Dealing with Digital Data in the Practice of Law: Do You Know Where Your Data Is?

By Andrew Beckerman-Rodau

Computers improve productivity. An attorney can quickly and easily modify documents. Networked computers enable almost instantaneous transfer of documents among support staff, colleagues, clients, and other parties involved in a transaction. Additionally, an Internet connection enables documents to be quickly and effortlessly shared among different parties without regard to physical location. For example, Ms. Attorney can write a first draft of a contract that can be sent to Ms. Client as an email attachment. Typically, Ms. Client would be able to download and read the draft in a matter of seconds (or at most minutes) whether she is across town or on the other side of the planet. Using a conventional word processing program, Ms. Client can make changes to the draft and email it back to Ms. Attorney. Once Ms. Attorney and Ms. Client finalize the draft, it can be forwarded, via email, to counsel representing other parties to the contract. Such transactions have become common place in light of the ubiquitous usage of email and word processing programs today.

The rapid expansion of wireless networks over the past decade has also increased productivity. Attorneys increasingly carry a PDA, such as a Blackberry, a laptop computer, or both. Wireless Internet access, commonly referred to as hotspots, abound. The ubiquitous Starbucks contain hotspots in most of their locations. Increasingly, airports offer wireless Internet access. And, most major business hotels offer wireless Internet access that is increasingly provided at no charge. Most recently, wireless telephone providers have begun to offer high-speed wireless Internet access throughout entire metropolitan areas, such as Boston. Some cities are even contracting with private companies to install wireless access for all city residents.

From one perspective, the widespread use of computers and digital data has not changed what an attorney does. They still spend substantial time drafting and reviewing documents. The use of computers and the Internet has merely replaced the use of the mail, the fax machine, and couriers in many situations. However, the increase in computer usage brings with it a decreased ability to control documents and to protect confidential client data. In the pre-computer era, documents had to be typed or printed and physically delivered to recipients for review. The nature of such documents made copying them difficult and time-consuming. The likelihood that a document would be subject to being copied and widely distributed was limited simply due to the difficulty and expense of doing this. In contrast, a document in digital form can be copied and widely distributed almost instantaneously whether it is one page or 500 pages in length. Additionally, the Internet allows such transfers to reach virtually around the world in a matter of minutes. Likewise, in the pre-computer era physical security measures such as locked file cabinets were generally adequate to protect confidential client data, especially since neither members of the public nor unauthorized persons would be allowed to wander around a law firm and rummage through client files. The attorney controlled access to the files and the documents contained in the files. Saving client data in digital form on a computer makes it more difficult to control access to such data.

The movement from a paper-based world to a digital world has not altered the obligation of attorneys to safeguard client information pursuant to the rules of professional responsibility. Such rules, which govern attorney conduct, generally mandate that an attorney must use reasonable efforts to safeguard client data against unauthorized or inadvertent disclosure by either the attorney[1] or non-attorney employees, such as paralegals, law students, investigators, and IT personnel.[2]

Although many legal issues involving the storage and safeguarding of digital data have not been definitively addressed by courts, state bar ethics and professional responsibility committees have provided some guidance in formal opinions. The Maine Professional Ethics Commission opined that an attorney could maintain all

Andrew Beckerman-Rodau is professor of law & co-director, Intellectual Property Law Concentration, Suffolk University Law School, Boston, MA. Reach him at arodau@suffolk.edu. www.suffolk.edu/arodau.

client files exclusively in digital form provided that she also maintained copies of any software needed to access the files in the future.[3] A recent opinion by the Nevada Committee on Ethics and Professional Responsibility went a step further by advising that confidential client computer files could be stored, without the consent of the client, on a computer system maintained by a third party who was not controlled by the attorney.[4] The opinion advised that this was not a breach of the attorney's obligation of confidentiality to a client provided that she acted competently and reasonably in insuring confidentiality.

DIGITAL DATA LOCATIONS

The first step in protecting digital client data requires knowing its location. Unlike paper documents, which have a physical location, digital documents may inadvertently reside in multiple locations. Additionally, substantial hidden data may reside in digital documents. Consequently, it is imperative to understand all the locations where digital data may reside before protective measures for client data can be both understood and implemented.

In most work environments, including law offices, personal computers appear on every desk. Each attorney, legal assistant, and many other employees have individual computers. It is typical for all such computers to be networked in order to enable users to share files. Additionally, networks usually are connected to the Internet to enable access to email and other Web-accessible resources. In this environment a file created by an attorney may reside on the computer that he or she is using. Alternatively, it may reside on a central file server even though it appears to be located on the user's computer. If the computer system uses a backup system, a copy of the file may also be located on a backup device, such as a magnetic tape, a CD, or a separate disk drive. When traveling to see a client, files also may be copied to an attorney's laptop, or they may be transported on a small keychain drive.

