INTERNET MISUSE IN THE WORKPLACE: A LAWYER'S PRIMER

Vol. 72, No. 10 November 1998 Pg 22 Eoghan Casey and James Garrity Misc

C omputers are swiftly transforming the work environment, creating new opportunities and problems so quickly that keeping up is often difficult. The typical 1998 desktop business computer has more raw computing power than many mainframe computers had in 1990.[1]

In many organizations, computers are used at every level—by owners, managers, and both professional and clerical staff. Computers also have finally legitimized the home office as a true equivalent of the traditional office environment. Though these advances in technology have brought many benefits to the workplace, they have also enabled employees with malicious intent and broad system access to cause grievous harm to their companies, coworkers, and clients. In fact, past studies of workplace computer crimes cited in the FBI's Law Enforcement Bulletin identified full-time employees, followed by part-time and contract employees, as the most significant threat to an organization's computer systems.[2] W hy is this so? One reason is that employees have a level of access to internal networks and data that a hacker can only dream of. Another is that employees sometimes have personal interests, motives, and grievances that conflict with those of his or her employer. The Internet can satisfy those interests, and employees have not overlooked it.

Lawyers are well positioned to help clients understand Internet-related risks, to develop Internet usage policies, to conduct investigations, and to initiate civil and criminal actions when clients discover employee misconduct. This article is a primer for lawyers on those risks. It explains basic Internet features, and how employees may misuse these features. It also outlines the major laws governing Internet and computer misconduct, and discusses ways of preserving evidence. But appreciating the risks is personally important for lawyers as well. Any computer from which law firm employees can get to both client data and the Internet poses a risk. The possibility that client or law firm data can be compromised means that lawyers must for their own purposes understand how firm employees may misuse the Internet.

Scope of the Problem

The commission of crimes or civil wrongs via the Internet[3] can be subtler and more damaging than the same acts committed in traditional fashion. On the Internet, hate mail needs no paper, no envelopes, and no stamps; pornography needs no film

screen, projector, or
printer. Manufacturers now ship most mass-market computers Internet-ready, with sophisticated communications software that can send and receive documents, videos, photographs, audio and computer programs. Microsoft's latest operating system, Windows 98, completely integrates Internet access into the operating system itself, making it more difficult than ever to block employee access. Malicious employees can make files and records disappear with the push of a button, and distribute confidential records worldwide in a matter of minutes. Alternatively, an employee can transfer records to a personal e-mail address so the stolen data can be distributed or analyzed at a more leisurely pace. Employees also can configure their company's computer to allow remote, unauthorized users to search system directories and files, retrieving whatever data the intruder chooses.[4] Or the employee can leave data where it is, but download military-grade encryption software[5] and scramble it, making it useless. The potential for harm is especially great in organizations, including law firms, that trade in information and thus are essentially electronic "data warehouses." These entities are ripe targets for malicious employees. every size, and in both the public[6] and private[7] sectors. While some employers have elaborate policies and procedures in place for preventing Internet misuse, those policies often are too vague, outdated, or not actively enforced. Managers also may overestimate employee loyalty, or their own skills in detecting computer-based misconduct. For example, many believe users can only transfer computerized files as attachments to a delivery vehicle such as e-mail. In fact, one can easily transfer files via the Internet without e-mail. Depending on the method used, there may be no physical sign on the organization's system that the transfer occurred.[8] Moreover, segregating the helpful from the harmful is no easy task. Once connected to the Internet, an organization will find it difficult to impose content-based restrictions (unlike Westlaw or Lexis and similar services, which allow selective access to content).[9]

Internet Services and Associated Risks

Given the complexity of the Internet, it can be daunting to address the opportunities that it enables. This section reviews some of its basic features, with the goal of simplifying the areas most likely to be accessed by employees using the Internet.

The World Wide Web. The web is what most people think of when they hear the term "Internet." Using the web, organizations and individuals alike make information and commodities available to anyone in the world. Employee visits to illicit sites on the World Wide Web are commonplace. Thousands of free websites contain inappropriate material that ranges from pornography to stolen software to advice on illegal activities. Such sites are usually found by using free "search engines" to track

down material on a specific topic. Using any of several popular search-capable sites on the web, a user can enter desired words or phrases and retrieve a list of relevant sites. The user then can go directly to any of the listed sites, returning to the list as desired to go directly to any other site on the retrieved list. This process is sometimes referred to as "surfing" the web.

E-mail. E-mail is the most familiar method for sending and receiving information through the Internet. All major online services include e-mail functions as a standard feature. Employees can transmit e-mail to others whether or not they use the same online service and despite their location within or outside the United States. Most e-mail services allow you to "attach" computer files. E-mail attachments can include any kind of computer file, including text, photos, sound, video, or an entire computer program. This means that virtually any form of intellectual property can be compromised with e-mail.

