TechnoFeature™

Practice management and technology articles written by experts.

A Lawyer's Guide to Mobile Computer Security

By Jim Calloway, Ellen Freedman, and Reid F. Trautz

(Originally Published in Immigration Law Today, Oklahoma Bar Journal, and The Pennsylvania Lawyer: Ellen Freedman, Reid Trautz, and Jim Calloway, A Lawyer's Guide to Mobile Computer Security, Immigration Law Today, Jan/Feb 2007, Oklahoma Bar Journal, November 4, 2006, The Pennsylvania Lawyer, March/April 2007.)

INTRODUCTION

A personal computer is lost or stolen every 12 seconds. Most contain confidential or sensitive information.

An article in the Sept. 22, 2006, online issue of Enterprise Security Today was titled, "Hundreds of Census Bureau Laptops Lost." The article went on to detail that the Census Bureau has had 217 laptops, 46 portable data storage devices, and 15 handheld devices become lost or stolen since 2003. All held confidential information. In fact, the Commerce Department performed a review and found that since 2001, the department's 15 operating units had lost an astounding 1,137 laptop computers, all containing confidential information. The monthly newsletter Privacy Journal reported 24 significant instances of Social Security numbers and other sensitive data being placed at risk through stolen or lost laptops in 2006.

Of course just one missing laptop can expose a great deal of information. Most will recall the media firestorm when a laptop containing personally identifiable information of 26.5 million veterans and family members was stolen from the home of an employee of the Veterans Administration.

Having to explain to a client or disciplinary authority about lost or exposed client data on a missing laptop would be unpleasant and difficult. With all of the reported instances of this happening, how could anyone seriously maintain that they had no idea that a laptop with confidential information could be lost or stolen?

But PCs aren't the only mobile devices that can contain confidential information. Virtually all mobile devices and removable media could potentially expose the typical law firm to embarrassment and even serious ethical breaches if they fall into the wrong hands. Law firms need to start devoting more attention to protection of information on USB devices like thumb drives and iPods or other MP3 players; to removable media like CDs, DVDs, floppy disks and external hard drives; to seemingly innocuous devices like dictation recorders; and to wireless devices like cell phones, smart phones, and personal digital assistants (PDAs).

We should also be aware that information can be stolen from a computer without the alarm created by vanishing hardware. Software is readily available on the Internet for efficiently purloining data. For example, third-party packet capture driver applications enable nefarious use of USB thumb drives. It prepares the device to enable both data and large applications to be copied onto the removable media within seconds. Now a hacker no longer needs to have a laptop available to compromise a network. A USB flash drive can be plugged into a PC and used to steal large quantities of information rapidly. Similar software for MP3 players is now available.

It would be easy for a short-sighted law firm manager or IT director to decree that no client information would ever be taken out of the office on a mobile device. But the demands of today's workplace make laptop computers, PDAs, flash drives, and other devices almost a requirement for many. It would be inconceivable to travel to visit with a client in another state without taking a laptop packed with information about the client's files so that any question could be answered quickly. Remote access to the office network over the Internet is an important

(Continued on next page)

productivity component for lawyers who are home with a sick child or traveling. And, of course, email with documents and other data files attached leaves the office regularly.

It follows then that when we talk about mobile security, we are primarily talking about training staff and lawyers to be aware of the risks of losing important information and adopting policies to secure confidential information. There is a need for every firm to develop and implement a computer use policy which carefully balances the need for security with the need of users to accomplish tasks effectively and efficiently without creating undue administrative burden.

This article will examine the various areas to be considered when drafting and implementing a computer use policy.

A personal computer is lost or stolen every 12 seconds. Most contain confidential or sensitive information.

METADATA

By now most lawyers should be aware of the fact that documents contain hidden information called metadata. There have been some embarrassing moments for individuals who are unaware that the documents they emailed contained hidden information which might embarrass the sender. For example, some of the most problematic items of metadata are deleted comments or document revision history. Tools that expose metadata and instructions on how to look for it are readily available on the Internet. Sending a document to opposing counsel that potentially exposes the client's comments made while reviewing the document could constitute a major ethical breach.