Commonly, files are sent to other attorneys, clients, and other parties as email attachments. These emails and their associated attachments will often be copied into a sent mail folder on the sender's computer. They will also be copied to the inbox of the recipient's computer. Copies may reside on a mail server computer used by the sender and on a similar mail server used by the recipient of the email. Additionally, copies may be stored on backup media used to backup the mail servers.

HIDDEN DIGITAL DATA

Digital copies of documents, such as word processing documents, PowerPoint documents, and spreadsheets, include hidden data often referred to as metadata. If you look at a printed document, it does not reveal all the changes and modifications made to the document during the editing and review process. It does not tell you who authored and edited the document. It does not tell you the specific computer on which the document was written or who the document was sent to for review. In contrast, a digital copy of the document may contain all of this information. Although this metadata is hidden, much of it is easily retrievable with inexpensive off-the-shelf software or free software downloadable from the Internet. Additionally, a computer system will create metadata that is used to store, index, and find data. Such metadata is most analogous to an old-fashioned library card catalog.

Although it is difficult to erase all hidden or metadata data, it is possible to destroy most of such data embedded in a document. Microsoft provides a free utility[5] that integrates itself into programs such as Word, PowerPoint, and Excel. This utility can be used to effectively delete most metadata. Third-party programs that scrub hidden data are also readily available. Finally, converting documents to graphical formats, such as PDF, eliminates most metadata.

DATA PROTECTION

A system for backing up data is essential, since computer storage media can and do fail. Such failures are typically without prior warning, so lack of an adequate backup system can be catastrophic. Recreating data is costly. Additionally, some data may not be capable of being recreated. This can create substantial costs and potential liability for a client. Additionally, it can be argued that an attorney's failure to use an adequate backup system is unreasonable. This is especially true today, when robust automated backup systems are relatively inexpensive. Hence, lost data due to lack of a backup may render an attorney in violation of his or her ethical obligation to reasonably protect a client's data pursuant to the rules of professional responsibility.

Relying on floppy disks, zip disks, CDs, or DVDs as backup media is inadequate. Magnetic media, such as floppy disks or zip disks, provide short-term backups but are prone to failure over time. In many cases, data will become very difficult to retrieve from such media after a few years. Likewise, optical media, such as CDs or DVDs, are also poor media for long term backups. Although they may last up to 10 years, such optical media can suffer from deterioration of the disk coating, which will render the stored data unreadable. Other common options include magnetic tape backup systems and external hard drives. For large amounts of data, tape backups tend to provide

a good option due to their capacity. However, the cost of hard drives has been continually decreasing despite large increases in data capacity. Consequently, external hard drives or network hard drives may be the most cost effective backup media today. The safest backup strategy requires use of multiple media, since it is statistically improbable that several backup media will simultaneously fail. One reliable approach in a networked environment is to have all users store files on a network server. Automated backup software can run in the background in real time backing up each computer user's files to the local drive on his or her computer. Additionally, the network server hard drive can be periodically backed up onto a tape drive or a redundant hard drive. This approach, which is used by the author, recently resulted in no data loss despite a catastrophic network server hard drive failure combined with a backup system failure.

Another option is storing data offsite with a third party. Businesses provide data storage backup for a wide variety of costs. Critical data that can neither be lost nor replaced can be stored with companies that provide highly secure redundant data storage sites in various secret locations dispersed over a wide geographic area. Less costly options also exist. However, one important concern is how the data will be transferred to the storage company. Some enterprises ship media containing data via the mail or via commercial package delivery services. This has resulted in instances of lost data. Alternatively, data can be sent to a storage company electronically via an Internet connection. If encryption is used such data transmission is relatively safe.

Probably the most critical aspect of a data backup strategy, without regard to what system or hardware is used, is to automate it so that it is performed on a regular basis without the need for human intervention. If a backup strategy is not automated, no assurance exists that it will be performed on a regular basis. This can lead to a devastating result, since data storage device failures tend to happen without advance warning.

In addition to protecting data from loss or destruction, data must be safeguarded to limit unauthorized and inadvertent access. If computers are networked, any openly accessible computer may provide a doorway for accessing confidential data stored on computers connected to the network. Think of each computer as a door to your file room where confidential client data is openly available. Unsecured networked computers are akin to allowing unlimited access to the door to your file room.