The identity of the sender of an e-mail transmission may not be easy to figure out. A user can forge a return address on e-mail messages to conceal its origin. Several hacker sites on the Internet explain the procedure. An employee can send harassing e-mail that says the author is anyone he or she chooses, such as "YourTormentor@Forever.com." Sometimes a person skilled in Internet crime can discern the sender's identity. Computers usually relay e-mail transmissions on the Internet across several networks before they reach their destination. The transmission of an e-mail message leaves an evidence trail that may permit eventual identification. Sending truly anonymous e-mail—completely stripped of any identifying information—is possible technically, but it requires more effort than most people are willing to expend.[10]

Newsgroups. Internet newsgroups are essentially computer-era bulletin boards. Here anyone can post text, photographs, software, and full-motion videos for unrestricted, worldwide copying. Most newsgroups are part of a free, global system called the User's Network (Usenet). There are over 30,000 newsgroups on Usenet,[11] covering every imaginable topic, from the trivial[12] to the criminally deviant.[13] Newsgroups are easy to use, similar in many ways to e-mail. The main difference between the two is that e-mail messages are private messages to specific individuals, while newsgroup messages are available to the public. Newsgroup postings often contain forged e-mail return addresses. Any office computer that can reach the Internet can access Usenet.

Unlawful pornography is more likely to be found on Usenet than on the web because of Usenet's greater relative anonymity. A sample Usenet newsgroup database search[14] conducted for this article, and using the terms "pedophile," "preteen," and "girls," retrieved more than 50 sites whose newsgroup title alone suggests the availability of

unlawful content. Since Usenet messages are broadcast to millions of people around the world, it is the perfect medium for employees who are trying to reach a large audience.

Chat. Live conversations between users on the Internet exist in many formats (text, audio, video, and virtual reality), on all conceivable topics, and take place 24 hours a day. IRC (Internet Relay Chat) is currently the largest chat network and can be used by anyone with Internet access. Online services such as America Online and Yahoo also offer chat rooms, but the topics of conversation found within these mainstream services tend to be far milder than those in the freewheeling Internet environment.

The IRC network is accessible using free or low cost, easy-to-use software.[15] Two of the most popular IRC software programs are mIRC and PIRCH. On IRC at any given time, there are thousands of chat rooms in operation worldwide. Many IRC chat rooms exist solely to facilitate unlawful activities, primarily through the exchange of computer files. Employees can send any type of computerized company or firm record this way. Employees can load IRC software and even allow other IRC users to access the organization's computer files directly. There generally is no record of file transfers on the IRC network or on the victimized computer. In other words, a company or firm whose data is being compromised in this way may never know it occurred.

ICQ ("I seek you") is a relatively new live chat network with a difference. Instead of gathering in chat rooms, ICQ users must seek each other out and jointly agree to have a conversation. While this limits contact with others on the ICQ network, it enables more private conversations than other chat networks. In this respect, misconduct facilitated by ICQ is more difficult to detect because a third party cannot participate in ICQ conversations unless invited. While users must register with ICQ, they can do so with false names and e-mail addresses. In the next version of ICQ software, users will be also able to hide their Internet Protocol address, an identifying number that law enforcement officials have long regarded as immutable evidence of a user's identity. As an indicator of the high volume of activity on the Internet even in comparatively unknown areas like ICQ, it is worthwhile noting that ICQ announced that it reached the *14 million user* mark in early July 1998. In February 1998 ICQ set new records for new subscribers in a single day (50,000) and for the number of users online at one time (400,000).[16]

Theories of Liability

Understanding the basic makeup of the Internet is necessary to prevent and investigate its misuse. A review of some basic liability considerations also is helpful, because it illustrates why an active prevention program is important. The Internet's

simultaneous presence in all states and countries, and its ability to let users make thousands or even millions of copies from a single posted document, photograph, video, or song poses unique problems of criminal, civil, and ethical liability.

An employee's misuse of the Internet poses risks of criminal and civil liability for the organization and the employee. For professionals such as attorneys, physicians, and others with an ethical obligation to safeguard client confidences, misconduct involving client information may lead to ethical grievances where a professional fails to protect confidences from disclosure. Other problems can include embarrassing press coverage, the loss of business, the temporary or permanent seizure of part or all of the organization's computer system, the disclosure of internal company secrets, and the possibility of additional criminal charges or civil actions based on other information discovered on the organization's systems during the initial investigation.

Criminal liability. The risk of criminal charges for an employer generally depends on whether the employer (or a principal) was an active participant in the offense. Key laws governing Internet crime focus on the offending user, not the owner, of the system. Nonetheless, even a genuinely innocent owner has some risk. Law enforcement may err in arresting an owner, for example, because of a mistaken belief about the way computers store data. Unlike physical filing cabinets—which generally are very close to the owner of its contents—the "virtual" filing cabinets of online directories and files are all in the same place, and often are accessible to hundreds of employees in remote locations. An employee attempting to hide illicit computer files might store them in a supervisor's or coworker's directory, creating at least a surface impression that the files belong to the supervisor or coworker. A truly malicious employee could do this and then place an anonymous call to the police, falsely alluding to "vague comments" by the victim about having some "special files" in his system. If the idea of employees planting false computer evidence seems far-fetched, consider this: In 1996, an employee of the Oracle Computer Corporation actually won a $100,000 settlement in a wrongful termination suit based on a phony e-mail message she concocted in her supervisor's name. Only after the employer settled the case, and the supervisor's reputation was in tatters, did investigators determine that the message was a fake.[17]

