# SAFEGUARDING LAPTOPS, ELECTRONIC DEVICES, AND PROTECTING CONFIDENTIAL CLIENT DATA

Ellen Freedman, CLM


---

It's a dangerous world for electronic gear, and the confidential data which resides on it. According to the FBI, more than 1700 computers are stolen in the U.S. every day, and 97% are never recovered. Add to that the Blackberrys, PDAs, and cell phones, and that adds up to a tremendous amount of confidential information falling into the wrong hands. Where are your exposures? How do you protect your devices? What can you do to maximize your protection of sensitive data? Finally, when all else fails and there is a breach of security, what must you do to respond? This article will attempt to answer as many of these questions as possible in the space provided.

The inherent portability of most electronic devices today, coupled with ever increasing storage and computing power, creates greater exposure for loss of sensitive data. Inadvertent loss is the first exposure; usually caused by leaving one's cell phone, PDAs, digital recorder, or other device absentmindedly behind. I have had more than my share of calls from attorneys on board a train or plane, or just out of a taxi, to advise me that they accidentally left one of the above devices behind on their seat. Not once was the device recovered.

Surreptitious surveillance is yet another risk. Large screens on laptops are easily viewed from a distance or by a nearby passenger, and confidential information is quickly betrayed. The consequences can vary based on what is seen.

Of course, the largest risk is from outright theft of your device. Here's a true story shared with me today by one of my peers in another state:

> *One of our attorneys was working on his laptop while riding on the light rail transportation in one of our cities yesterday evening. As the train was about to pull out from a stop, a quick thief ran by,*

*grabbed his laptop right out of his hands and darted off the train just as it pulled out. He filed a report with the police and train security. He's wondering what other measures he should take.*

One of the biggest risk areas is at an airport. In the post-9/11 world, heightened airport security has actually increased your risk, as there is a potential to become separated from your electronic gear, or at least lose sight of it, for longer periods of time. Thieves have been known to snatch and grab gear, particularly laptops, from the security belt before owners get through.

Sometimes thieves work in pairs. One loiters at the end of the security belt, while the other gets in front of you and purposely triggers the metal detector with coins, jewelry or other metal devices. As the conspirator in front of you very slowly unload pockets and gets rechecked, your laptop passes through xray and into the hands of the other conspirator, before you even get through the metal detector. Therefore, your first goal is to prevent that from happening as much as possible.

If you are traveling with a companion, have him or her pass through the metal detector first and wait at the end of the xray belt, while you send items through. If you are traveling alone, do not release your items into the xray unit until the person in front of you has cleared the metal detector.

Make your laptop bag as searchable as possible by xray or hand inspection in order to reduce any time your items are out of your sight. Use twist ties to keep cables in order, and zip top bags for any small gadgets and stray parts. For less familiar equipment like GPS devices, and compact cameras, keep the owners manual near to the device in a clear bag, in order to help security personnel quickly identify what he or she sees as a harmless consumer device. Have your devices charged and ready to run if asked, so that you don't have any delay created while you pull out and connect a charger, and search for an outlet.

It's not always possible, but try to maintain visual contact with your bag. And speaking of bags, consider one which doesn't look like a typical computer bag. The one I use is a bag designed for transporting large file folders, but it looks like a rolling overnight bag. I customized the inside myself using Velcro and a laptop bag I took apart. Not only does it actually provide better protection for my large laptop than a regular bag, but it holds

projector cables, tools, adapters of all sorts, extension cords, a power strip, and lots more. Yes it's heavy. On the other hand, whenever I arrive somewhere I'm prepared for anything, and no thieves would suspect there's a laptop in the bag based on appearance.

Other things which help foil thieves is a bag which is bright, personalized, and easy to identify in a crowded concourse. Even something as simple as an oversized fluorescent luggage tag firmly affixed can deter a thief.

If you want to do something to make your gear more recoverable, you need to make it virtually impossible to sell on the black market. That means having it permanently marked in some way. The unique bar-coded ID plates and permanent glue you get through www.stoptheft.com (only $25.50 each for quantities of less than 10), will enhance your chance of recovery. And there are all sorts of other security enhancements available. Take a look at http://tinyurl.com/m2tpv for more.

