IN BRIEF

April 2017

Issue 131

OSB Professional Liability Fund

www.osbplf.org

Malpractice Prevention Education for Oregon Lawyers

Unwanted Data: How to Properly Destroy Data in Hardware

If you have old computers and other office equipment in your law office or home, there is a good reason they are still with you and not in the dumpster. This article will discuss why you should be concerned about the data in your devices and the proper way to dispose of them.

Why It Matters

Oregon Rule of Professional Conduct 1.6(c) requires lawyers to take reasonable steps to prevent the inadvertent disclosure of or unauthorized access to client information. To comply with this rule, you need to make sure client data stored in your computer and other media aren't compromised when you get rid of the devices. This requires you to ensure that data stored on these devices cannot be reconstituted after they leave your control. It's necessary that you permanently wipe data from the devices before donating or recycling them. Disposing of office equipment or devices without first permanently deleting data is an ethical and malpractice risk.

Deleting Files Is Not Enough

When you delete files on your computer and then empty the recycle bin, that operation does not permanently erase the files. Although you can no longer see the files, they are still in the operating system. The files aren't completely gone until you override the space with something else. Even reformatting or partitioning the hard drive will not permanently delete data. That task only erases the location of the data but not the data itself. You need to do more. Unless data on your computer is permanently deleted, it is recoverable using a low-level disk editor or a recovery tool.

Options for Permanent Data Erasure

You have two ways to completely destroy data: (1) use specialized software to overwrite the data or (2) physically destroy the hard drive.

Using Data Sanitization Software

Specialized software tools permanently delete files from your computer by overwriting the information with random data. When this "data sanitization" method is used, overwritten data can never be un-deleted with a file recovery tool. Software programs that permanently delete selected files are called file shredder programs. Software programs that completely erase the entire hard drive, not just selected files, are called data destruction programs. Both programs use different data sanitization methods (such as Secure Erase, DoD 5220.22-M, Gutmann, Random Data) to overwrite data. Some software programs overwrite deleted data only once; others overwrite three, seven, or more times. The more overwrite passes a program makes, the longer the sanitization process will take.

Whether you should use a file shredder program or a data destruction program depends on your needs. If you are planning to recycle, refurbish, or donate your computer, then use a data destruction program to completely wipe the hard drive. If you are still using your computer but want to permanently delete unwanted files, then a file shredder program is appropriate.

Below is a list of sample file shredder and data destruction programs for Windows.

DISCLAIMER

This material is provided for informational purposes only and does not establish, report, or create the standard of care for attorneys in Oregon, nor does it represent a complete analysis of the topics presented. Readers should conduct their own appropriate legal research. The information presented does not represent legal advice. This information may not be republished, sold, or used in any other form without the written consent of the Oregon State Bar Professional Liability Fund except that permission is granted for Oregon lawyers to use and modify these materials in their own practices. © 2017 OSB Professional Liability Fund.

File Shredder Programs

- **zDelete** (**www.zdelete.com**) – Has free and paid versions. The paid version offers more features for $29.00 per license. When you download the program and install it on your computer, a ZDelete Bin will appear on your desktop and replace the Windows Recycle Bin. You simply drag and drop files in the ZDelete Bin, and that document will be completely deleted. User instructions are available at: **http://www.zdelete.com/downloads/ZDelete-User-Guide-11-25-2016.pdf.**

- **Eraser** (**https://eraser.heidi.ie**) – Freeware. Once the software is downloaded and installed on your computer, an Eraser icon will be automatically added to the Windows contextual menus. Just right-click on the file, select the "Eraser" option, and then click on "Erase." You can also schedule an erasing task to wipe out data on a recurring basis. The default data sanitization method that Eraser uses is Gutmann-35-passes, so it overwrites the deleted data 35 times. This means if you have many files to delete, it might take a while.

- **Freeraser** (**www.freeraser.com**) – Freeware. Once downloaded and installed, a Freeraser trash bin icon will appear on the desktop. Drag and drop files into the folder to permanently delete them.

- **Other free programs:** Securely File Shredder, File Shredder, Secure Eraser, WipeFile.

Data Destruction Programs

- **DBAN (Darik's Boot and Nuke)** (**https://dban.org**) – Freeware. Erases hard disk drives (HDDs) in PC laptops, desktops, or servers. Download the program to a CD or flash drive, then boot from it. Follow the instructions on DBAN's menu interface. The paid version, Blancco Drive Eraser, complies with the Department of Defense data sanitization guidelines, provides a certificate of data removal, and offers more options, including data erasure for solid state drives (SSDs).