In many ways, laws treat a computer used in Internet-based crime as a weapon, much like a gun or a knife. Its use can therefore lead to additional charges[18] or a heightened degree of severity.[19] Its national and worldwide accessibility creates risks of legitimate multiple prosecutions or lawsuits in several jurisdictions simultaneously.[20] For example, some states treat a computer crime as having occurred in their jurisdiction if in the process a transmission used any computer in their jurisdiction. Networks route the typical Internet transmission through several relay computers—chosen during

transmission by the networks, not the user—on its way to the intended recipient. Thus, transmission of a single e-mail conceivably could violate the laws of many states.[21] Prosecutors might interpret some state laws to treat, as a separate offense of "distribution," each download of an obscene photograph that your employee posted. Postings in Usenet newsgroups, for example, can be downloaded an unlimited number of times, since each user is merely downloading a copy, not the original. Finally, some Internet transmissions may violate the laws of several countries. The transmission of certain material, such as images depicting nudity, may violate the laws both of the United States and the country in which the material is received or available. Investigators in any jurisdiction may pursue an Internet crime where their laws permit prosecution.[22]

Florida's principal law on crimes against computer software, hardware, and access is the Florida Computer Crimes Act.[23] The act treats computer crimes as against intellectual property,[24] and is designed to supplement, not replace, other available charges. It criminalizes the act of modifying, destroying, disclosing, or taking "data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network."
[25] It proscribes similar conduct toward computer equipment and supplies, and makes it a crime to gain unauthorized access or to deny access to legitimate users. Another Florida statute, the Computer Pornography and Child Exploitation Prevention Act of 1986,[26] makes it a crime to use a computer to upload, transmit, print, send or receive, or buy or sell child pornography. The statute also proscribes the use of a computer to lure a minor into certain sexual activities, and makes it a crime for any "owner or operator" of a "computer on-line service, Internet service, or local bulletin board service" to knowingly permit subscribers to use the service to violate the act. Importantly, the statute does not define these terms, a noteworthy omission for companies with a presence on the Internet. The language is clearly aimed at major Internet service providers, such as CompuServe and America Online. Less clear is whether it applies to companies that maintain a website as an adjunct of their regular business, to allow clients to post messages, upload or download files, or participate in chat sessions.

At the federal level, there are several legislative enactments aimed at computer crime. But the manner in which statutory enactments are passed—by appending short new amendments to existing laws, using "short titles" that suggest a comprehensive new body of law—can slow the process of identifying Internet-related laws. For example, one law curbing the Internet's use as a trading post for child pornography—the Child Pornography Prevention Act of 1996[27]—is a four-paragraph amendment to a law preceded by an amendment titled the Child Protection Restoration and Penalties

Enhancement Act of 1990, which was preceded by an amendment titled the Child Protection and Obscenity Enforcement Act of 1988, which was preceded by an amendment titled the Child Sexual Abuse and Pornography Act of 1986, which was preceded by other amendments that date back to 1977, almost 20 years earlier.

The federal equivalent of Florida's Computer Crimes Act is an enactment known as the Computer Fraud and Abuse Act (CFAA).[28] Like its state counterpart, it is very broad in scope and is the federal government's core deterrent against crimes made possible or easier because of computers. Reduced to its essence,[29] the CFAA makes it a crime for an unauthorized user to access a computer that is federally owned or is a "protected computer" for the purpose of 1) obtaining records from a bank, credit card issuer, or consumer reporting agency; 2) committing fraud or extortion; 3) transmitting destructive viruses or commands; 4) trafficking in stolen passwords; or 5) threatening to damage a computer system in order to extort money or other things of value. A "protected computer" is a computer 1) used exclusively by a financial institution or the United States Government; 2) used on a nonexclusive basis but where the conduct affects use by the financial institution or the government; or is 3) used in interstate or foreign commerce or communication. This last element is intended to keep the federal government out of purely local computer crimes, but the multistate nature of Internet transmissions suggests that almost any Internet activity will amount to "interstate commerce."

Another federal law that has considerable relevance to the workplace—because of the popular practice of downloading copyrighted works from the Internet—is the No Electronic Theft (NET) Act. NET was signed into law in December 1997 by President Clinton. It specifically targets Internet-based copyright infringements.[30] NET was enacted to deter people from using online bulletin boards or newsgroups for the exchange of digital software, music, and video files. Some observers believe this law is the product of an entertainment industry upset over the ease with which artistic works and software can be distributed over the Internet. The lobbying effort for NET was similar to that used when VCRs became popular. Making unauthorized copies of copyrighted works has always been an actionable civil wrong, but was not a crime unless money was involved. Thus, perhaps the most significant change effected by NET is that criminal prosecution no longer will require a motive of financial gain. "Financial gain" (a requirement for some criminal copyright sanctions) is now defined to include "anything of value." This is essentially an end run around what was known as the LaMacchia Exemption, which exempted software copying from criminal prosecution unless it is willful and for profit. The reported impetus for NET was an MIT student who openly downloaded copyrighted works but distributed them for free to avoid criminal infringement actions.

