VOL. 30, NO. 2 AUTUMN 2004

Employee Relations LAW JOURNAL

From the Editor—
Technology's Influence on Labor and Employment Law — *Steven A. Meyerowitz*

When Applicants Apply Through the Internet — *Ely A. Leichtling and Pamela M. Ploor*

Using Digital Evidence to Ferret Out the Dishonest Employee — *Kelly J. Todd*

Protecting Trade Secrets: Steps Every Trade Secret Owner Should Know — *John M. Halan*

IRS Continues Efforts to Control Insurance Planning in Retirement Plans — *Robert H. Louis*

The Legal Overlay to Succession Planning — *James R. Redeker*

Coverage Under the FLSA and the New Regulations — *E. Fredrick Preis, Jr. and Reginald C. Johnson*

Accent Cases in Civil Rights Law — *Donald J. Peterson and Harvey e. Boller*

Enforcement of Non-Competition Agreements: Developments in Massachusetts — *Wilfred J. Benoit and Jennifer*

Adding Insult to Injury: Disability-Based Hostile Environment Under the ADA — *Douglas Massengill*

"But It's in My Contract...!" When employers Should — *Lisa Ballentine and*

Lex Mentis — *James J. McDonald, Jr.*

Employee Benefits — *Anne E. Moran*

ASPEN PUBLISHERS

VOL. 30, NO. 2/ AUTUMN 2004

EMPLOYEE RELATIONS LAW JOURNAL

ASPEN

Using Digital Evidence to Ferret Out the Dishonest Employee

Kelly J. Todd

The increased use of digital technology by business can create a breeding ground for employee dishonesty. Even the best internal control systems can be circumvented by an employee. Professionals charged with finding the truth must rise to the occasion, and investigate the dishonest employees using the same technology. Yet obtaining, accessing and analyzing the available digital evidence can be a monumental task without an understanding of the information that may exist and where it may exist.

According to the Association of Certified Fraud Examiners (ACFE), occupational fraud and abuse accounts for $600 billion in employer losses per year in the United States. Of this amount, the ACFE estimates that asset misappropriation, also known as "employee fraud," accounts for a staggering 90 percent of the losses. Employee fraud can occur in organizations of any size and regardless of the level of sophistication. Elaborate systems of internal control are often installed, yet even those systems can be ineffective when an employee is in collusion with another employee or an outside vendor.

In the age of computer technology, more frauds will be perpetrated with the use of computers. In response to this increase, attorneys and other professionals charged with finding the truth must keep in step with technology if they are to ferret out the dishonest employee. Consequently, computer discovery can cause extreme challenges for these professionals. Simply locating, searching and managing digital evidence requires an understanding of technology that often goes beyond that of the most experienced computer user. Furthermore, because of the fragile nature of digital evidence, spoliation must be avoided to preserve the admissibility of the evidence in a court of law.

The distinguishing factors between digital evidence and traditional paper documents are vast. Moreover, because most digital evidence is never printed to paper, the amount of information available in the digital form can be staggering. For example, a ten gigabyte computer hard drive (considered small by today's standards), can potentially contain in excess of 4.5 million pages of text data.

Kelly J. Todd, CPA, CVA, is a Senior Manager at Summerford Accountancy, PC—Fraud & Forensic Accountants, headquartered in Birmingham, Alabama. Her work as a forensic accountant and fraud examiner includes work for defense and plaintiff attorneys, audit committees, corporate boards, and government inspector generals. Ms. Todd may be reached at *kelly@summerfordcpa.com*

Interestingly, and of enormous benefit to the investigation, electronic documents thought to be deleted or lost by the user can be recovered. Valuable information such as the time, date and author's name may be embedded in the electronic version of a document. Comparisons of computer backups to existing documents can be used to show that a critical document was altered and when the event occurred. And, in the case of electronic mail, casual and candid correspondence may be frozen in time.

DIGITAL EVIDENCE

Any information stored and/or used by computer technology is considered to be digital evidence. Digital evidence can reside on a multitude of various storage devices, known as media. While the most common media is the computer's hard drive, investigation relevant data may exist in many forms, including:

- Compact discs or diskettes
- Backup tapes
- Personal digital assistants, such as PalmPilot or iPAQ
- Thumb drives or other removable storage drives
- Internet ready cell phones
- Digital watches
- Digital cameras

It is important to collect and examine all these types of media, which may have been created by the dishonest employee. Removable media; that is, storage devices that can be removed from the computer often contain information that the fraudster either does not want to keep on a company computer or has deleted from the computer hard drive. Removable media is often overlooked; however such media may contain information that is not available anywhere else.

