The New York Times
nytimes.com

November 3, 2005
Basics

Deleted but Not Gone

By THOMAS J. FITZGERALD

Maintaining privacy in the era of digital information requires work on a number of fronts, whether fending off spyware, protecting important files with encryption or configuring a Wi-Fi hot spot to keep interlopers off a wireless network.

One basic privacy measure, however, is easily overlooked: proper data destruction.

Deleting confidential data completely is essential when donating or selling old computers, and it can also help maintain privacy on computers that may end up lost or stolen. And for businesses looking for ways to comply with the security requirements of laws like the Sarbanes-Oxley Act, a sound policy on data control and destruction is crucial.

When normal deletion methods like the Recycle Bin or the delete command are used, the computer's operating system, for the sake of speed, creates an illusion that data has been deleted. In fact, it merely earmarks that region of a disk or drive as being available for new data to overwrite the old data. Until that overwriting occurs, the old data can be retrieved with undelete programs and tools used by data recovery labs and law enforcement agencies.

There are, however, several options for securely eliminating data from hard disks, U.S.B. flash drives and other storage media. These programs overwrite data with meaningless characters to render it unrecoverable with today's data recovery techniques. Some of the programs can overwrite entire drives, while others can single out individual files or other information saved by a computer's operating system or programs like Web browsers. Shredding machines that can destroy diskettes, CD's and DVD's are also available.

Several programs are available to overwrite entire hard disks. These programs wipe away everything, including programs, documents and the computer's operating system, so users need to be sure to have backup copies of important data and software before using them.

For example, Darik's Boot and Nuke, known also as DBAN, is a free open-source program available at dban.sourceforge.net. It runs on Windows computers and offers six methods to overwrite data, including a Defense Department standard (DoD 5220.22-M) that can overwrite the disk three times, as well as a method called PRNG Stream Wipe, which can make a user-defined number of disk overwrites using randomly generated characters.

The program, available in two formats, can be burned to a CD or copied to a diskette. After a computer is started with either type of disk inserted, DBAN's menu will load. (The computer's boot device order, located in the BIOS, may need to be adjusted to load disk-wiping programs, which run their own operating systems.)

DBAN has won users partly because it is free, but also because of its open-source format. According to its author, Darik Horn, the program's coding can be scrutinized by anyone, which can help assure reliability. "In the current marketplace there's a huge push for reviewability, for openness," Mr. Horn said. "People want to trust their products."

Mr. Horn said a single overwrite should be enough to render data unrecoverable, but he recommends at least four overwrites to guard against possible future advancements in data recovery techniques and other unknowns.

Another program for wiping entire disks on Windows computers is WipeDrive from WhiteCanyon ($39.95 at www.whitecanyon.com). It offers 12 overwriting methods, including the Defense Department standard with three overwrites, although the company's president and chief executive, Steve Elderkin, said methods that use a single pass are almost always enough to render data unrecoverable.

"If you overwrite it once, it's gone," Mr. Elderkin said. But doing more than one overwrite is probably a good idea for disks more than five years old and also for smaller drives, as well as for peace of mind, he said.

WipeDrive has been available since 1996, Mr. Elderkin said. A single pass takes three to five minutes for each gigabyte of disk space, depending on factors like a disk's speed. The program can examine all sectors of a disk to verify whether overwriting was successful.

WhiteCanyon also offers MediaWiper ($39.95), a program that can overwrite data on removable storage devices like U.S.B. flash drives, memory cards, diskettes, Zip drives and external hard drives connected to U.S.B. and FireWire ports. It offers four overwriting methods, including an option with 12 passes. It also has a verification feature that can examine all sectors of a drive.

Macintosh computers come with a tool to erase entire disks and attached drives. The feature, called Disk Utility, is included in the Utilities folder, and also on the system installation DVD or CD.

In Mac OS X 10.4, or Tiger, the program offers three overwrite choices: once with all zeros, a Defense Department standard with seven overwrites, and the Gutmann standard, which has 35 passes. (To gain access to these features, select a drive, then click Erase, and then select Security Options.) The installed application can overwrite attached drives. To overwrite the computer's hard disk, start the computer with the installation DVD inserted and press the C key to enter Disk Utility.

To delete individual files there are programs, often called file shredders, which also use overwriting to render data unrecoverable.

For example, Window Washer from Webroot Software ($29.95 at www.webroot.com) includes a feature called bleaching that offers several overwriting methods, including a National Security Agency standard of seven overwrites, and the Gutmann standard of 35 overwrites.

With bleaching enabled, Window Washer can securely delete individual files, folders and contents of the Recycle Bin. It can also overwrite free space on drives, which may contain old data from files deleted using routine methods. It can seek out information left behind by Web browsers, including browsing histories, cookies and cached images. And it can securely delete files saved in Windows temporary folders.

Another file-shredding program, called ShredIt, is available in versions for both Windows and Macintosh computers from Mireth Technology ($19.95 for downloaded versions at www.mireth.com). The program's overwrite methods include user-defined options with up to 35 passes. Another useful feature, in the Macintosh version, is the option to overwrite rewritable CD's.

Other options for deleting files securely are included in Acronis Privacy Expert Suite from Acronis ($29.99 for a one-year subscription at www.acronis.com), and PGP Desktop Home ($99 at www.pgp.com) from the PGP Corporation.

For Mac users, the Mac OS X operating system (version 10.3 and up) has a tool called Secure Empty Trash that deletes individual files in the trash using the Defense Department standard with seven overwrites. To use it, choose Secure Empty Trash in the Mac Finder menu.

And finally, there may be instances when physical destruction of digitally stored data is required or more convenient. Several shredders are available, including the Royal MD100 Media Destroyer ($89.95 at www.royalsupplies.com), which can break CD's, DVD's and diskettes into tiny fragments and can fit on a desk. The Powershred PS-70 from Fellowes ($179.99 at www.officedepot.com) shreds CD's and DVD's, accepts 14 sheets of paper at once, and can shred credit cards, staples and small paper clips.

And of course, one way to ensure that data on a hard disk will never be recovered is to destroy the disk. You can do that by removing the disk's platters and grinding them to bits - an extreme option, but effective.