A federal law that provides criminal penalties for intercepting e-mail—which raised questions about employer monitoring—is the Electronic Communications Privacy Act (ECPA).[31] The ECPA makes it a federal felony to intercept electronic communications, or to disclose or use the contents of an electronic communication, notably e-mail. Employers often ask whether the ECPA prevents them from monitoring e-mail as part of an employee's Internet activity. For several years, the capability has existed to allow employers to remotely view real-time images of employees' computer screens, to monitor keystroke rates, and to track the time an employee's keyboard is idle. Now, "filtering technology" software makers encourage employers to "fully understand how the Internet is being used within the company" by organizing employee Internet activity, including e-mail, "into one of 29 categories to produce graphical analysis of Internet activity."[32] Another program allows managers concerned with Internet policy violations to "see who violated the policy, when and how many times," and then "either discuss the issue with the employee off-line or use the software to begin blocking access and issuing violation messages."[33]

The ECPA contains no flat rule excluding employers. However, it contains several statutory exceptions that suggest employers are protected in most cases. The ECPA creates a "provider exception" that allows the provider of a computer system (such as an internal company network) to "intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service *or to the protection of the rights or property of the provider of that service*.. . . "[34] In cases of Internet misconduct, employers can argue that interceptions were needed to investigate a possible security breach.[35] Second, an employer can argue that the computer and e-mail system provided to the employee and used to review e-mail was furnished and used in the ordinary course of business and do not constitute the "electronic device" contemplated by the ECPA.[36] Courts have demonstrated a willingness to examine the nature of the interception, and the intercepted communications, to decide if the "ordinary course of business exception applies.[37] Third, an employer can argue express or implied consent. Whether this exception applies will again depend on both the nature of the monitoring and the content of the communication. In all cases except during an active investigation of employee Internet misconduct, an employer is better served by adopting express Internet monitoring policies and procedures, and by requiring employees to sign an acknowledgment of the policy.

Civil liability. Internet-related misuse can result in civil litigation against both employee and employer under a number of legal theories. Civil liability poses a greater risk to the organization because negligent policing of Internet activities, and not actual knowledge of the wrongdoing, will be the claimed shortcoming in most

instances. Based on the kinds of activities discussed at the outset in this article, possible civil claims may include sexual harassment,[38] discrimination, fraud, and trademark and copyright infringements. Other claims may include invasion of privacy and negligence. Possible plaintiffs include the intended targets of the employee's conduct (employees at other locations, customers, third parties), unintended targets (*e.g.,* third parties who loaded a virus-infected program, or who inadvertently saw a malicious or threatening communication), clients of the employer (whose confidential data, or trade secrets, were disclosed), and other employees of the company (who may have had confidential personal data revealed by the offender).

Ethical violations. The risk of the malicious disclosure of client secrets may be one of the most personally compelling reasons for lawyers in particular to understand how the Internet works and how client confidences can be severely and irreparably compromised without effective Internet usage policies. The Rules Regulating the Florida Bar impose a solemn obligation on attorneys to maintain the confidences of their clients. Other professions, such as CPAs and physicians, have similar obligations. Rule 4-1.6, titled Confidentiality of Information, provides that "A lawyer shall not reveal information relating to representation of a client except as stated in subdivisions (b), (c), and (d), unless the client consents after disclosure to the client." The Comment to Rule 4-1.6 states that "The observance of the ethical obligation of a lawyer to hold inviolate confidential information of the client not only facilitates the full development of facts essential to proper representation of the client but also encourages people to seek early legal assistance." In law firms with Internet access, client confidences are at risk of both intentional and accidental disclosure. Depending on how the employee makes the disclosure, complete retrieval of the information may be impossible.

No state bar association appears to have addressed the ethical issues raised by storing client data on the same computer that has national or worldwide data distribution capabilities. Some state bars have passed on the subject of attorney-client e-mail transmissions[39] but The Florida Bar has not. However, prudence dictates those professional associations such as law firms, CPA firms, and medical groups should use available security precautions such as encrypting software when transmitting communications that rely on the Internet for delivery.

Looking for Clues to Employee Misconduct

Unless the misconduct is an isolated incident or the work of a highly skilled employee, there usually will be some tangible evidence of Internet misconduct, whether it is stored on the employer's system, on a remote system, or is manifested in other ways (*e.g.,* computer printouts, company telephone records, incoming e-mail messages,

floppy disks). The proper investigative methods used by the employer, attorney, or computer expert will depend on the perceived scope of the violation and the possible responses if misconduct is established, *e.g.,* employee discipline, civil litigation, or criminal charges. Computer evidence is inherently fragile. Hence a cautious and informed approach is necessary, based on a plan thoughtfully developed before misconduct has occurred.

Of course, before an employer undertakes a search of an employee's work space, counsel should confirm that the search does not violate the employee's privacy rights. Courts have held that in some situations employees may have a reasonable expectation of privacy in their work area. This is true in both public and private sectors. Workplace investigations of state or other government employees are subject to the limits of the Fourth Amendment's proscriptions against unreasonable searches and seizures. Still, the U.S. Supreme Court has refused to impose warrant or probable-cause requirements on government employers. Instead, it has adopted a reasonableness standard for government workplace searches, and deemed such searches permissible either for work-related purposes (*i.e.,* to find a needed file) or to investigate suspected work-related misconduct.[40] The Fourth Amendment does not bind private employers, but they may find their bed of thorns lies in a state common law action for invasion of privacy. The reason for the search, the nature of the position held by the employee, and the thing searched (*e.g.,* a desk, a computer, or personal briefcase) all are important factors in determining the propriety of the search. In either sector, however, an employer can lower an employee's expectation of privacy by adopting a clear policy about what is not considered private and thus is subject to search.

