The Duty to Delete: Preventing Inadvertent Disclosure of Confidential Information Before Donating Technology

Joshua de Larios-Heiman practices civil litigation. His clients include individuals and businesses in the finance, technology, management consulting, insurance, entertainment and hospitality industries. He received his Juris Doctor from the University of San Francisco, School of Law in 2005, and an undergraduate degree in history from University of California, Berkeley in 1997.

Are you thinking of giving away that crappy old laptop to charity? Are you pumped about jettisoning that piece of junk that gives off high pitched squeals and smells of ozone when it is turned on?

Wait a minute! Have you ever given a computer away? Where did it go? What was on the hard drive? Who has it now? Consider two recent news stories:

- In 2006, a friend of Artist Nancy Koan happened upon a laptop discarded in a garbage area in a downtown New York apartment building. The friend gave the computer to Ms. Koan. Ms. Koan gave the computer to the New York Times. According to the Times, that computer contained confidential emails belonging to Goldman Sachs employee Fabrice Tourre. What followed was an exposé of Goldman Sachs' role in the mortgage crisis and an ongoing suit against Mr. Tourre by the United States Securities and Exchange Commission. http://www.nytimes.com/2011/06/01/business/01prosecute.html.
- As I write, London detectives are currently examining a computer, paperwork and a phone found in a bin near the riverside London home of the former chief executive of News International, Rebekah Brooks. http://www.guardian.co.uk/media/2011/jul/21/phone-hacking-charlie-brooks-computer

Access to an opposing party's unredacted data is the stuff of which plaintiff dreams are made. In fact, I recently prevailed in Kaiser arbitration largely due to the fact that Kaiser employees posted their true thoughts about my client in a messaging system Kaiser believed undiscoverable. I discovered the systems and moved for their production. The arbitrator determined the messages were indeed part of my client's medical record and ordered Kaiser to provide the data.

Conversely, access to un-redacted data by an opposing party is the stuff of which litigation nightmares are made. I can't even imagine what opposing counsel thought when they learned they had to produce Kaiser's secret messages.

Every attorney must comply with the laws and ethical rules related to data retention. A legal duty arises to preserve documents and data if they are relevant to a lawsuit that one reasonably anticipates will be filed in the future. *See, e.g., Federal Rules of Civil Procedure; Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (Zubulake IV); Shamis v. Ambassador Factors Corp., 34 F.Supp. 2d 879, 889 (S.D.N.Y. 1999).*

Just as a lawyer must properly preserve data, a lawyer must take reasonable precautions to ensure that their clients' confidential information remains secure. A recent article in the July/August 2010 issue of American Bar Association's *Law Practice Magazine* titled *"SAFEGUARDING CONFIDENTIAL DATA: Your Ethical and Legal Obligation"* addressed the ethical, common law and regulatory duties lawyers are under to safeguard client data. http://www.americanbar.org/publications/law_practice_home/law_practice_

archive/lpm_magazine_articles_v36_is4_pg49.html

As part of that duty to safeguard client data, a lawyer must take reasonable efforts to properly erase data before discarding hard-drives. Clearly, the duty to delete data may be overridden by a duty to preserve evidence. Assuming all data has been successfully and ethically backed-up and the duty to preserve evidence has been satisfied, how does an attorney go about disposing of a hard drive with sensitive information on it?

They go about it reasonably. Here, what does "reasonably" mean? According to the ABA article, the definition of "reasonable" with respect to safeguarding confidential data is "evolving."

In an attempt to determine what "reasonableness" might mean here, I contacted my person most knowledgeable on the subject: John Salomon. John is principal information security consultant at the international consultancy group, Chakraborty Software, GmbH.

Although he seriously denies the comparison, John resembles a real life James Bond. He speaks at least four languages. He consults for Europe's largest banks and pharmaceutical companies on data security matters. Most of his work he can't talk about without killing me. He splits his time between Zurich, Amsterdam and Paris. He graduated from U.C. Berkeley where he was a Computer Science Undergraduate Association board member. After graduation, he was a systems engineer for Perot Systems, and has an MBA from INSEAD. Since I can't afford his hourly rate, he agreed to answer my questions in exchange for a beer next time he is in San Francisco.

JdeLH: Is it okay to just give the computer to charity as is? If not, why?
JS: It's always okay to give things to charity, particularly some of the excellent organizations that refurbish old equipment and provide it to schools and the needy, thus avoiding toxic landfill clutter. But before you allow anything out of your control, ask yourself whether there is anything on that PC that you'd want plastered on a billboard on Main Street – because that's basically what you're doing. This includes:

- data stored on hard disk,
- removable media (CDs/DVDs) left in drives (it happens), and
- asset tags, post-it notes, etc. that could give clues as to its provenance or to sensitive data like passwords.

There are simple, proven ways to avoid this, which involve a combination of technology and proper processes.

Some charities provide services to wipe hard drives and other storage media upon receipt – but this is something you can and should do before a computer system leaves the building.

JdeLH: Is deleting the sensitive files sufficient to prevent access?
JS: It depends on what you understand by "deleting". First, it's important to note that this depends entirely on what operating system you use – MacOS, Windows, Linux, etc.

Without going into too much technical detail, in most computer systems, when you delete a file, you're not actually removing the contents as you would when burning a paper file – all you are doing is telling the operating system, "it's OK to overwrite this physical part of the disk." When writing new files the system will look for space that is not yet "taken" and then put new information there. Until that actually happens, it's still extremely easy for a professional or even a motivated amateur to recover what was previously there.