Law firm personnel must appreciate the potential problems of metadata and deal with it before emailing a document outside of the office. One way to create a document that is virtually metadata free is to create a new "clean" document just before emailing it. First open a blank document. Then one can select the text in the original document, copy it to the clipboard, and paste it into the new blank document to create a new document with no troublesome metadata.

WordPerfect users might consider upgrading to version X3, which has a "save without metadata" feature. There are various commercial products available for both viewing and deleting metadata from a document, such as the Metadata Assistant from Payne Group. Another option is to always have a policy of printing a document to PDF before allowing it outside of the office. While PDF documents created in this manner retain some metadata, it is limited and not of the type likely to expose client confidences or to prove embarrassing.

DOCUMENT SECURITY

While the issue of metadata is getting all the attention these days, we cannot overlook the basic matter of office processes for protecting access to sensitive documents. There are two ways to protect access to documents and the confidential information contained in them: authentication and encryption. Encryption is explained further below.

Not all documents generated by a law firm contain sensitive or privileged information. But documents are the lifeblood of attorneys. Attorneys have a duty to preserve and protect the confidentiality of that information. That task is made more difficult when documents are accessible across a firm network or shared electronically with clients, co-counsel, opposing counsel, and the courts via email, e-filing, and extranets. Securing confidentiality is now much more difficult than just locking a file cabinet or a desk drawer.

Authentication is the common term for proactively limiting access to electronically created documents only to those people we want to have access. We can easily install authentication requirements on a computer to view a document, folder, or the entire computer. Biometric authentication — fingerprint and iris scans for example — is an emergent method, but passwords are by far the most common

(Continued on next page)

form of authentication. All computers should require at least one password to log onto the computer. Moreover, individual documents containing sensitive information that are shared electronically should also be individually password protected.

Passwords can be very strong or relatively weak. A strong password will be at least nine characters in length and contain both letters and numbers or typographic symbols.

Even a relatively insecure, or "soft" password may have some benefits. A firm could adopt a universal password for all documents to be taken outside of the firm in any way, including by email attachment. This password would be communicated to clients, co-counsel, and opposing counsel by phone. While the widespread knowledge of this password would limit its effectiveness, it would go a long way toward protecting "lost" documents disclosed via mis-addressed email, a lost CD-ROM, or a lost USB flash drive.

Policy should require that the password never be given out to a caller, but only via a return call to a phone number contained in the firm's records. It should also never be sent out via email, especially in the email transmitting the document.

HOW TO PASSWORD PROTECT DOCUMENTS

Taking this extra precaution is quite easy, whether you use Word or WordPerfect to create your documents. In MS Word 2003 under "Tools" "Protect Document" you can limit editing to read-only, comments, and track changes. Under "Tools" "Options" "Security" you can enable password protection to open or modify a document. There are also privacy options, such as "make hidden markup visible when opening or saving" and "warn before printing, saving or sending a file that contains tracked changes or comments."

In WordPerfect, click "File" "Save As." Check the "Password Protect" box in the lower corner of the dialogue box that opens. Then click "Save" and enter a password in the dialog box that opens.

Even though all of the law firm staff are presumed to be trustworthy, it may make sense to utilize password protection on some occasions so that particularly sensitive client documents are only accessible by a few.

LOCKING DOWN PDF FILES

Another way to protect documents from unwanted changes or exposure is to consider saving your Word or WordPerfect file in Portable Document Format (PDF). This is also known as "publishing to PDF." WordPerfect has this function in all recent versions. Adobe Acrobat is the preferred, if most expensive, method but there are utilities that provide less expensive PDF publishing. By using these tools, law firm users can "lock down" documents, disallowing printing, copying, editing, commenting, or even opening the document. One can encrypt the file or use secure digital signatures and other authentication protocols. By "locking down" PDF files, attorneys can make sure that the document is used in the way they want, without exposing it to alteration or copying. In other words, it is a more secure way to send documents to clients and opposing counsel and know they cannot be altered, or that one can easily see the alterations, depending upon the options you chose.

A strong password will be at least nine characters in length and contain both letters and numbers or typographic symbols.

ENCRYPTION

Password protecting a document reminds one of the old adage that locking your doors will keep out honest people, but would likely only slow down a professional thief. For critically important information, document encryption is the solution rather than password protection. A marital dissolution settlement proposal might be effectively protected by a password. However, information about a proposed multimillion-dollar merger or the defense of a criminal matter making national headlines might need to be encrypted.