System programs and files. There are several ways to find out which websites and what materials were viewed on a given computer. Obviously, the bookmarks or favorite places in a person's web browser will give you a list of frequented sites. However, this information is easily altered or deleted and may not accurately reflect the user's activities. More thorough records of what were viewed can be found by examining the cache, history, and "cookies" of a specific browser.

default most web browsers store temporary copies of web pages on a computer to improve performance. Unless altered by the user, this copied material is stored in a directory called "cache" by Netscape[41] and "Temporary Internet Files" by MS Internet Explorer. Files are stored in the cache until more recent files overwrite them. Also, both major browsers keep a history of the media that has been viewed along with associated dates and times. The Netscape Navigator history file is called "netscape.hst" and can be viewed by typing "about:global" in the location field of the browser. Similarly, MS Internet Explorer has a history folder that can be viewed using

the Go – Open History Folder menu option. How far back the history extends depends on how users configure the browser and how carefully an employee cleans up after browsing the web. In some cases, the history is complete. In others it is nonexistent. The absence of history can suggest either a lack of web activity or covering behavior.

"Cookies," which are lines of text entered into a special file named the "cookie" file when certain (but not all) web pages are visited, can provide additional information about an employee's web travels. Many websites use cookies to keep track of their visitors' interests and past visits, usually for marketing purposes. Though cookies contain some information that will be meaningless to most people, they clearly show that the employee visited certain websites.

System files are also an obvious and excellent source for clues of employee misconduct. For example, searching a computer for certain words or phrases, or even for certain file extensions (GIF and JPG for image files, and MOV, MPEG, and AVI for video files), can reveal evidence. Most Windows-based systems permit searches using only the file extension as a search term.

E-mail. Many organizations routinely review their employees' e-mail. E-mail can be examined on the main e-mail server or on employees' individual computers. Even after users have deleted e-mail, it can remain on a computer indefinitely. Also, since many organizations regularly back up computer data, employers can sometimes recover e-mail years after its first transmission, even if the author honestly believes her or she has erased all traces of it.[42]

Newsgroups. If an employee has posted messages on any of the more than 30,000 public newsgroups, finding them and printing copies using one of several free Internet sites may be possible. The most developed, Dejanews,[43] allows searching by user name, by company name, and many other terms. Newsgroup postings several years old can be found using this feature. A search using the terms "attorney" and "Florida Bar" for this article retrieved 21 messages from the year 1995 alone. Newsgroup postings can be deleted, but this is not a widely known fact nor is the process simple or self-evident. Dejanews also has a profile feature that allows one to retrieve a list of all messages posted by an individual. Dejanews does not archive images, but several other archives do, including images from pornographic newsgroups. Usenet archives are used by organizations to learn more about their employees, are used to gather evidence for criminal and civil cases, and also are used by criminals to gather information about victims.

Besides the messages stored in Usenet archives, computers often store information about an individual's Usenet activities. Most newsreaders (*i.e.,* software used to view newsgroups) keep records of which newsgroups were visited and which messages have been read. How this information is stored depends on the newsreader but is rarely difficult to find and interpret.

Chat. Evidence of employee misconduct on a chat network is fleeting because, unlike Usenet or e-mail, computers do not usually record activities on live chat networks. One cannot search chat networks for past visits, file transfers, or conversations after the fact. Additionally, as was mentioned earlier, some chat software enables two computers to bypass the chat network's computers once a connection between the two is made. Therefore, even where a chat server can log and store communications between users, those servers will be unable to maintain them once the users connect themselves directly to each other's computers. These transient attributes of chat networks make them an ideal haven for criminal activity.

The first step in determining if employees are using Internet chat is to look for the software on the computer(s) in question. Popular chat-specific software often includes the IRC designation in its name, such as mIRC, PIRCH, VIRC, OrbitIRC, and EZ-IRC. Many of these programs can be downloaded free directly from the Internet. Even if a computer does not contain specific chat software, it is still possible that an employee may be using a chat program and transferring or receiving files. Yahoo[44] and America Online have chat rooms that employees can access with regular browsers. Also, while some chat software such as mIRC can record chat room conversations word-for-word on a real-time basis, this is not the default setting. Unless the employee configures the software to log activity, or unless the system administrator does so, the computer will not create log files. Barring enactment of a company policy of electronic monitoring, there is very little that can be done to detect employee misuse of chat networks.

Transmissions. Transmissions to and from an employee can be an excellent source of information and evidence. They can confirm abusive or unlawful activity already suspected or alert the organization to new forms of abuse. Apart from what the e-mail or file contains, transmissions usually contain a wealth of clues about the source and destination of the transmission, even where the sender's identity appears unknown.

Collecting and Preserving Evidence

Once employee misconduct is detected, the associated evidence should be carefully collected. A mistake in collecting and preserving the evidence is often irreversible. Computer evidence is "live" in the sense that, unlike documents, mishandling can change its inherent state. Even the possibility of alteration can destroy the company's case because it may not be possible to prove a negative—that nothing has been changed. Consequently, there is no margin for error. Companies that can foresee the possibility of employee Internet misuse must develop—with their legal counsel[3]—complete policies and procedures for handling problem situations. When the company is satisfied that wrongdoing has occurred, it should take certain steps at once to set the stage for proper evidence collection.[45]