- **HDDErase** (**http://cmrr.ucsd.edu/people/Hughes/secure-erase.html**) – Freeware. You can use HDDErase in two ways after you download the program to your computer. The first is to burn the .iso file to a CD and boot from it to erase your hard drive. The download folder includes a HDDEraseReadMe file that has instructions on how to create the boot disk. The second is to install the .exe file in Windows and use it to securely erase data from different devices, such as a USB drive, another internal hard drive, or an external hard drive.

- **CBL Data Shredder** (**www.cbldatarecovery.com/data-shredder**) – Freeware. You can burn CBL Data Shredder directly to a CD and boot from it to erase the hard drive. You can also install the program in Windows like a regular program and run it to delete other devices, such as flash drives or another internal hard drive.

- **Other data destruction programs:** KillDisk, MHDD, Format Command with Write Zero Option.

For Mac OS

The Macintosh has built-in secure data sanitization features that permanently delete selected files or wipe the entire hard drive. Secured Empty Trash, available in the Finder menu, deletes selected files and overwrites them with a single pass of zeroes. The hard drive can be wiped out using the "Secured Erase Options" in Disk Utility. There are different security options for erasure depending on the version of Mac OS you are using. Always select the most secure option.

Physically Destroying the Hard Drive

You can also permanently destroy your hard drive by brute force. You would need to open the computer to locate the hard drive, then locate and access the disk platter inside the hard drive. It is the platter (the device that stores most of the data on your computer) that you need to physically destroy. Take the drive outside and use a hammer to smash it to pieces. You could also drill a few holes in the platter just to be safe. Once the drive is physically obliterated, take the parts to any place that recycles electronics.

Alternatively, take your computer to an electronic recycling facility to physically destroy the hard drive. Some vendors allow you to witness the onsite destruction. Two vendors in the Portland Metro area provide this service:

- **SBK Green Century Electronic Recycle**
  http://www.greencenturyonline.net/destruction.html
  2950 NW 29th Ave., Portland, OR 97219, 503.764.9963
- **R.S. Davis Recycling**
  http://portlandrecycling.com/electronics-recycling
  10105 SE Mather Road, Clackamas, OR 97015
  503.655.5433

Data in Your Office Equipment

In addition to computers, lawyers also use copiers, scanners, printers, and fax machines in their law practices. It is unlikely that your personal scanner or printer has a hard drive inside. But many multi-functional printers retain an image of the printed, scanned, or copied document and store them in the hard drive.

If you are leasing office equipment, ask the leasing company if the machine has a hard drive and what happens to the data stored on that drive. Also ask whether the machine has a wipe-disk function that can be used to erase data when decommissioning the machine. Review the contract to verify whether and how data are destroyed once the machine is returned to the leasing company.

If you want to get rid of your own office equipment, it's a good idea to open the machine and search for anything that looks like a disk. If there is a disk, remove it from the machine and smash it into pieces with a hammer. Recycle the pieces appropriately.

Data in Cloud Storage and Mobile Devices

Let's not forget data you store in the cloud, your smartphones, and on tablets. Similar to a computer, the cloud server doesn't erase files from its system when you right-click to delete them. These files are merely hidden from you but are still somewhere in the cloud server. Major cloud storage providers like Google Drive, OneDrive, and DropBox have options that purport to permanently delete files from their servers. Some providers will automatically purge deleted files after a certain period of time. It's hard to know whether their "Permanently Delete" (DropBox) or "Delete Forever" (Google) options truly expunge the files from their servers. Make sure you review the provider's user agreement or privacy policy to understand what happens to the files you "delete" or "permanently delete."

As for mobile devices, Apple and Android both have factory reset and remote-wipe functions that erase the devices. Before selling, donating, or recycling your device, make sure you erase all contents and settings. Use the remote-wipe option if the device is lost or stolen.

Conclusion

Protecting client information requires that you securely destroy data stored in old computers and office equipment. You could do this by using software to wipe the hard drive, physically destroying the hard drive, or taking it to a professional to do an onsite destruction for you. Choose a method that is most convenient for you.

Hong Dao
PLF Practice Management Advisor