense for the organization.

Whose Cost Is It?

While the responding party normally bears the cost of gathering responsive documents, Federal Rules 34 and 26(c) allow courts to shift the cost of document production upon a showing of "undue burden and expense." In some cases, courts require some sort of expense sharing, or may require the requesting party to pay the entire cost.

An example of the reasoning employed by some courts can be found in *Rowe Entertainment, Inc., et al. v. The William Morris Agency, Inc., et al*., in which eight cost shifting

factors were considered: (1) specificity of the discovery requests; (2) likelihood of a successful search; (3) availability from other sources; (4) purposes of retention; (5) benefit to the parties; (6) total costs; (7) ability of each party to control costs; and (8) the parties' resources.

Why Keep It At All?

Given the grief involved in document retention, companies may ask why they should retain anything. Obviously, the documents may be needed for the company's own defense. There may be a statutory or common law duty to retain the records in their original form. And the company will have the best chance of defeating a spoliation claim if it has a "reasonable" records management policy that is consistently enforced.

A finding of spoliation can be very costly. Even in jurisdictions where there is no independent tort of spoliation, courts have given juries an instruction on "spoliation of evidence" which essentially say that if a party destroyed it, you can assume that it was harmful to that party.

Not only traditional "documents" must be preserved, but it is also important that other electronic media such as website content be retained as well. While there is little case law to date, at law, a California court sanctioned a party under a spoliation theory when it changed its web site during litigation.

Who Pays For All This?

The approach many courts took in the early years was that since the company chose electronic storage, it bore the cost of production in a readable format. In *McPeek v. Ashcroft*, the Court recognized that electronic document creation is the norm. Some courts now hold that the less likely it is that something relevant will be found; the more likely it is that the requesting party will pay. Some of the considerations discussed are:

- The likelihood of retrieving relevant facts;
- The degree of relevance of the information sought;
- The specificity of the request;
- Availability from other sources; and
- The cause of difficulties or expenses in retrieving.

Many courts encourage cost sharing or a sampling to determine the "success" of the discovery efforts. Some, however, continue to maintain that the cost of complying with an electronic discovery request is simply a cost of doing business.

Why A Forensic Expert?

Many companies will want to use their own MIS/IT specialists to gather information. Computer forensics can be defined as the employment of a set of predefined procedures to thoroughly examine a computer system using software and tools to extract and preserve evidence. Forensic analysis goes well beyond the simple gathering of information. Even turning on a computer can corrupt evidence. Did you know, for example, that:

- Booting up the system may alter time stamps;
- Routine system maintenance may alter or destroy data;
- Saving new data may overwrite old data;

- Installing new software may overwrite data; and
- Using virus programs may alter data.

Forensic experts can image a computer without ever turning it on; enabling them to testify that the data has not been altered in any way. Forensic experts understand the protocols necessary to make their findings admissible. They can assist in protecting the data and the chain of evidence by following forensic procedures including:

- Identify the target computer system and peripherals;
- Secure the immediate area;
- Record the exact date and time;
- Note any information visible on the computer screens;
- Disconnect any modems or networking cables;
- Conduct an orderly shutdown; and
- Locate and secure any storage media.
- Forensic experts have the tools and know where to look. They examine such areas as:
- Allocated file space;
- Swap files;
- File slack; and
- Unallocated space (deleted files).

What Will The Forensic Expert Need?

The forensic expert can help counsel identify what information should be requested in discovery. Records may include Word processing documents, including drafts or versions not necessarily in paper form, databases or spreadsheets, E-mail, voicemail, or other computer-stored communications; and relevant system records, such as Internet logs, history use files and computer access records. Places to look may include:

- Active computer files on network servers;
- Computer files on desktops, laptops, local hard drives, etc.;
- Backup resources, wherever located;
- Archival storage, wherever located;
- Laptops, home computers, PDA's, etc.; and
- Media or hardware on which responsive data may have been "deleted" but may be recoverable.

Some Of The Lingo

A **bit** (Binary Digit) is the smallest unit of information. It is magnetically encoded and represents 0 or 1 in binary numerals.
A **block** usually consists of 512 bytes.
A **byte** (Binary Term) consists of 8 bits.
A **cache** is a small fast memory holding recently accessed data, designed to speed up subsequent access to the same data.
A **cookie** is a packet of information sent by an HTTP server to a World-Wide Web browser and then sent back by the browser each time it accesses that server.

A **file** is a basic unit of storage. It consists of numbers, words, images, or instructions. It is stored as space allows, in groups of blocks.
To **partition** means to divide a physical disk into smaller, usable logical segments.
A **sector** holds a single block of data.

Conclusion

Although computers have been utilized in business for years, we are still discovering the many ways in which the manner in which they preserve data can be a sword or a shield. To be forewarned is to be forearmed.

Joel Mirman *is a Shareholder and member of the Litigation Practice Group. He can be contacted at* ***jmirman@bdblaw.com*** *or* ***614.227.4264***.
First published in Columbus Bar Briefs (Summer, 2003)