Separate employee and computer. The employee and his or her computer terminal must be separated as quickly as possible, to prevent the destruction of evidence. It is possible to delete all information on a computer's hard drive in a matter of minutes, and/or to notify associates via the Internet of the employer's discovery of wrongdoing. The separation should be done in as nonintrusive a manner as possible, since it is always possible other employees are involved. The employer should change the suspected employee's passwords to all company programs and accounts, remotely if possible, to maintain the terminal exactly as the employee left it. The employee's work area also should be secured but not altered. Items that the employer must preserve in "as was" condition include the computer hardware (*e.g.,* the keyboard, monitor, CPU, and mouse), software (such as disks, tape, removable disk drives, and PCMCIA cards), documentation (manuals, printouts, notebooks, or notepads), and other components (including the printer if needed and all cables). Trash cans are favorite repositories for employees who sense something is amiss, and should be secured to ensure crucial evidence does not disappear.
ise a strategy: the choice of remedy (*e.g.,* criminal, civil, or merely disciplinary, including termination) and the degree of preservation and collection justified by the wrongdoing. Team members might include a company principal or manager; the company's attorney; the company's system administrator; a private investigator or computer expert; and, in some situations, a representative from a law enforcement agency. The involvement of state or federal law enforcement agencies requires thought, because it is not always clear what agency has jurisdiction. Care needs to be taken to ensure that the company does not inadvertently become a target of the investigation. Also, the involvement of law enforcement can mean unwanted publicity, delays, and the loss of control over the investigation. It often leads to the seizure of corporate computer components as well, although as a rule most agencies have become conscious of the need for a company victimized by computer misconduct to keep as many system components as possible.[46]

Collect the evidence. Once a decision has been made, the next step for company officials and their counsel will depend on whether the matter is being handled as a civil wrong or as a crime. If the company and its private advisors will handle it as a civil problem, evidence collection for use in supporting employee discipline or civil litigation can begin. As a rule, videotaping the computer, computer screen, and surrounding work area is appropriate. Still photographs also should be taken, particularly of the components' serial numbers, model numbers, and brand names to permit certain identification of the components later. Computer parts usually are interchangeable, and a large organization may have hundreds of identical-looking components in the same location. The team should label cables and wiring to permit easy identification and reassembly if the terminal and its components must be separated to move them to another location for further inspection.

If the employee turned the computer off before leaving, a concern is whether the employee has configured it to delete data if it is started in his or her absence. Because of this risk, good investigators will use a "boot disk" to start the computer, thus preventing the system from running any programs the employee set up to destroy data when the system is turned on. A boot disk is a floppy disk that contains the information necessary to start or "boot" the computer's systems from the A drive, which is usually a slot on the side of the metal box containing the hard drive. Also, the system should be checked for viruses before evidence is collected, so that other systems used to review the data are not infected. Digital evidence should be downloaded on new virus-free, blank, formatted diskettes. This reduces the risk that the team will inadvertently modify the data being downloaded. Directory and file names, creation dates, and the contents of each file must be left exactly as it was found. Once investigators have stored all of the desired evidence, they should clearly label each disk and write-protect it so that others do not modify the data. It is wise to create one or more additional sets of disks containing the downloaded information. At least one backup copy should be left unexamined so that one pristine copy of the evidence exists. This pristine copy can be useful to anyone who needs to verify that the employer did not tamper with the evidence. The company must protect computer diskettes from dirt, fluids, humidity, impact, excessive heat and cold, magnetic fields, and static electricity.

Where the evidence is dynamic, such as chat room sessions, it is still possible to collect evidence for use later. Some chat progams, like mIRC, have logging capabilities that automatically record the entire chat session. It is also possible to buy software that allows remote monitoring of employee computer terminals that will allow investigators to print or store the information that appears on-screen. Still photos or even videotapes of live screen activity are also possible and can be invaluable evidence of misconduct. In some cases an attorney might recommend that two or

more of these methods be combined. Redundancy in computer-evidence cases can help defend claims of alteration by the employee. If a challenge to one form of evidence arises (such as the log file, which is created on a real-time basis but can be altered just like a computerized deposition transcript), the attorney can offer a second form, such as a videotape of the chat session.

There are several subtleties to saving evidence of Internet sites an employee has visited, or of e-mail transmissions. Internet or websites often contain both text and images. They often contain highlighted connections (hyperlinks) to other parts of the site, or to other sites altogether. Newer websites may also contain divided screens or "frames" that require separate steps to save each part of the screen or frame. All the components of the screen can and must be saved to ensure the employer can present an exact duplicate of the site at the time the employee visited it. When saving e-mail or Usenet messages, saving the information showing the route the e-mail took from the sender to the recipient (called the "header") is important.

If the matter is to be referred to law enforcement authorities, management must treat the employee's work area as a crime scene. Nothing should be altered in any way. In a criminal investigation, the chain of custody will be critical. A prosecutor must be able to show who collected the evidence from the crime scene, who secured it, and where investigators transferred and maintained the evidence until it is used at trial. The fragility of computer evidence can lead to arguments of tampering or modification (in civil and criminal trials), so preservation of the scene is essential. After crime scene investigators have secured the scene, company officials can discuss the prompt return of components needed to operate the business, and the need to protect confidential data that law enforcement may seize as part of the initial investigation. As discussed above, law enforcement authorities are increasingly willing to consider and use evidence collection techniques that avoid or reduce business disruptions.

