



August 17, 2008

ON COMPANY EQUIPMENT, DON'T EXPECT PRIVACY

BY MILDRED L. CULP

This article has appeared in print in the *Dallas Morning News* (August 17, 2008) and the *Hartford Courant* (August 18, 2008).

Most people are getting very comfortable with technology. Nontypers have evolved into typers. Nonwriters have learned to get by. People who were once not inclined to make telephone calls now make them without blinking. Using technology, though, may put them at risk either on or off the job site.

Hope Haslam is director of Consulting Services at Epiq Systems Inc., based in Kansas City, Kan. She works in the New York City-based eDiscovery Group, which advises corporate and legal clients about large volumes of stored electronic data that might become part of a lawsuit, if it hasn't already.

"We identify relevant data," she says, which suggests that "the trend to mix work and life might well be colliding on technology, at work and at home or on the road. If someone is on a PDA or laptop or personal machines at home, we can advise the corporation to go out and collect that data. This can be frightening to employees, because there could be some very personal information there."

Ms. Haslam, who lives in Dallas, says that in Texas, pornographic material gets reported, even though it's totally unrelated to work. Of course, if you reveal any ailments or other information you didn't want the world to know, it's too late. You've already left a digital footprint.

Let's say you own a cellphone, and your company reimburses you every so often for calls. Whose phone is it? "All of this is getting very sticky," she says. Employers will have some rights to it. Her solution is to tote two telephones, everywhere.

In *Blown to Bits: Your Life, Liberty and Happiness After the Digital Explosion*, authors Hal Abelson, Ken Ledeen and Harry Lewis say that employers aren't out to straitjacket employees, that "they have to be able to investigate wrongdoing for which the employer would be liable."

IBM Internet Security Systems' Peter Evans of Atlanta molds strategy to evolving security threats. As vice president of marketing, he says hackers and generational trends are putting some workers and their companies at risk. Because Gen X and Gen Y are accustomed to collaborating online – and not necessarily through e-mail – they might not be aware of the risk their practices take on when they move to "highly regulated environments."

Financial services is one such industry. "The organization needs to protect data and credit card information," he says. "An employee might put information out there that would be excellent for a hacker. Filters are watching for data leaking."

Hackers are like retailers, Mr. Evans says. They watch people at work and use what they see "to take control of a laptop." This means that you can be very vulnerable, becoming "the weak link that could put a business at risk."

Says Ms. Haslam, "Employees need to understand their corporate policies about the use of PDAs provided by the company."

She suggests employees go to human resources together to get policies or updates.

It's best to communicate in writing, she says, or, if you use a telephone, send an e-mail about the conversation.

Mr. Evans suggests several resources to help you deal with these issues, including the ePolicy Institute, Security Smart Newsletter, and, more in depth, the *X-Force Threat Insight Monthly*, published by his organization. They'll help you navigate around your responsibility with today's technology.

Mildred L. Culp is a syndicated columnist who covers emerging trends in the workplace.

Reprinted with permission of Passage Media.

WorkWise is a registered trademark of Executive Directions International, Inc.