COMPUTER FORENSICS: THE COVERT OPERATION

Computer forensics is the science of retrieving electronic information that exists even though it may be the intention of the user to conceal or destroy the information. Due to the fragile nature of digital evidence and the technical issues which arise with such evidence, courts will commonly defer to an expert witness. This expert should have a background in computer forensics. Similar to law or any other profession, all specialties are not created equally. Many attorneys have mistakenly

used individuals without the appropriate expertise only to find out that the evidence was inadmissible in court because the methods used were not forensically sound. The forensic specialist will have a wide range of experience and the necessary resources to handle the various technological requirements that will be encountered. Furthermore, the trained and experienced computer forensic specialist will have the expertise to properly handle and preserve evidence, safeguarding it so that it is admissible in a court of law.

When acquiring digital evidence to ferret out the dishonest employee, the computer forensic specialist will likely conduct the examination covertly. A covert operation is necessary to keep the dishonest employee and any possible accomplices from becoming aware that they are being investigated. Of course, employee privacy rights must be observed during this process.

In preparation for the examination, it will be advantageous for the forensic specialist to have knowledge of the operating and backup systems used by the employer; this allows the forensic specialist to be prepared with the proper hardware and software when arriving at the investigation site. The cooperation of the employer's system administrator can be invaluable at this stage. Be aware, however, that oftentimes due to the adversarial nature of the investigation such cooperation is not a possibility. Likewise, rarely does a system administrator want to see anyone, let alone an outsider, opening drives or attaching peripheral devices to their computer system.

IDENTIFICATION OF DATA

Digital evidence exists in many forms and locations within any computer system. Consequently, to find useful information requires an understanding of the types of information available as well as where such information may exist within the computer system.

Active Data

Active data is the information readily available and accessible to users. This data can easily be viewed through file manager programs. Active data includes spreadsheets, databases, word processing files, business application files, e-mail, electronic calendars and address books.

Deleted Files

Often individuals try to destroy documents by deleting them. But

what does it truly mean when a file is deleted? In most operating systems, "deleted" does not mean destroyed. When a file or e-mail is deleted with a computer operating system, the data itself is not removed. Rather, the process of deleting simply indicates to the computer operating system that the physical space belonging to the deleted file is available for additional data to be stored. As a result, the data that makes up the file remains on the hard drive until it is overwritten by new data or "wiped" through the use of utility software. Unlike active data, the "deleted" data cannot be viewed with file manager programs.

Deleted files can often be restored. As "deleted" files are overwritten by new data, the loading of new software or "wiped" with utility software, only pieces of the file may be recoverable. It is important to note however that partially recovered files should not be ignored. Partial files can help to identify possible motive or intent, passwords, addresses, assets, or other information that may shed valuable light on the investigation.

Hidden, Encrypted and Password Protected Files

Case relevant data may be hidden, encrypted, or password protected in attempts to thwart anyone who is trying to retrieve sensitive information. Information can be hidden by renaming files to a common name that appears to be part of the operating system such as files containing the file extension ".com," or ".sys." While on the surface these may appear to be legitimate files, the trained computer forensic specialist will examine an element of the file known as the file header that will show the true identity of the file.

Encrypted and password protected files may require more effort and analysis than files that are hidden in a simple manner. A variety of tools can be used in an attempt to gain access to files protected in this manner. Use of the tools does not guarantee that the file will be accessed and that the information will be retrieved.

Depending on the type of encryption used or the complexity of the password protecting access to the file, the computer forensic specialist will use either a tool that utilizes "brute force" attack or one that dissects the encryption key. Obtaining access with a "brute force" attack can result in quick access to a file, whereas a tool that dissects the encryption key is required with complex encryption and can take much more time.

Automatically Stored Data

Computers store a great deal of data automatically. The user may

have been aware of this data and simply forgot to destroy it, while other users will be completely unaware of its existence. Many software manufacturers build in automatic backup features that create and periodically save copies of the file being worked on by a user. These files are created and saved in order to help users recover data lost due to a computer malfunction. Typically, the file copies are not stored in the same directory as the active file. Additionally, on most networked systems, file copies are saved to the user's hard drive rather than to the network file server. As a result, a document (or some version of it) that was purged from the file server may exist as a file copy on the user's hard drive.