Passwords are a first line of defense for securing computers. The amount of security provided by passwords is proportional to the password procedures employed. Short easy-to-guess passwords that are never changed can significantly undermine security. It is preferable to use long passwords that include letters, numbers, and symbols. Moreover, passwords should be periodically changed, preferably at least every few months. A simple technique for creating complex passwords that are easy to remember is to memorize a sentence. The first or last letter of each word in the sentence can be used as the password. Adding a number and symbol to the password will increase its strength. Strong passwords should meet the following criteria:

1. They should consist of more than eight characters.
2. They should include letters, numbers, and symbols.
3. They should include large and small letters.
4. They should not include sequential or repeating combinations of numbers or letters.
5. The should not consist solely of adjacent letters on the keyboard.
6. They should not consist of common words with numbers or symbols substituted for certain letters.
7. They should not consist of your login name, your name, your birthday, your spouse's name, your children's names, your pet's name, or any other easy-to-guess word or name.
8. They should not be a word found in an English or foreign language dictionary.
9. They should be easy to remember but difficult for a third party to guess.
10. They should not be too difficult to remember, since this will result in the password's being written down, which can defeat the benefit of a strong password.[6]

A simple online utility maintained by Microsoft, available at *http://www.microsoft.com/athome/security/privacy/password_checker.mspx*, can be used to provide a rough evaluation of the strength of a password.

In addition to the above rules, some additional ones apply to computers used in the workplace or on laptops carried during travel. The "remember password" option should not be checked, since this would allow third-party unauthorized access without the need to know the password. The newest versions of the Netscape and Firefox Web browsers include a convenient function that can automatically remember usernames and passwords for Web-accessed sites. This function, if activated, can allow unauthorized third-party access. Workplace computers will be unattended at times, so it is recommended that a screensaver be activated with a password being required to deactivate the screensaver. Finally, a power-on password provides an extra layer of security because it must be entered before the computer operating system will boot up.

Due to limited cost and ease of setup wireless networks are becoming an increasingly common method of providing network access. However, if such wireless

devices are setup without enabling built-in security, a wide doorway into your network is open and easily exploited. Virtually all laptops currently sold include wireless cards and software that automatically picks up and identifies available wireless networks. Since wireless networks use radio waves, the signal from the network can not be contained within an office. Hence, a laptop in an adjacent office or on an adjacent public road will automatically pick up the network's signal and allow access if network security is not enabled. In addition to enabling security, it is advisable to configure the network so that it does not broadcast its availability. If this is done, the conventional network software preinstalled on most laptops will not indicate the existence of the wireless network.

Publicly accessible wireless networks, such as in hotels or in airports, can create a security risk when accessed by a laptop. These networks are designed to be open and freely accessible. Consequently, these networks provide little or no security. This enables third parties to capture data sent to and from your laptop via the wireless network. One solution to this problem is use of a virtual private network connection (VPN). A VPN essentially creates an encrypted private data path between your laptop and a remote server that operates over any network, including publicly accessible wireless networks. Software for creating a VPN can be installed on a firm's computer network. Or, commercial VPN providers can be used for a fee.

Portable storage media, such as external hard drives, flash memory, and keychain drives, are becoming increasingly common. This is due in large part to significantly increased storage capacity coupled with significantly reduced cost. Generally, files are stored in native format on such devices so they are easily read by anyone with physical access to the device by merely connecting it to a computer. Encrypting data stored on these devices, which can be easily done, greatly limits access to the data.

Equipment disposal is an often overlooked security weakness. Computers are routinely replaced every three to five years. The hard drives on old computers contain substantial amounts of data. Even if this data has been deleted, much of it can be recovered with inexpensive off-the-shelf software. Likewise, data can be recovered from portable media, such as floppy disks and zip disks, even if it has been deleted. Therefore, any data storage media should be physically destroyed, or prior to disposal, it should be subjected to an erase program that renders the data unrecoverable. It is important to understand the distinction between data deletion and data erasure. Data deletion merely modifies the data address so that the computer knows to ignore the data as if it does not exist. Eventually, the data will be written over by subsequent data. However, prior to being written over, the data continues to exist. In contrast, erase programs, when activated, will immediately engage in continually writing over the data to be erased. This method, which is used by the US military and other government entities, effectively renders the erased data unrecoverable in most circumstances.