Even if you're lucky and the operating system has put a new file where the old one previously was, it's still possible to recover data using forensic software. Investigators frequently rely on data recovery firms to provide evidence that is admissible in court; both commercial software, such as Guidance Software's EnCase, and open source/free software, has a long history in court cases in many jurisdictions, often providing crucial evidence in both civil and criminal cases.

JdeLH: Is reformatting the hard drive sufficient to prevent access? If so how does one do it?
JS: No. Think of it like a street map. Removing files gets rid of labels that indicate individual streets, landmarks, etc. Formatting the hard disk removes the scale, street index, front page of the map (i.e. "THIS IS A MAP") and other such information. But the underlying image is still there. By looking at the blank, unlabeled map, I may not be able to tell Elm Street from Sunset Boulevard, but I can still easily see what's where, how big it is, which are residential or industrial areas, etc.

In some cases, formatting is even easier to undo than file deletion.

If you're technically minded, Wikipedia has a great article on the phenomenon of "data remanence" – http://en.wikipedia.org/wiki/Data_remanence – the fact that data signatures remain even when deleted, and even after dedicated wipe methods are used.

JdeLH: You scared the hell out of me. What do you recommend? Should I physically destroy the hard drive?
JS: There is no reason to be scared. You would remove your personal effects before selling a car, right? This is no different.

There are services that physically destroy storage media – usually via heavy-duty shredder. Some govern-

ment and military agencies swear by this. If you are really paranoid, you can unscrew the hard drive case, take out the magnetic platters, and go to town with a hammer. For our purposes, while this makes great entertainment over a few beers, it's a bit excessive and a waste of perfectly good hardware.

The only method, short of physical destruction, considered adequately secure by the US Department of Defense, is called "degaussing", where a very strong magnetic current is used to completely scramble and remove remaining information. But again, this is excessive for most purposes, plus you probably don't have access to an industrial grade electromagnet.

The National Institute for Standards and Technology (NIST) considers "scrambling", or multiple overwrites of files, to be sufficient.

Mac users have a utility called "secure empty trash" for users. The tool Disk Utility also includes a drive space secure erase. You should run this from the boot DVD.

Other systems you can use include File Shredder, Eraser, or Ccleaner – these are only a few of the numerous good tools in existence. To be really secure, you should always run these from an external boot disk – Darik's Boot and Nuke is an easy way to do this. A reasonable list of tools can be found here:

http://www.thefreecountry.com/security/securedelete.shtml

Some of these cost money, some are free – beware of downloading software from anything that looks like a link farm rather than a security site.

JdeLH: Is there any way of being absolutely sure the data is destroyed?
JS: Take off and nuke the site from orbit, it's the only way to be sure.
JdeLH: What reasonable efforts do you think must be taken to properly erase a drive? (Feel free to answer with "Jeez, I'm not an attorney I don't know" or "I don't know what the legal standard is, but I recommend...")
JS: How about "while I am not qualified to give legal advice, and would encourage anyone to make sure they're not breaking any laws (you can remove this if it's too bloody obvious). On a purely technological level I think it's not too much to expect anyone discarding a storage device or computer system previously used for sensitive data processing to take at least some basic steps. No matter how little computer-oriented you are, something like running a secure erase program is pretty basic, and step-by-step instructions are out there in spades". As for "reasonable"...um, er, um, yeah. I hate that word. Most people aren't :)
JdeLH: Lawyers love checklists. Can you provide me a checklist to follow

before I give away a computer?

JS: Sure. I'll give you three. The first checklist is a set of questions to answer before giving away a computer. The second and third are rules of thumb checklists for destroying data both for during regular usage and when actually getting rid of the computer.

Checklist Before Giving Away A Computer

1. Has the data been backed-up?
2. Are you sure you want to destroy the data?
3. Would destroying the data comply with the laws and ethical rules surrounding data retention?
4. Have you taken reasonable efforts to delete the data against unintended disclosure?
    a. Do nothing (inadvisable)
    b. Delete Files (inadvisable as deleting not enough)
    c. Reformatting Hard Drive (generally advisable but not as secure as writing over hard drive)
    d. Writing over the hard drive using software (advisable)
    e. Physically destroying the hard drive (advisable, if data is of sufficient security)

General Rules Of Thumb Checklists For Destroying Data

1. DURING DATA USE
    a. Use encryption tools, such as FileVault (included with MacOS), TrueCrypt (Mac/Windows, free) or PGPDisk (Mac/Windows, commercial), or BitLocker (Windows Vista/7 Enterprise and Ultimate editions). It's good policy, and protects you from loss or theft anyway.
    b. Regularly wipe free space, use secure delete tools for data you no longer need, keep track of where you store your files. Together, these steps will also make it easier to more securely delete data when you get rid of the PC.
2. WHEN GIVING AWAY A PC
    a. Remove all external storage media (CD/DVD, floppy, USB keys)
    b. Clear the laptop of all asset tags (not manufacturer serial numbers, as you'll make someone's life miserable later), post-it notes, or any stickers your company or users might have added
    c. Shut down the system, physically power it off, unplug it, and remove the battery (laptops).
    d. (for non-Macs:) start the system, enter the BIOS (usually by pressing a key on startup, look for a message at start) and find the option to reset BIOS settings to factory default
    e. Boot the system with your install DVD (Mac) or one of the above tools (Windows) and perform a secure deletion of anything.
    f. Bask in the knowledge that you've just donated a squeaky clean system to a good cause.