Other examples of automatically stored data include cache files and history files indicating internet sites the user has visited, temporary files, swap files, and enhanced metafiles. As with partially recovered files, automatically stored data can provide valuable information to the investigation. Even if the aware user deleted this information, it may still exist in unallocated space similar to the deleted files discussed previously.

E-mail

E-mail has become a prevalent source of communication in business. The informal nature of e-mail has caused most users to treat it more like casual conversation and less like formal correspondence. Consequently, users often do not think twice about discussing a subject using e-mail that they would never put in traditional written correspondence, treating e-mail more like casual verbal conversation. Not only does e-mail create a more permanent record than most users realize, the computer tracks when it was sent and opened in multiple locations. One e-mail can be saved on numerous servers and is easily forwarded to a person unknown to the original author. These characteristics, combined with the ever-increasing use of e-mail as a primary tool for communication, make e-mail an excellent evidence source for ferreting out the dishonest employee.

Background Information

Unlike paper documents, digital evidence contains a wealth of additional and valuable information. While data files and e-mail are often targeted for evidence, the background information that is inherent with electronic data can often times provide the footprint necessary to identify the who, where, what and when necessary to develop the facts of the investigation.

An electronic trail is left every time a user logs on to the network. Computer logs track network usage, typically containing information about who, when, where and how long a user was on the system. Information may also reside about who modified a file last and when the modification was made. Additionally, the computer log may indicate when and by whom files were downloaded to a particular location, copied, printed or purged.

Employers in increasing numbers are installing software designed to monitor employees' use of company computers. This software records information such as programs used, files accessed, e-mail sent and received, and internet sites visited.

Other background information which may be valuable in the ferreting out the dishonest employee includes non-printing information. One of the many disadvantages to printed documents is that they are printed under user definition; that is, the user defines what information is to be printed and often leaves potentially valuable information behind. Other non-printing information includes:

- Date and time stamp
- Automatically stored revisions to documents
- "Hidden" or non-printing comments in word-processing and spreadsheet programs
- Changes made to an electronic calendar and the time those changes were made

Backup Data

Backup data involves the copying of electronic data to removable media, usually a tape, in order to provide users with access to data in the event of a system failure. Networks are normally backed up on a routine schedule, while individual users rarely, if at all, follow a regimented backup routine. Typically, network backups capture only the data saved on the centralized network file server and do not capture all the data stored on the individual users' hard drives.

Commonly, tapes are rotated on a weekly basis with either a full weekly or monthly backup being pulled from the rotation. Monthly backups are often maintained anywhere from several months to several years. As the backup schedule progresses, the media are "rotated"—recycling older media back into the rotation as new backups are created.

Backups can potentially provide valuable information in an investigation. Namely, they provide a historical snapshot of the data stored on

a system on the particular day the backup was made. Reviewing a series of backup tapes can provide information about how a particular matter progressed over several weeks or months. There are several drawbacks to using backup tapes, which should be noted. First, the tapes can hold a large amount of data that is only loosely organized and usually compressed. To access the data on backup tapes often requires decompressing the data and restoring it to the host drive. This can be burdensome, as most organizations do not have enough drive space to restore backups without overwriting current data. Second, finding relevant data requires restoring a tape, viewing its directories and searching within the directories for specific files. If the file is not on the tape, the process must be repeated for each backup tape. With a large number of backup tapes this can be an expensive and time consuming process. Finally and most importantly, backup tapes generally only backup active data and do not contain deleted files and other valuable residual data.

PRESERVATION OF EVIDENCE

One of the most important aspects of digital discovery, whether for a covert investigation or for other discovery purposes, is preservation of the evidence. Computers change important dates every time an electronic file is opened, read or copied. In fact, simply turning on the computer changes the dates of hundreds of files. All parties must be put on notice that digital evidence relevant to the investigation, both on computer systems and removable media (which includes backup tapes) must be preserved.

Preservation can fall into one or two categories. The first category involves evidence which is in the client's possession. The second category involves evidence that is controlled by an external third party. Determining who has control of the evidence before it is examined forensically will provide the basis for how it should be preserved.

