ELECTRONIC EVIDENCE IN SMALL CASES AND PRIVATE LITIGATION

Linda Volonino, Ph.D.

I. NEW TECHNOLOGY, OLD TACTICS

The development of electric lights at the turn of the 19th century gradually and grudgingly replaced gas lighting in homes. This new technology was so misunderstood that people would change their light bulbs in a hurry so the electricity did not "leak out." Despite the technological advance, outdated tactics remained. The familiarity of old tactics makes them comfortable and resistant to change—even when they are wrong or better methods have emerged. Similarly, misunderstanding electronic evidence (e-evidence) and how it can be discovered and used cost-effectively in small cases and private litigation has constrained its use. Such a constraint may disadvantage a client, case, or career.

Failing to build or defend a case in the best manner—which may be informed by electronic records, documents, or data—may not only prejudice the case, but be deemed malpractice. The power of e-evidence together with expert interpretation(s) of that evidence can incriminate or exonerate a client, or otherwise determine the outcome of a case.

This article discusses e-evidence—and computer forensic recovery of that evidence—with a focus on the two primary considerations affecting its use in smaller cases and investigations: effectiveness and cost.

II. E-EVIDENCE BREEDING GROUNDS

Since development of the World Wide Web in 1991, we have witnessed astonishing growth in the personal, professional, and criminal use of networked computers, the Internet, e-mail and voice-mail systems, and wireless devices. Computers and communication devices create and store huge amounts of "digital details" in their memory, data files, and logs. In addition, as files and messages are saved or sent, software automatically generates artifacts, or metadata.[1]

Far more information is retained on a computer or handheld device than most people realize. Rarely are users aware that their activities have left multiple trails of evidence.[2] As such, they make no attempt to purge those trails regardless of how incriminating they might be. Even techno-savvy users who want to go undetected may not be able to delete or disguise all trails of their activities or artifacts completely. This creates breeding grounds for evidence that lawyers could use to support or defend their clients.

Another factor enhancing the effectiveness of e-mail and other electronic records is their perceived candidness and credibility. The sample cases in Table 1 illustrate not only how effective and credible e-evidence can be, but also that it may be the only evidence.

Table 1—Effectiveness of E-Evidence

CASE 1: WRONGFUL TERMINATION

In 1997, Adelyn Lee, the administrative assistant who Oracle CEO Larry Ellison had been dating, filed a wrongful termination case against Oracle. During e-discovery, a damaging e-mail sent to Ellison from Lee's supervisor stating, "I have terminated Adelyn per your request" was recovered. Oracle paid $100,000 to settle the lawsuit. However, the supervisor persisted in denying that he had sent the e-mail. A comparison of the time the e-mail was sent to the supervisor's cell phone records substantiated his alibi that he was traveling in his car at the precise time the e-mail was sent. In fact, Lee had sent the e-mail to plant e-evidence.

CASE 2: ANTI-TRUST

In the *Bristol Technology, Inc. v. Microsoft Corporation* anti-trust case, Danbury, Connecticut company Bristol Technology sued Microsoft for $263 million in damages. Damaging to Bristol's case was an e-mail sent in May 1998 from a Bristol director to CEO Keith Blackwell wherein he referred to the upcoming lawsuit as the "We 'sue Microsoft for money' business plan." This candid or unguarded comment cast the trial as a gold-digging expedition. The 8-member jury handed Microsoft a victory on July 16, 1999 with a $1 award to Bristol. After the trial, plaintiff's lawyer complained that the jury focused on the e-mail message and disregarded relevant evidence. To the jury, the e-mail message was the relevant evidence.

CASE 3: SERIAL MURDER
The serial killer who called himself “BTK,” the abbreviation for the killer's *modus operandi* of "bind, torture, kill," strangled to death four family members in Wichita, Kansas in 1974. BTK continued to kill for 16 years, but there was not enough evidence to identify BTK until February 2005. BTK had mailed a computer disk containing a message to KSAS-TV. That disk tied Rader to the murders. FBI analysts recovered files from the disk indicating that it had been used at Christ Lutheran Church. Dennis L. Rader, who was president of the congregation, was one of the 10 people who had access to the church’s computer. A subsequent search of Rader’s hard drive recovered the “BTK message.” After being charged on March 1, 2005 with ten BTK slayings, Rader admitted to the murders.