In addition to backing up digital data and protecting it from unauthorized access, precautions should be taken to preserve data integrity by blocking viruses and spyware. Although it is impossible to totally eliminate these risks, it is possible to substantially minimize them. First, appropriate software, including a firewall program, an antivirus program, and an antispyware program, should be installed on all computers. Highly effective versions of such software are available today at modest cost. Typically, multiple firewall and multiple antivirus programs cannot be simultaneously run on a computer. However, it is generally possible to simultaneously run multiple antispyware programs. Running such multiple programs is advisable, since spyware is perhaps a bigger problem today than viruses. Nevertheless, virus and spyware programs are effectively worthless unless they are updated on a continuous basis. Likewise, if you use a Microsoft operating system, it is imperative that regular free software updates are downloaded from Microsoft's Web site.[7] Typically, these updates are actually software repairs or patches in response to newly discovered security vulnerabilities.

LITIGATION RISKS

The widespread reliance on digital data in lieu of paper documents has radically altered discovery. In the past, discovery involved obtaining and manually reviewing voluminous amounts of paper documents. Today, electronic discovery of digital data is commonplace.[8] Parties subject to electronic discovery risk disclosure of more information than anticipated. Copies of documents that you believe no longer exist as well as hidden metadata may be unknowingly given to opposing counsel pursuant to discovery demands. The result could be inadvertent disclosure of trade secrets or other proprietary information. Additionally, attorney-client privileged data can be inadvertently disclosed. The consequences of disclosing such privileged data vary in different jurisdictions although in some jurisdictions it may result in a waiver of the attorney-client privilege. Often email is a fertile source of damaging information due to the informal nature in which employees exchange information via email. Moreover, courts have come to understand the difference between providing printed documents and electronic documents. Consequently,

attempts to provide paper documents in lieu of digital documents have been rebuffed by courts.[9]

Parties seeking discovery must also be technologically knowledgeable to insure they ask for the most useful information and data. The format of the data requested can be critical. For example, obtaining images of hard drives can yield more information than receiving data files copied to a CD, and knowing where to look for data is critical. Understanding the numerous places relevant data can exist, as discussed above, enables discovery requests to target potentially important data.

Electronic discovery also may increase costs because attorneys need training to insure they are sufficiently tech-savvy. Typically, forensic computer specialists must be used to collect and review computer data obtained in the discovery process to ensure useful data is harvested. Compliance with electronic discovery requests can also require costly computer experts to insure proprietary or privileged information is not inadvertently disclosed.

ELECTRONIC DOCUMENT RETENTION PROGRAM

Businesses have long relied on document retention programs as a method of determining how long documents should be kept prior to destruction. Ostensibly, one justification for destroying documents was the expense of storing an ever increasing amount of paper. The relatively low cost of digital storage makes this justification less convincing with regard to documents and data stored in digital form. However, managing and knowing the content of computer data, including metadata, can become an expensive and time consuming task. Consequently, retaining an unlimited amount of digital data increases the likelihood of inadvertently disclosing damaging and/or proprietary information. These risks provide a strong justification for developing an electronic document retention program. However, when setting up such a program it is important to be cognizant of state and federal requirements which may set different time periods for keeping different types of documents. Additionally, a mechanism must be in place to halt document destruction in the event of pending litigation. Otherwise substantial legal sanctions could apply if the destroyed data would have been information subject to a discovery request.

EMPLOYEE ISSUES

Data protection ultimately depends on employee conduct. Employee computer usage policies that are enforced are a necessity in a modern computerized work environment. Security policies requiring strong passwords that are periodically changed can be mandated by setting up such electronic policies on all workplace computers. Once created these policies insure compliance by rejecting weak passwords and automatically requiring creation of new passwords at a prescribed time interval.

A computer usage policy should address all of the following:

1. Downloading programs and data from the Internet. This should be prohibited, unless absolutely necessary, since this is prime source of viruses and spyware.
2. Installing programs and data brought from home. This should also be prohibited since it is another prime source of viruses and spyware.
3. Creating and protecting passwords. It is important to both emphasize the importance of picking proper passwords and the importance of safeguarding them by not writing them down in easy to find locations.
4. Secure storage and destruction of all portable data storage media such as disks, CDs, DVDs, and keychain drives. It is critical that employees understand that portable media continues to hold data even if the data has been erased. Hence, such portable media should not be left unattended unless it is placed in a secure location. Also, portable media such as disks or CDs should be physically destroyed prior to being disposed of in the trash.
5. Modifying existing computer equipment such as by adding modems or wireless access points. These devices should never be employee-installed because they can comprise even the best network security.
6. Usage of email and if used, blogs, Web sites, and IM. These are all commonly used tools today in many work environments. It is important for users to know that anything put in an email or an IM exchange or uploaded to a Web site or blog will often be permanent. Hence, a good rule of thumb is nothing should be written that the user would be uncomfortable seeing on the front page of the local newspaper.
7. Notifying employees that computers, computer equipment, and all data belongs to the employer. This can help limit any problems with employees installing personal programs or data on the computer which is an inherent security risk.
8. Automatically terminating all computer access when employment ceases for any reason. This limits the risk of a disgruntled involuntarily terminated employee's destroying data or engaging in other destructive actions. It also limits a former employee working for a competitor from using information from his former employer for the benefit of the competitor.

