



Employees' Personal Storage Devices Create Data Security Risks

BY DAVID NOLTE

Employees have a variety of inexpensive digital storage devices available to them that, when used at work, pose significant data security issues. An employer's data have never been less secure and harder to control. Legal professionals must be aware of these issues in order to properly advise their clients and to handle data appropriately within their firms.

MP3 players (including Apple iPods), digital cameras, mobile phones with memory cards and flash drives can be connected to an employer's computer system, usually through a USB (universal serial bus) or firewire connection. Storage sizes of one gigabyte (GB) are common for digital cameras and flash drives. MP3 players have considerably greater storage. To put this in context, the average word processing file is around three pages long, with a size of between 25 and 35

kilobytes (KB). That means a 20 GB iPod could hold approximately 700,000 documents. Experts predict flash drives holding 10 GB of data and 1-inch hard disk drives holding 60 GB are coming soon.

THEFT OF PROPRIETARY INFORMATION

The threat of information theft has existed since the earliest floppy disk drives, although then, the amount of data that could be removed was much less. CDs and DVDs increased the concern because of their ability to store much greater volumes. Still, carrying around a stack of CDs is more conspicuous than carrying an iPod, and an iPod has much more storage capacity.

When someone initially learns that anyone can walk into the office and take a USB flash drive, iPod or other personal gadget from his pocket, grab ample amounts

of data and then leave without being detected, the first response is usually a desire to lock down computers to prevent this.

It's not that easy. USB connections are used for keyboards, mice, printers, scanners and other necessary devices. In addition, the flash drives (also called thumb drives and keychain drives) are exceptionally handy and enhance worker productivity when files need to be easily moved and shared. Of course, this same ease makes the devices (and the data on them) so difficult to control. Although software is available to prevent using a USB port for recording purposes, this increases network administration complexity and eliminates the advantages of this technology.

EMPLOYEE RIGHTS

Preventing employees from bringing these devices into the workplace is difficult. Their small size allows them to be easily carried to the office in a pocket or handbag. Short of instituting an unfriendly policy of not allowing employees to use their own electronics, combined with an invasive search program to enforce the policy, it is virtually impossible to keep these devices out of the workplace. Even if the employer was willing to alienate its workforce, privacy and human rights laws might prevent implementation of an effective program to eliminate these devices. For example, forbidding employees from using their MP3 players during lunch and other breaks is of questionable legality and is difficult to police and enforce.

Employers must consider whether the benefits from these devices outweigh the risks. There are no easy answers, but most employers who explicitly address the issue (instead of letting events occur out of ignorance or inaction) usually do so with non-technology solutions. If management chooses to allow the employees the convenience of using these devices at the office, clear guidance should be provided regarding expectations and the consequences for misuse. Generally, the solution for these risks is not more technology, but thoughtful policies and procedures.

OTHER EMPLOYER RISKS

These portable devices can also be used for uploading data, thus raising the real concern that these often unprotected devices carry a virus, worm or other malicious program.

Because these devices are so small and portable, they are also more easily lost or stolen, thus raising the

issue of whether important consumer or trade secret data have been compromised. A recent survey indicated that about 80 percent of users who transfer data to mobile devices use no encryption to protect the electronic contents. If consumer data are recorded on such devices, the practice is likely illegal and could cause serious legal exposures.



ELECTRONIC DISCOVERY RAMIFICATIONS

Once company data are copied to your employee's personal media, the firm's normal storage mechanisms and controls are no longer enforced. As described above, this causes risks for malicious software and security, but such data also avoid normal rotation of media that appropriately eliminates unwanted and unneeded copies of old and superseded data. Nevertheless, such data still belong to the employer, and the employee is still within the employer's control. Consequently, a properly drafted subpoena can reach these "rogue" storage devices.

The lessons are obvious. Parties seeking production of electronic information should draft their requests to include data maintained on employees' personal mobile storage devices. Similarly, employers' policies on document retention should address the need to eliminate these extra copies after their immediate approved use is complete. ✱

about the author

David Nolte is a founder and principal of Fulcrum Financial Inquiry LLP, a Los Angeles, California-based consulting firm that helps lawyers with electronic discovery. For more information about Fulcrum, visit www.fulcruminquiry.com. Contact the author at dnolte@fulcruminquiry.com.