Conclusion

A well-designed Internet access policy, developed before a problem is discovered, is the key to minimizing the risk from an employee's unauthorized Internet activities. It is important to balance the legitimate privacy interests of employees with the legitimate workplace and security needs of the employer.[47] Lawyers should be prepared to address these Internet-based problems, both within their organization and on behalf of clients who experience such problems. Though specific security procedures are beyond the scope of this article, many organizations offer help in developing proper security procedures. The Computer Emergency Response Team (CERT)[48] is an excellent resource for exploring computer security issues that a law firm or its clients may face. CERT is at Carnegie Mellon University's Software Engineering

Institute (SEI) in Pittsburgh, Pennsylvania. It is operated by Carnegie Mellon and sponsored by the U.S. Department of Defense. One goal of the program, according to CERT, "is to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks." However, since no plan is failsafe, policies and procedures should include contingency plans to address problems when they arise. With an understanding of the Internet and the associated laws and liabilities, lawyers and their clients can timely and properly address Internet misuse in the workplace. q

[1] *See* Anonymous, Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network 164 (1997) (noting that workstations selling for five and six figures in the 1980s now sell for about $800 and do not in any way compare to today's typical desktop computer).

[2] *See* Carter & Katz, *Computer Crime: An Emerging Challenge for Law Enforcement*, FBI Law Enforcement Bulletin (Dec. 1996).

[3] The original paper outlining the concept of the Internet—as a web-like military computer network capable of surviving atomic attack—can be found and downloaded at **<http://www.rand.org/publications/classics/>**. *See also American Civil Liberties Union v. Reno,* 929 F. Supp. 828 (E.D. Pa. 1996) (describing the Internet and its uses).

[4] It is also worth noting that the risk of an organization's computers being attacked through a connection to the Internet has increased dramatically in the past year. *See Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute (March 1998).

[5] The Massachusetts Institute of Technology (MIT) makes PGP Version 5.0 ("Pretty Good Privacy," an understatement by all accounts) available for free downloading over the Internet. The site is at **<http://web.mit.edu/network/pgp.html>**.

[6] *See Knox v. State of Indiana*, 93 F.3d 1327 (7th Cir. 1996) (use of state computers to engage in sexual harassment via e-mail messages to victim).

[7] *See Greenslade v. Chicago Sun-Times, Inc*. 112 F.3d 853 (7th Cir. 1997) (use of newspaper computers to engage in sexual harassment via e-mail).

[8] The use of the Internet to accomplish direct file transfers is discussed *infra* in the section on Internet Relay Chat (IRC) networks.

[9] Filtering software can restrict access to Internet sites. It functions by comparing its internal list of off-limits sites and terminology to an employee's intended Internet destination or search terms. Access to sites the software deems offensive is then blocked.

[10] True e-mail anonymity is achieved by encrypting it and then routing it through several anonymous remailers. This way, no single remailer knows both where the message came from *and* where it is going. Most remailers perform this service free of charge. A sophisticated encrypting remailer program, Mixmaster, is available for free on the Internet, at **<http://www.obscura.com/~loki/>**. *See* **<http://www.obscura.com/~loki/remailer/mixmaster-faq.html>**

(explaining anonymous remailing).

[11] The sheer volume of newsgroups in existence makes it a practical impossibility for one ISP or online service provider to offer access to all Usenet newsgroups. Thus, ISPs select the newsgroups that their customers can access. There are indirect methods of accessing newsgroups not carried by an ISP. An employer should not assume that an employee cannot access certain groups just because the company's ISP does not offer them.

[12] *See, e.g., alt.smokers.cigars* (cigar aficionados); *alt.tv.seinfeld* (for viewers of the popular TV series).

[13] *See, e.g., alt.sex.pedophilia.pictures, alt.sex.pre-teens* (for pedophiles); *alt.warez.ibm-pc* (for unauthorized copies of IBM-compatible software); *alt.phreaking, alt.2600 and alt.bbs* (tips on theft of telephone services).

[14] The search was conducted using DejaNews' Newsgroup Interests search feature, at **<http://www.dejanews.com/>**.

[15] The mIRC program is a "client" program. A client program is simply software that requests access to another computer, here the IRC networks. Clients are so named because they require a connection to another network computer (called a "server") to function. In contrast, more familiar software such as WordPerfect or Lotus are self-contained programs that do not depend on remote computers to perform their functions.

[16] ICQ is on the Internet at **<http://www.mirabilis.com/>**. Its software can be downloaded directly to an employee's computer from this site.

[17] *Fired Oracle Worker Convicted for Phony E-Mail*, Bloomberg News (Jan. 29, 1997).

[18] *See, e.g.,* Fla. Stat. §815.07 (1995). For an excellent summary of state computer-related criminal statutes, and the complete text of relevant excerpts from each state statute, *see* Icove, Seger and VonStorch, *Part IV, Computer Crime Laws* 83–85, 239–332 *in* Computer Crime: A Crimefighter's Handbook (1995); *see also* **<http://www.eff.org>** (Internet site for the Electronic Frontier Foundation, which has downloadable copies of state computer crime statutes).

[19] *See* Fla. Stat. §921.0012(3) (1997) (designating computer offense devised to defraud as Category 3 felony); *United States v. Delmarle*, 99 F.3d 80 (2d Cir. 1996) (upward departure from sentencing guidelines based in part on "[t]he use of Internet computers to transfer child pornography").

[20] Venue in the prosecution of online crimes has been determined using traditional tests, permitting actions to proceed "in any district in which the offense was committed." *United States v. Thomas,* 1996 FED App. 0032P (6th Cir. 1996). Based on the sweeping scope of many state statutory enactments on computer crimes, and the "everywhere, all at once" nature of the Internet, traditional venue tests might allow prosecution in any of the 50 states.

[21] *See* Cal. Crim. Code tit. 13, §502(j) (deeming California as situs of computer crime if any computer within that state was accessed during offense); Tenn. Code Ann. §39-14-603(3); S.D. Codified Laws §43-43B-8.