CASE 4: VEHICLE RECORDERS
Most new vehicles come installed with an event data recorder, or "black box," that stores facts about the driver's speed and handling. In November 2004, Danny Hopkins was convicted of second-degree manslaughter in the October 2003 death of Lindsay Kyle in a car accident. Hopkins vehicle's event data recorder showed that he was traveling 106 mph four seconds before he crashed into the back of Lindsay's car, which was stopped at a red light. Had the car not been equipped with the new event data recorder, a forensic investigation of skid marks and crash damage could have been used to estimate the speed of the car. In this case, the recorder evidence improved both the precision and degree of confidence that the driver's speed was 106 mph and the precise time of the impact.

Whether representing plaintiffs or defendants, attorneys may need to be aware of the opportunities and risks posed by e-evidence and its discovery in order to make justifiable decisions.

III. E-EVIDENCE LURKS AND LEAVES TRAILS
E-evidence is like a vampire lurking out of sight that can neither be destroyed nor intimidated. Potential evidence lies in wait in e-mail, instant messages (IM), voice-mail, faxed and printer servers, Internet chat room conversations, Internet cookies and blogs, and web site registrations; logs of web site visits, downloads, cellular calls and text messages; online meetings, credit card records, digital cameras, PDAs (personal digital assistants), GPS (global positioning systems), online banking and financial records, word processing documents, spreadsheets, databases, contact management files, and digital image, movie, and sound files. These devices and media create records and an invisible evidentiary minefield or gold mine.

Because it is not readily visible, metadata is often overlooked by users. Metadata can be so incriminating that the New York State Bar Association Committee on Professional Ethics published an opinion in 2001 stating lawyers should not surreptitiously look at another lawyer’s metadata.[3]

Unlike other forms of evidence, e-evidence tends to be more complete, can show intent or behavior patterns, and is harder to refute or deny. For example, metadata can be as revealing as a fingerprint or ballistic print. It can reveal the names of everyone who has worked on or viewed a specific document, text and comments that have been deleted, and different drafts of the document. Table 2 lists several examples of what computer forensics commonly reveals.

Table 2—What Computer Forensics Can Reveal

Computer forensics can reveal what users have done on their computers or digital devices, including:

- Theft of intellectual property, trade secrets, or confidential data.
- Work time spent surfing the Internet or chatting.
- Times, locations, and costs of meetings and trips.
- Lifestyle and political activities.
- Defamatory statements in chat rooms, usenet groups, or IM.
- Harassing, hateful, or other objectionable e-mail.
- Downloading of criminally pornographic material or unlicensed software.
- Online gambling, insider trading, solicitation, drug trafficking
- Files saved, accessed, altered, or deleted.
- Violations of non-compete agreements.
- Documents showing a party's negligence.
- Earlier safer designs of a defective product in a product liability suit.
- Earlier draft of a sensitive document or altered spreadsheet showing intent in a fraud claim.
- Personal relationships and hidden assets of interest in divorce cases.

IV. E-EVIDENCE ROI

Electronic discovery or computer forensics is not always extensive or complex. Identifying potential types and locations of e-evidence and how to collect it to preserve admissibility will require a computer forensics consultant or investigator, but cost-containing or low-risk approaches are possible. Computer forensics experts can provide well-advised approaches and theories to structure a solid case, or a defense. A preliminary investigation of the circumstances can be conducted to get better informed and to estimate the potential payoff of more extensive investigation. Even when plaintiff or defendant lawyers deal only with hard copies of e-evidence, the computer forensic consultant may identify anomalies, proof of tampering, or inconsistencies based on a review of the paper documents.