Even the best-laid plans can go awry. What else should you do? What other precautions should you take?

Use a password on every device which permits one. It's ok to pick one password that works for you and use it on all your devices, to make it easier to remember. Just don't also use it for your bank cards or as your credit card PIN.

A password which contains a combination of letters and numbers works best, and if you can add a special character like a dollar sign, ampersand, or asterisk, it will become virtually unbreakable. Try to think in terms of a phrase which is easy to recall. For example, if you pass 4 traffic lights on the way to work you may want to use "4stop*light" as a password. Happily married? Try "gr8marriage." Your screen saver on the laptop should have a password, too. That way if you step away from your computer, no one else can access it once the screen saver begins. But be sure never to walk away from your laptop or other valuable electronic gear in a public place, even if you have your eye on it from a distance. Or let me rephrase that – how fast can you run in pursuit? If you're not in shape for a long fast sprint, take your gear with you.

Consider purchasing a thumb-print reader security device for your laptop or buy one with it incorporated. Have your computer guru install a boot password on your laptop. This prevents it from being rebooted at all without your password. That means that a thief has to discard the hard drive and replace it with another in order to use or sell your laptop. That's ok, because at least your data is safe. That's the most important thing.

If you have a wide-screen, high definition, or large display, consider one of the monitor covers which makes it impossible to view the screen from an angle.

Of course, you definitely want to consider encrypting the sensitive documents on the laptop for an extra measure of security. Third party products can automate this process quite easily.

Laptop computers are frequently accessed by unauthorized users. That results when they are used in insecure locations such as conference rooms, temporary offices, and hotels, to name a few. In most cases, the laptop is used in a public area where the rightful laptop user is not well known to others. This situation makes it easy for an unauthorized user to view or use the laptop without looking suspicious.

If you are in such a situation and have to step away from your laptop, even if only for a few minutes – think bathroom break during a seminar – remember to lock it. First, I suggest you minimize all your applications using the efficient keystroke combination of Windows Logo Key + M. That way no one sees what was on the screen previously. (Note: to restore all the programs and documents to the same minimize or maximize status they were before, use the keystroke combination Windows Logo Key + Shift + M.) Then press CTRL + ALT + DELETE, and select *Lock Computer* from the menu. Your logon password will be required to unlock the computer, thereby preventing unauthorized access.

Another way laptop users can secure data is by being selective about what they store on the laptop. When working away from the office, use resources that the computer can link to via the Internet as the sources of confidential data. Intranets, extranets, and Web sites protected by private passwords are examples of such sources not located on a laptop's hard drive. If the laptop is lost or stolen, the client data will not be compromised. This is particularly true if you don't store the passwords to such resources on the

laptop itself, or if the passwords are well encrypted to prevent unauthorized access.

Another method is to "pack" what data you want on a secure keychain a/k/a flash-ROM drive with automatic encryption. Then store the device separately from the laptop, thereby leaving no sensitive data on the laptop at all. The keychain device is small enough to fit in a shirt pocket or on a keychain (hence the name) yet usually large enough to transport critical sensitive documents. Not enough? Consider a mini external USB hard drive. I just purchased one for only $120, which is smaller than the palm of my hand and holds 8 Gb of information.

What if your laptop or PDA is stolen and you haven't taken any special precautionary measures to secure the data, such as encryption, separate storage, boot passwords etc.? Well, the resulting conclusion will vary from state to state. In some states encryption and other security measures are considered a standard of care which the attorney must meet. In Pennsylvania it is not yet clear what security measures meet the standard. Certainly malpractice concerns are sufficient to suggest you do not want to be the deciding test case.

At a minimum, you should not only report the theft to the police and your business insurance carrier, but you should also put your malpractice insurance carrier on notice. Do you have a duty to notify clients if anything pertaining to their matter was on the stolen computer? That's a question which is best answered by the PBA Ethics Hot line. You can contact Louise Lamoreaux at 800-932-0311 x2214 or via email at Louise.Lamoreaux@pabar.org.

*A version of this article originally appeared in the 9/4/06 issue of the Pennsylvania Bar News.*