Evidence in the Client's Possession

Every effort should be made to safeguard the computer and other removable devices from further use. When an employer believes that they may have a problem with an employee, time is of the essence when it comes to digital information. Every effort should be made to have the forensic examination completed as soon as possible. In fact, if the employee has been terminated or is aware that an investigation is pending or underway, all access to computers and digital information

should immediately be restricted. An employer's worst threat from cyber-crimes does not come from outside the organization, but rather from their own employees. A disgruntled employee can wreck havoc on information systems in a matter of seconds. Not only can the employee attempt to cover their own tracks by deleting incriminating evidence, they can potentially steal sensitive trade secrets, encrypt programs which render them useless, and a myriad of other devastating possibilities.

Evidence in an External Third Party's Possession

When the digital evidence is in a third party's possession, a letter of preservation will be needed. A letter demanding preservation of computer evidence can be an important tactic in civil litigation, where a discovery order to access an opponent's computer systems may take weeks. Sending such a letter is important to establish notice that the recipient has a legal duty to preserve electronic evidence relevant to the case.

The letter of preservation should begin by outlining the type of information to be preserved, including:

- Data files created by word processing, spreadsheet or other application software
- Electronic mail, including message contents, header information and logs of electronic mail system usage
- Databases, including structural information about the databases
- Network activity logs and audit trails
- Electronic calendars and address books

The letter should also outline that this information may exist in places such as network servers, mainframe computers or minicomputers; standalone PCs, network workstations and laptops. Data may also reside on off-line data storage media including backups, floppy diskettes, and other removable media. Specify that no potentially discoverable data should be deleted or modified and that procedures that may affect such data should not be performed unless all potentially discoverable data has been copied and preserved.

Preserve the Chain of Custody

Electronic evidence is fragile by nature and can be easily altered without proper handling. A chain of custody verifies that information

was neither altered in the copying process nor during analysis. A solid chain of custody is essential to authenticating computer-based evidence copied during a forensic investigation.

Preserving the chain of custody for digital evidence, at a minimum, requires proving:

- No information has been added, deleted or altered
- A complete copy was made
- A reliable copying process was used
- All media was secured

Accurately copying all data on a drive requires making a sector-by-sector copy of the drive. A sector-by-sector copy (also called an image copy) creates a mirror image of the drive being copied, thus capturing all data, including residual data, on the drive surface. In *Gates Rubber Co. v. Bando Chemical Indus., Ltd.,*[1] the court defines a mandatory legal duty to perform proper computer forensic investigations. The court criticized a party's expert for not making an image copy, concluding that when collecting evidence for judicial purposes a party has "a duty to utilize the method which would yield the most complete and accurate results."[2]

There are several types of software designed to acquire and preserve electronic evidence by evidentiary standards. Such software verifies the accuracy of the mirror image by means of cyclical redundancy checksums distributed throughout the copying process. The audit file, which is created during the copying process, documents all events that occur during the restoration process. The time required to create a mirror image is dependent upon several factors, including the size and speed of the source hard drive.

When restoring the mirror image for examination, best practices include checking for viruses on any software and media to be used with up-to-date virus checking utilities. To protect from adding to or changing the data on the mirror image, the image should be "write-protected." Additionally, a working copy of the original mirror image should be made and used for the examination. All media (copies and originals) should be labeled by time, date and source and stored in a secure place.

Searching the Data

Once the data has been gathered, it must be searched for case relevant information. This can be a monumental task, given the vast

amounts of data that will potentially be recovered. The key to effective data searches is taking the time to plan what is essential to the investigation, and sharing this with the forensic specialist. Items to consider include:

- Define the objective of the investigation
- Specify relevant time periods
- Identify the relevant data; that is, if paper documents were used for the investigation, which documents would those be
- Provide search terms, including any important words, names, phrases, locations, hobbies or assets that may be pertinent
- Provide any known e-mail addresses, screen names, passwords, or log-on names that may have been used
- Determine whether there are other computers or devices that may contain key evidence

CONCLUSION

Business and individuals now use computers to store and communicate tremendous amounts of information. Because much of the information is never printed to paper, the digital evidence can be a tremendous asset to an investigation involving employee dishonesty. Overlooking discovery aimed at computers and computer-based evidence greatly increases the odds that a critical piece of evidence will go unnoticed. The discovery of digital evidence does not require that the attorney become a computer specialist. Rather it requires a fundamental understanding of the information that may exist and where it may exist.

NOTES

1. Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90 (D.C. Col., 1996).

2. *Id*. at 112.