Processing electronic data can become extremely time consuming and costly. A good electronic evidence discovery expert will suggest steps that can be taken to decrease time and expense. Other aspects of e-evidence discovery that an expert should be able to advise on include: preservation, acquisition, chain of custody, production, and the advantages of advanced full-text searching. This type of consulting can save the client money and expedite the control of case evidence.

Discovered e-evidence may help corroborate a witness' testimony, support other technical evidence, or poke holes in opposing counsel's case. The more knowledgeable and prepared an attorney, the better equipped he or she is to serve clients and maintain a position of credibility and strength in litigation.

Examples in Table 3 demonstrate positive return on investments (ROI) from e-evidence in small lawsuits or cases. They also show that computer forensics investigations can be conducted without incurring high costs for specialized tools or expensive procedures. This may be news to many who have learned about computer forensics from the media.

Table 3—Examples of E-Evidence in Smaller Cases and Private Litigation

Example 1:
After being fired for repeated inventory re-ordering mistakes, a kitchen worker files a wrongful termination suit claiming she had been framed. She claims that a co-worker deliberately had changed formulas in the spreadsheet used to calculate order quantities, which caused her errors. The plaintiff's proof is the spreadsheet file. Rather than settle, a computer forensics consultant is retained who informed defense lawyers that it was impossible for plaintiff to have such "proof" because that particular software does destructive updates.

Example 2:
An insurance company refuses death benefits to a wife whose husband had hung himself in their home. A brief review of his hard drive and Internet activities reveals his auto-erotic (AE) obsession and instructions for short-of-death hanging. Evidence indicates that he accidentally killed himself, but had not committed suicide. Taking discovery a step farther, an Internet search turns up statistics on the AE accidental death rate and famous people who had died under the same circumstances.

Example 3:
In a malpractice suit for unnecessary removal of a limb, the surgeon blames the hospital lab for incorrect biopsy analysis. An analysis of the logs shows that the surgeon proceeded before the results of the biopsy were posted.

V. E-EVIDENCE IN THE MEDIA

Much of the learning about e-evidence or computer forensics does not occur in law schools, but rather via media reports on high-profile cases or brief CLE sessions. It might be learned from TV series[4] dealing with sensational crime detection methods. The media has reported cases prosecuted by the Department of Justice (e.g., the Microsoft "Cyber Trial of the 20th Century"[5]), the Securities and Exchange Commission (e.g., the Big 5 accounting firms—now the *Big 4*), and New York AG Eliot Spitzer (*every* major Wall St. brokerage firm, Microsoft, and the Big 5). Class-action lawsuits by defrauded investors and international investigations of cyber-terrorism and money laundering by the Department of Homeland Security have invariably relied on e-mail and electronic records.

These mega-scale cases depended on complex computer forensics techniques and tools to search and recover incriminating e-evidence that had been deliberately hidden, encrypted, deleted, password protected, or somehow obscured through spoofing (a form of forgery).[6] Recovering such e-evidence typically involved a corps of experts searching tediously through thousands of backup tapes and systems, e-mail servers, and network and web logs of Internet Service Providers worldwide. An unfortunate consequence of this educational method is the mistaken belief that e-evidence is for massive cases and not scalable to smaller ones.

VI. DIGITAL PROFILES OR DOSSIERS

Ninety-two percent of new information is created and stored on electronic media.[7] Paper and hardcopy no longer carry all of the necessary information. Electronic records not only can be used to prove straightforward charges, such as illegal possession of pirated software or child pornography, but also to imply motive or intent by forming a "digital profile or dossier" of an individual or the circumstances surrounding a lawsuit or case.

E-evidence is being relied on not only to prove straightforward charges, such as illegal possession of pirated software or child pornography, but also to imply motive or intent by generating a "digital profile" of a crime suspect.

Prosecutors trying Alejandro Avila for the rape and murder of 6-year-old Samantha Runnion in California introduced e-evidence of child pornography allegedly found on his computer hard drive.