Encryption is the process of obscuring data or

(Continued on next page)

information to make it unreadable without special software or knowledge to decrypt it. Governments and military have long used encryption to protect sensitive communications, but commercial encryption products have emerged in the marketplace to protect software, Internet communications, mobile data, cell phones, and other sensitive information.

To encrypt digital information, the document, folder, or data file is run through a software application to obscure the information. There are various levels of obscuring, generally stated in "bits;" the higher the bits, the harder to decrypt the information. Currently 256-bit encryption is a common standard, but super-sensitive documents will have higher levels. The way to de-encrypt the information is with a "key." The key is often a pass code or another software program tied to the original encryption software.

For critically important information, document encryption is the solution rather than password protection.

An obvious danger with document encryption is that the loss of the key effectively "loses" the document.

Let us now consider security concerns related to computers and storage devices rather than just documents.

CD-ROMS, DVDS AND FLOPPY DISK DRIVES

Although one can encrypt or password protect CD-ROMs, DVDs, and floppy drives, it generally makes more sense for the user to encrypt or password protect the documents individually as noted in the preceding section. It is also probably a good practice to keep a business card in any disk carrier just in case an honest person finds it if it is lost.

USB FLASH DRIVES

The use of USB flash drives is increasingly widespread. A USB flash drive is a small removable data storage device that plugs into almost any computer built in the past five years or so and is commonly used to transport and share documents. These devices are as small as a matchbook or ink pen but can hold thousands of documents, hundreds of photos, songs, or slide presentations. It is plugged into the USB port on any other computer for access to any documents and other files previously transferred to the device.

These tools can be especially helpful if you do not have remote connectivity to your office network. USB flash drives have largely replaced floppy disks for transporting a few documents home. For example, if a lawyer needs to redraft one agreement or finish drafting an article over the weekend, it can be copied to a USB flash drive when leaving the office. Then one can plug it into another computer and work on the document. When finished, one should save it only on the flash drive, not the other computer's hard drive.

Although these devices are very convenient, there are two main security issues: They are easily misplaced, and they can leave confidential data on the temporary host computer.

To avoid losing the flash drive, attach it to your office or car keys with a small but secure chain. Treat it like a million dollar nugget of gold; you always know where it is at all times. Why? Because that may be the cost to settle a malpractice claim if confidential information is lost or stolen.

PROTECTING THE DATA ON YOUR FLASH DRIVE

The two most common methods to protect this data are authentication and encryption.

As discussed above, authentication is often a password to access the data. Some lawyers take the precaution to use a password to access the flash drive contents and a second password for each file or folder on the flash drive.

Encryption is the other method of protecting your data. Although some flash drive users view this as an inconvenience, it is much more secure than just a password.

Flash drive manufacturers continue to meet the

(Continued on next page)

security demands of consumers and now add authentication and/or encryption software to some flash drive models. For example, Lexar Media adds password-protected 256-bit AES encryption to its JumpDrive Secure flash drive. Not every document needs to be protected, but it's nice to know you can secure critical documents and data with less worry if it is lost.

PORTABLE HARD DRIVES

Portable hard drives are external storage devices that can be easily transported in a briefcase, purse, or pocket. These devices make it easy to carry your data backup home. They can hold more information than a flash drive, often as much or more than any computer in your office. They connect to any computer through a cable, usually a USB or Firewire cable.

The portable hard drive has leaped in popularity as the physical size of the devices has dropped, the storage capability has skyrocketed, and the prices continue to fall. Manufacturers include Iomega, Seagate, Pocketec, and CMS Products.

Many smaller firms are buying two of these devices to use for their data backup protocol instead of using a magnetic tape drive. Coupled with reliable back-up software (included with some portable hard drives), the firms swap the two hard drives on a daily or weekly basis, keeping the other in a secure off-site location.

As with any other information-laden storage device that leaves your office, it must be secured against the possibility of theft or being lost. Again, authentication and encryption are the best methods to protect data confidentiality.

