



William J. Kovatch, Jr.
Attorney at Law, PLC



Protecting Proprietary Information
This Month: Flash Drive

Flash drives: they are amazing little devices, aren't they? I sometimes joke that I carry my entire life around on my flash drive. They make life so convenient. If I get struck with inspiration at night after my wife and I have put the kids to bed, I can just pop my flash drive in my home computer, and bring my files with me to the office the next day. If I'm on the road, I can use my flash drive with my laptop and work on the same files I would have in my office. On Sunday, if I need to print-out hand-outs for my Sunday School students, I can just pop my flash drive into the church computer, and there they are. In fact, while I originally bought a flash drive with 4 gigabytes of memory, I recently upgraded to 8 gigs when I saw a half price sale.

So what's the problem? After all, doesn't the Department of Commerce recommend the use of removable media to store electronic documents with proprietary information? Isn't this a better arrangement than storing such documents on a computer's hard drive or a law firm's network?

The problem is that flash drives may be too convenient. They are so small, they fit nicely in a front pocket. It's easy to lose track of a flash drive in among your keys. I can't tell you how many mornings I've gone crazy because I neglected to put my flash drive in its normal spot. Now imagine if I stored proprietary information on my flash drive (which I don't), and lost track of that tiny thing. For antidumping and countervailing duty attorneys, that would be an APO violation.

Additionally, tiny flash drives are hard to detect. You may have a system in your law firm where all removable media are carefully logged, tracked and stored in a secure location. Then along comes some young hot-shot who doesn't like working with these restrictions. So, he brings in his own flash drive, saves the files he's been working on, and brings his flash drive home. Now your firm has lost control of the proprietary information on that flash drive.

Flash drives can also be a tool for nefarious activities. Several flash drives come equipped with software meant to hide the user's activities from the network. Some of these programs allow a user to "surf the 'net " without leaving a trace of the websites that were visited on the host computer system. Add to the fact that flash drives are easy to hide, it's easy for someone with malicious intent to sneak in a flash drive, download sensitive files, and use the Internet to disclose those files in an untraceable fashion.

What is a diligent firm to do? First, a law firm must have clear rules for electronic documents that contain proprietary information. Through those rules, the law firm should be able to track who has had access to proprietary information, if copies, including electronic copies, have been made, and where those copies are. Storing proprietary data on removable media, such as CD-ROMs, may still be preferable to storing data on a computer's hard drive or a computer network. But, such media should be catalogued and tracked.

What about flash drives? After all, they are removable media. And even though flash drives are easy to lose, the data can be encrypted. Isn't that sufficient?

The use of encryption software has its own trade-offs. For example, such software has the tendency to slow down data transmission on a flash drive. Encryption software, therefore, could meet with some resistance from users attracted to the flash drive because of its convenience.

In the end, it is a question of how comfortable the law firm is with using, or permitting the use of, a small device that is easily lost to store proprietary data. It is also a question of how confident the law firm is with its encryption technology and with the willingness of its employees to follow the rules.

Once the rules are in place, the rules and reasons behind the rules must be communicated clearly to everyone who works with proprietary information. A reasonable system should include regular training and re-training of the law firm's employees.

With proper management, flash drives and other types of technological innovations can still help to make us more efficient. But, proper management involves an understanding of the risks, and the need to develop procedures to mitigate those risks.

William J. Kovatch, Jr. served for four years as the APO Coordinating Attorney in the Office of Chief Counsel for Import Administration. He is available to train legal staff on the Department of Commerce's APO system, and the protection of proprietary information.