



The Privacy Arms Race

Fancy new software lets managers spy on employees -- and employees evade the scrutiny. Um . . . trust, anyone?

From: Issue 84 July 2004, Page 28

By: Lucas Conley

URL: http://www.fastcompany.com/magazine/84/open_essay.html

In the 1830s, workers at New England's textile mills lived in company houses, worked in company factories, and worshipped at the company church. Attendance was mandatory. Milton Hershey and Henry Ford are both famous for having hired detectives to keep an eye on their employees outside of work. Ford even created his own sociological department, staffed by 50 inspectors who kept tabs on autoworkers' behavior off the job. Misbehave, and your wallet got a little lighter come payday.

So why are we surprised when, generations later, employers do their darnedest to invade our privacy? This is as it has always been: Bosses, more or less in the name of productivity, pursue as much information as possible about their workers, and employees try to dodge the prying eye. It's an unending, escalating arms race between the control freaks and the goof-offs.

Today, the war has gone high-tech. Office drones are likely to have their Internet travels, emails, and instant messages monitored, and perhaps their every keystroke logged. Global-positioning systems track long-haul truckers' speed violations, unnecessary pit stops, and circuitous routes. Car salesmen are fitted with RFID tags to keep tabs on their test drives.

Well, bravo for technology -- and for those industrious bosses! They are, after all, just playing by the rules. The problem is that the rules haven't kept up with the means. The last significant update to workplace privacy law was passed by Congress in 1986. Since then, wireless communication, email, and the Internet have moved the privacy war into the legal no-man's-land of the digital world.

Which leaves us confronting, slack-jawed, such innovators as Stellar Internet Monitoring LLC. Stellar, a startup in Naples, Florida, sells a Web-based application that tracks employee Internet use to the tenth of a second. Bosses can log on anywhere, via the Internet, pull up graphs detailing the time you dedicated to eTrade and MulletsGalore.com -- and calculate the cost of those minutes in wasted pay.

Such a service, it seems, is not a tough sell. "We're not doing any calling," says president Don Innis. "People are calling us." Toby Dutter, vice president of Indianhead Insurance Agency Inc., in Wisconsin, called Stellar after his IT consultant told him it might be a smart move. He found that 25% of his 40 employees were abusing policies, particularly with instant messaging. "I'd always read about wasted time," he says. "Didn't think we had it because we're so busy. Found out [I was] wrong. We don't have a problem anymore."

Gulp. In 1997, 15% of large U.S. companies monitored employees' email, according to the American Management Association. Today, it's 52% -- and much higher than that in the technology sector. In part, the surge is a reaction to heightened regulatory scrutiny in the post-Enron era. The in-the-know employer just wants to make sure he's staying out of Eliot Spitzer's way.

But the upshot, says Lewis Maltby, is that "if privacy in America were an animal, it would be on the endangered-species list." Maltby is president of the National Workrights Institute, a spin-off of the American Civil Liberties Union. He has watched two federal bills advocating improved rights for U.S. employees bite the dust, one in 1994 and another in 2000. The more recent, the Notice of Electronic Monitoring Act (NEMA), would have obliged companies to tell employees if and how they were being tracked. Today, only half of employers who monitor let their workers in on the secret during training. Small wonder, then, that the ACLU receives more complaints about workplace-rights violations than any other issue.

In the absence of better rules, there are two ways to think about this situation. The first relies on the shared assumption that companies and workers are basically evil -- and so escalates the battle ever upward. That's the implicit theory behind products such as StealthSurfer, a \$99 USB plug-in from Stealth Ideas Inc., which acts as a removable drive that stores any cached sites, bookmarks, browser histories, or files. In the next year or so, Stealth Ideas plans to launch enhancements allowing users to cloak

their activity from workplace-monitoring software like Stellar's.

Alternatively, we could figure out how to trust each other. Sandy Hughes leads Procter & Gamble's global privacy council, in charge of setting guidelines for 98,000 employees in 80 countries. Hughes could hold every P&Ger to the letter of the law in their respective nations. But that would be insanely hard -- much more so than, say, treating employees like grown-ups.

So while P&G does monitor online activity of operating units to gauge trends, it doesn't track individual movements. "At some level," says Hughes, "you have to trust your employees are going to be doing the right things. It gets down to being a business-driven, principle-based program, rather than legally based."

Could it work? Could reasonable boundaries and a modicum of respect for individual rights prove more effective than tech-enabled micromanagement? Invading privacy won't inspire much in the way of morale, much less productivity. And if your workers aren't motivated to do their jobs well anyway, another layer of surveillance isn't the answer.



Copyright © 2004 Gruner + Jahr USA Publishing. All rights reserved.
Fast Company, 375 Lexington Avenue., New York , NY 10017