Periodic employee training sessions are important to educate employees about the risks related to the use of digital data. Absent such training on an ongoing basis employees are unlikely to take data risks seriously.

IT personnel typically have virtually unlimited access to all computers and computer data. This is both a consequence of the need for such access in order to maintain and troubleshoot the computer resources and due to the very nature of their expertise. Hence, it is critical to perform background checks on all technical support personnel. It is also important to make certain IT personnel are adequately trained since this is not a government regulated profession. Improper or negligent conduct by IT personnel can severely impact a law firm and its clients if digital data is lost, damaged or improperly released to the public. Additionally, attorneys can be held liable for actions of IT personnel. Pursuant to the rules of professional conduct, attorneys are obligated make certain non-attorney employees protect confidential client data pursuant to the ethical standards applicable to the attorney even though non-attorneys are not subject to these rules.

CONCLUSION

The use of computers in the practice of law does not alter the obligation to protect confidential client data. Computer usage increases productivity but makes protection of confidential data more difficult. In contrast to paper documents, digital versions of documents are easy to copy and distribute. Moreover, the inherent nature of computer systems results in copies of digital documents being stored in multiple locations that decreases the ability to control such documents. Digital data also must be protected against loss by creating backup copies and by properly disposing of media containing digital data. Likewise, appropriate software must be installed to protect against electronic threats from viruses and spyware. Understanding and appropriately removing hidden metadata from digital files can reduce litigation risks from the inadvertent disclosure of confidential client data. Adoption of electronic document retention programs can further reduce litigation risks. Finally, adoption of a computer usage policy coupled with ongoing education about the risks inherent in the use of digital data is necessary to insure that digital data is properly safeguarded.

NOTES

1. *See, e.g.*, ABA Model Rules of Professional Conduct, Rule 1.6 (reprinted in Thomas D. Morgan & Ronald D. Rotunda, 2003 Selected Standards on Professional Responsibility at 25 (2003)).
2. *See, e.g.*, ABA Model Rules of Professional Conduct, Rule 5.3 (reprinted in Thomas D. Morgan & Ronald D. Rotunda, 2003 Selected Standards on Professional Responsibility at 114 (2003)). Although the Rules of Professional Conduct do not apply to non-attorneys (*see, e.g.*, In the matter of Burns, 657 N.E. 2d 738, 740 (In. Sup. Ct. 1995)), such rules require an attorney to make certain non-attorney employees abide by these rules, and the attorney may be responsible for violation of these rules by non-attorney employees (*see, e.g.*, Daines v. Alcatel, 194 F.R.D. 678, 681-682 (E.D. Wa. 2000)).
3. *See* Maine Professional Ethics Commission of the Board of Overseers of the Bar, Opinion No. 183 (Jan. 28, 2004) (available at *http://www.mebaroverseers.org/Ethics%20Opinions/Opinion%20183.htm* (last visited Mar. 14, 2006)).
4. *See* State Bar of Nevada Standing Committee on Ethics and Professional Responsibility, Formal Opinion No. 33 (Feb. 9, 2006) (available at *http://www.nvbar.org/Ethics/Ethics_Opinions_DETAIL.htm* (last visited Mar. 14, 2006)).
5. Information about metadata and Microsoft data removal tool is available at *http://office.microsoft.com/en-us/assistance/HA011400341033.aspx* (last visited Mar. 15, 2006).
6. *See http://www.microsoft.com/athome/security/privacy/password.mspx* (last visited Mar. 19, 2006). *See also http://www.utexas.edu/computer/passwords/choose.html* (last visited Mar. 19, 2006).
7. Information about Microsoft security updates is available at *http://www.microsoft.com/security/default.mspx* (last visited Mar. 15, 2006).
8. Fed. R. Civ. P. 34(a)(1) makes electronic documents discoverable.
9. *See, e.g.*, Gilliam v. Addicts Rehab. Ctr. Fund, Inc., 2006 WL 228874 (S.D.N.Y. Jan. 26, 2006).