In Scott Peterson's double-murder trial, prosecutors introduced GPS data from Peterson's car, cell phone records, and Internet history files from his personal and business computers to provide jurors with enough circumstantial evidence to imply a motive. Civil litigations can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases. Insurance companies may be able to mitigate costs by using e-evidence of possible fraud in accident, arson, and workman's compensation cases.

VII. E-EVIDENCE IN PRIVATE LITIGATION AND ARBITRATION CASES

When you consider that business transactions and communication occur electronically, and corporate e-mail use has increased exponentially, it's understandable that electronic files and e-mail are playing a larger role in litigation. Evidence that would have been impossible or extremely difficult to obtain can now become part of the fact-finding process.

According to the *2004 Workplace E-Mail and Instant Messaging Survey* of 840 U.S. companies from American Management Association and The ePolicy Institute[8], over one in five employers (21%) has had employee e-mail and IM subpoenaed in the course of a lawsuit or regulatory investigation—up from 9% in 2001 and 14% in 2003. Another battled workplace lawsuits triggered by employee e-mail.

Casual, private, or seemingly irrelevant e-mail messages may be deemed "business records," which strongly worded disclaimers may not be able to repudiate. And business records are clearly discoverable. Communications made in confidence are not protected from disclosure if they fit the definition of business record. Furthermore, even e-mail or IM that do not meet the definition of business record (at the time of its creation) can 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.

VIII. Conclusion

Since the 1990s, there has been a huge increase in the amount of electronic material that is discoverable for use as e-evidence. Competent representation is moving toward the use of e-evidence in any size lawsuit, investigation, or audit because it is effective. E-mail has provided a smoking gun in so many fraud, sexual harassment, discrimination, and wrongful termination cases, that discovery of e-evidence, or e-discovery, has become a jurisprudential growth area. Front pages of the Wall Street Journal frequently note an executive's incriminating e-mail being used to show intent or refute "not to my knowledge" defenses.

Lawsuits may be won or lost based on how the litigants use e-evidence. In sum, electronic devices, communication systems, files, messages, and metadata can be the critical evidence of what did or did not happen for plaintiffs or defendants.

[1] Metadata is created by the software, not the user. File creation date, date of last access, version number, author, and company are examples of metadata.

[2] Users may not think to clear the cache of their computers or digital devices. Cache is a buffer area of a computer or handheld device that stores data. For example, web pages that have been visited get stored in the computer's cache. The purpose of cache is to enable the PC to re-display those visited web pages without having to go back through the Internet to retrieve them. Even if users wanted to clear cache, they might not know how. Consider the steps needed to clear the content of web pages and server data from a Blackberry handheld device:

1. Highlight the BlackBerry browser icon and click the trackwheel twice to display the Browser Options menu.
2. Scroll to Options and click the trackwheel to open the browser options screen.
3. Scroll to General Properties and click to open the General Properties screen.
4. Click the trackwheel to open the Cache menu.
5. Scroll to Clear Content Caches and click the trackwheel to clear cache and return to the General Properties screen.
6. Press the Escape button repeatedly to back out to the BlackBerry main menu

[3] New York State Bar Association, Committee on Professional Ethics, Opinion 749 – 12/14/01. http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_749.htm

[4] Television shows include “Forensic Files,” “CSI,” and CSI spinoffs.

[5] During the cyber-trial of the century (20th century), investigators discovered damaging internal e-mail from a Microsoft executive in which he wrote that Windows "must be a killer on OEM shipments so that Netscape never gets a chance on these systems." The majority of evidence used by DOJ came from subpoenaed internal Microsoft e-mail, which prosecutors used to refute Bill Gates’ testimony.

[6] See http://www.webopedia.com/TERM/S/steganography.html

[7] Film represents 7 percent of the total, paper 0.01 percent, and optical media 0.002 percent. See http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm#summary

[8] See the 2004 Workplace E-Mail and Instant Messaging Survey, co-sponsored by American Management Association and The ePolicy Institute. http://www.epolicyinstitute.com/survey/index.html