From a security standpoint, these drives have the same attendant risks and protection schemes as USB flash drives. They are slightly more inherently secure when used as backups because the backup software will compress the data, often in a proprietary format. In addition, they sometimes work through proprietary installed software systems rather than the "plug-and-play" model of the USB flash drives. The finder of the lost USB flash drive merely needs to stick it into a computer's USB port to look at the contents. Spying on compressed data in a found backup portable hard drive would present a greater challenge to the average user.

MOBILE PHONES AND PDAS

The current generation of high-end mobile phones incorporates many of the information carrying characteristics of computers. Smart phones now incorporate all of the functionality of PDAs.

Unfortunately, password protecting a mobile phone would tend to reduce a great deal of its functionality and convenience. One should still consider whether documents placed on a mobile phone should be password protected. Probably the most practical advice is to consider whether sensitive documents should be placed on a mobile phone at all.

The most important apect of mobile security is for your law firm to consider everything in advance and draft a well thought-out policy.

Some PDAs and mobile phones now provide for remote purging of the information when they are lost. One law firm that unsuccessfully tried to utilize this feature on a phone learned that it would not work in the shielded lower floors of a parking garage, where it was lost.

LAPTOP COMPUTERS

The number of lawyers who have laptop computers is significant and steadily growing. It is a great convenience to have much of your client information, your forms, and other digital data with you when traveling or even going home at night. However, the loss or theft of a laptop is not as rare as one might think, as noted previously.

The minimum standard for laptop protection is that it should be password protected. For laptops that are typically attached to a network, this is already done by the network login password.

(Continued on next page)

Readers will begin to notice some familiar themes. Sensitive documents on a laptop can be either password protected or encrypted. Sometimes it may make sense to encrypt the entire folders for keeping important documents safe.

Laptops left unattended in a hotel room can be secured by chain lock devices similar to those used to protect a bicycle. (Just make sure you don't "secure" it to a table leg or something else that can be raised up.) Screen protectors can be used to block prying eyes when working in public or on an airplane.

The authors have received, but not yet reviewed, some sophisticated software packages that enable a stolen computer to "phone home" when it is connected to the Internet. There are also packages for remotely deleting sensitive information when the laptop is connected to the Internet. While these concepts are new and "cutting edge" at present, one can anticipate that they will become the minimum security standard within a few years. Likewise, it is no longer the stuff of science fiction to consider a laptop with fingerprint or iris scanning authentication.

We will continue to see both challenges and improvements with our digital security plans. One of the most interesting methods of laptop remote access security utilizes a key fob which displays a series of numbers. The displayed numbers change every few minutes and is synchronized with the office computer network. To log in to the network requires entry of the current set of numbers followed by a several digit number that the lawyer had memorized. The theory is that even if the purpose of the key fob is known and it was lost or stolen along with the laptop, one would still be unable to crack the network without the memorized set of numbers.

CONCLUSION

The most important apect of mobile security is for your law firm to consider everything in advance and draft a well thought-out policy. Training and education are also key. Like any other business, a law firm has to stay competitive. That will mean that a firm has to take advantage of the benefits of mobile technology. Thus, drafting a written plan for mobile computing security is important for both the law firm and the clients.

ABOUT THE AUTHORS

Jim Calloway is the director of the OBA Management Assistance Program and manager of the OBA Solo and Small Firm Conference. As a member of the ABA, he served as chair of the ABA TECHSHOW 2005 board, on which he has served as a board member for the past three years.

Contact Jim:
E: Jimc@okbar.org

Ellen Freedman, CLM, is law practice management coordinator of the Pennsylvania Bar Association and president of Freedman Consulting Inc.

Contact Ellen:
E: ellenf@comcast.net

Reid F. Trautz heads the American Immigration Lawyers Association's Practice and Professionalism Center, where he provides ethics guidance and practice management information and consulting services to AILA members to help them improve their businesses and the delivery of legal services to their clients.

Contact Reid:
E: rtrautz@cox.net

About TechnoFeature
Published on Tuesdays, *TechnoFeature* is a weekly newsletter containing in-depth articles written by leading legal technology and practice management experts, many of whom have become "household names" in the legal profession. Most of these articles are TechnoLawyer exclusives, but we also scour regional legal publications for superb articles that you probably missed the first time around.