

CAREER OPPORTUNITIES

Privacy and You

By Douglas E. Welch

These days, privacy seems as quaint a concept as a horse and buggy. Everywhere we go, everything we do—especially online—is being tracked by someone. While the data can be useful for online retailers, most of this information is simply a free-floating opportunity to snoop. Even worse, high-tech careerists are the makers of this privacy invasion. We create the tools that allow these invasions of privacy, and we are often the ones to suffer the most. Maybe the time has come to reduce the amount of data we collect so that everyone can benefit from some slim slice of online privacy.

We Love Data

As a high-tech worker, you live for data. Most of the systems you create are developed specifically to collect, sort and store data. Even more, you gather data about the operations of your systems. High-tech folks love log files. We want to know exactly what is happening where and when. These files are like the EKG of a system. They allow you to track its progress, solve its errors and improve its operation. Unfortunately, this love for log files has had unforeseen consequences.

Every single Web server, FTP server and other systems out there collect a staggering amount of data each day. Every single access is logged and later processed into statistical programs. When you start to combine this information, you can create an audit trail that rivals that of a corporate accounting system. You can develop reports that show who went where, for how long, looking at what. I would argue that such tracking is overkill for your average high-tech worker. Unfortunately, marketing and sales departments quickly latched onto this data as a way to increase revenues. The genie was out of the bottle, and we may never find a way to put the cork back in.

Turn Off the Spigot

Despite this love for data, high-tech workers need to

reconsider the effect that their data-gathering has on everyday life. With the FBI and other law enforcement agencies sifting through log files, library records and more, maybe we owe it to ourselves and those around us to collect a little less data, and throw away data once reports have been created.

As a Web site owner, I like to know how many visitors are viewing my site. It allows me to alter site design and content to serve the largest group of people. That said, do I really need to know that John Doe from Albuquerque read my August 2 Career Op column from his UUNET connection on a Mac running OS X? I think not. Would I like to know that someone came in from New Mexico and viewed a particular file on a particular day? Sure. The difference lies in the specificity of the data.

Raw log files contain too much information to keep them around. They invite abuse by others who would use this information to harass people, whether for criminal means or simply to sell them something. I am making a proposition that once raw data has been developed into a report, the raw data should be destroyed. Nothing good can come of the continued aggregation of raw data. It can easily be used to diminish what little privacy we have left.

Better still, I would call on all sysadmins to question just what data is being gathered on their users, and prioritize the need for this data. Could you stop gathering cookie information? Could you remove IP addresses from your log files? What data do you really need to do your job? What information are you gathering simply because you can? Each time you gather data—whether customer orders, account requests or log files—consider closely how this data might be used by others. Often, these uses can be far outside those originally intended.

There is a need today to maintain the smallest shred of privacy allowed to us. The headlong rush into online marketing has left many people wondering what privacy remains, if any. As high-tech careerists, you hold the power to allow or prevent further incursions into the day-to-day privacy of thousands of people. Consider your actions closely. The privacy you are diminishing is also your own. □