[22] *See e.g., United States v. Thomas,* 1996 FED App. 0032P (6th Cir. 1996) (criminal prosecution in Tennessee of California residents who operated online BBS featuring sexually explicit computer images that were acquired by Tennessee-based investigator).

[23] Fla. Stat. §815.01 *et seq.* (1997).

[24] For an excellent review of intellectual property protection in the Internet era, *see* David R. Ellis, *A Primer on the Law of Intellectual Property Protection,* 72 Fla. B.J. 34 (Jan. 1998).

[25] Fla. Stat. §815.04(3)(b) (1997).

[26] Fla. Stat. §847.0135(1) *et seq.* (1997).

[27] 18 U.S.C. §2251(c)(2)(A) & (B). The Congressional Findings preceding this act specifically cite computers and computer imaging technology as developments that have contributed to the problem of child pornography.

[28] 18 U.S.C. §1030(a)(1)–(7).

[29] This summary of the CFAA excludes some important provisions of the act that the authors felt had minimal relevance to Florida attorneys. The summary accurately portrays the general nature of the CFAA, but attorneys handling a specific matter that may be governed by the CFAA should thoroughly review it before discussing the matter.

[30] 17 U.S.C. §101.

[31] 18 U.S.C. §§2701 *et seq.*

[32] Excerpt from Internet site advertisement for WebSense Reporter Pro. *See* **<http://www.elmail.co.uk/security/websense/reporter.html>**.

[33] Excerpt from Internet site advertising Net Access Manager 3.0. *See* **<http://www.sequeltech.com/press/pr44.htm>**.

[34] 18 U.S.C. §2511(2)(a)(i).

[35] *See United States v. Mullins,* 992 F.2d 1472 (9th Cir. 1992) (employee's claim of ECPA violation rejected where employer intercepted communication during investigation of employee's misconduct).

[36] 18 U.S.C. §2510(5)(a). One view of the ECPA's definition of "electronic device" is that something more than the computer system itself, such as a separate device purchased specifically to eavesdrop, is required to constitute an "electronic device."

[37] *See Watkins v. L.M. Berry & Co.,* 704 F.2d 577 (11th Cir. 1983); *Epps v. St. Mary's Hospital of Athens, Inc.,* 802 F.2d 412, 416–417 (11th Cir. 1986).

[38] *See* notes 5 and 6, *supra*.

[39] *E.g., Iowa Formal Ethics Opinion 1996-1* (requiring attorneys who use e-mail to communicate with clients to use security measures such as encryption, and to obtain client consent or acknowledgment of risks associated with e-mail transmissions).

[40] *O'Connor v. Ortega,* 480 U.S. 709 (1987).

[41] The contents of the Netscape Navigator's cache can be ascertained by typing "about:cache" in the location field of the browser.

[42] *See Armstrong v. Executive Office of the President,* 97 F.3d 575 (D.C. Cir. 1996) (involving FOIA requests for e-mail authored by Colonel Oliver North, including one titled "Smoking Gun," that were previously thought deleted but in fact were stored on tapes as a result of White House archiving system).

[43] An excellent free service that is available for conducting searches of Usenet newsgroups can be found at **<http://www.dejanews.com>**.

[44] Yahoo! is located at **http://www.yahoo.com**.

[45] There are several excellent sources for information on how to seize and preserve computer evidence. One is a book originally conceived for the Behavioral Science Unit at the FBI Academy in Quantico, Virginia, *see* Icove, Seger & Vonstorch, Computer Crime: A Crimefighter's Handbook 391–396, 397–409. Another is a highly detailed memorandum prepared by federal law enforcement agencies, *see Federal Guidelines for Searching and Seizing Computers*, U.S. Department of Justice, Criminal Division, Office of Professional Development and Training, **<http://www.usdoj.gov/criminal/cybercrime/search_docs/toc.htm>** (150-page manual obtained under Freedom of Information Act).

[46] Some agencies are taking active steps to develop alternatives to system seizures. *See* Bowker & Drinkard, *Downloading: Using Computer Software as An Investigative Tool*, FBI Law Enforcement Bulletin (June 1996) (outlining benefits of downloading system data and evidence as less disruptive than traditional system seizures). This article can be viewed and printed on the Internet at **http://www.fbi.gov/leb/june961.txt**.

[47] P.D. Henry and G. DeLibero, *Strategic Networking: From LAN to WAN to Information Superhighways* 439–443.

[48] Information about the Computer Emergency Response Team, or CERT, can be found at **http://www.cert.org/**.

James Garrity *is a trial lawyer in the Employment Litigation Section of the Florida Attorney General's Office in Tallahassee. He graduated law school in 1984, clerked for Judge Daniel T.K. Hurley at the Fourth District Court of Appeal in West Palm Beach, and practiced in Tampa before joining the Attorney General's Office. He is a member of The Florida Bar's Computer Law Committee.*

Eoghan Casey *received his degree from the University of California at Berkeley. He spent four years working for NASA on the EUVE research satellite project, where he gained expertise in computer automation, computer networks, and the Internet. Mr. Casey also has expertise in programming and systems administration, and has performed extensive Internet development and research. He is a partner of Knowledge Solutions LLC (**http://www.corpus-delicti.com**), a training provider and information resource for attorneys, the forensic sciences, and law enforcement.*