

## Over Your Shoulder: Why Your Employer is Entitled to Watch You

*Ben Malisow* 2001-05-23

### Over Your Shoulder: Why Your Employer is Entitled to Watch You

by *Ben Malisow*

last updated May 23, 2001

---

One of the reasons the Internet continually been a subject of lively debate is the crackdown of employers on the use of web-surfing and e-mail applications in the workplace. This has caused no little travail for civil libertarians and privacy mavens who strongly believe that too much intrusion on the freedoms of a democratic society necessarily detracts from the benefits of living in such a culture. Their rationale is rather simple and straightforward: American taxpayers paid for the development and construction of the information superhighway, supports the market environment where such it (along with the many companies that profit from it) can flourish, and continues to pay for the privilege of utilizing it, they should therefore be entitled to flit about on it whenever and however they please, without pesky state troopers and private rent-a-cops abrogating that right.

Opponents of this perspective might object, using a tired analogy, to ask whether workers should be allowed to go for a spin to the local porn shop in the company car?

#### **The Why of It**

Employers have reasons to justify the supervision of employees (other than the fact that they happen to foot the bill, so they can). When decrying the inhumanity of transgressing on personal privacy, it's perhaps best to understand the rationale for such activity. Strangely, the initial and primary fear of the Internet held by most employers, that unrestrained access to the outside world would negatively impact actual work, is continually proven to be groundless. The U.S. Department of Labor reports that as information technology of all sorts inundates all strata of work environments in this country, productivity keeps rising. This is baffling to the Human Resources divisions of corporations, who seem to believe that workers will fall hopelessly distracted by even a window near their cubicles.

This might, in fact, be a blow in the name of socialism, supporting the tenet that a happy worker is a productive worker (then again, religion might be the opiate of the masses, but can it compete with terabytes of commercial pandering?) While use of the Internet for personal

activity might actually detract momentarily from business concerns, it is unlikely that such behavior will result in pathological levels of manic goldbricking from employees not otherwise so predisposed. Anecdotal evidence of individuals getting carried away might suggest that these same persons would find some way to shirk even in 18th-century Lowell factory townships.

Another reason businesses look at unrestricted access to external stimuli as something to worry about is the risk of negative publicity: when Microsoft's marketing question "Where do you want to go today?" is answered "HotYoungTeenLust.com" by your Accounting Department, you tend to get edgy about the next shareholders' meeting. American Puritanical hypocrisy aside, it's perhaps best not to let consumers know they're paying your employees to indulge their prurient interests.

This, too, may be a slightly overworked concern: recent reports that White House staff were using government networks to gather pornography resulted in very little public outcry. This might connote that Americans are now blasé about sexual shenanigans in the home of the Executive Branch, but it might also indicate a general apathy towards such behavior. The government, however, only stands to lose votes - businesses stand to lose market share, and are therefore (justifiably) more paranoid. In July, 50 employees of Dow Chemical were fired, and another 200 terminated for using company e-mail to circulate "inappropriate images."  
<http://www.usatoday.com/life/cyber/tech/cti298.htm>

Even strident advocates of civil liberties have a difficult time campaigning for the right to surf porn sites at work. Just about any lawyer will liken the wrongful termination suit of an employee caught collecting dirty pictures on company machines to the sexual harassment suit filed by a prostitute- like it or not, juries are simply not sympathetic in such instances.

And truthfully, such threats to the professional workplace environment can be effectively ameliorated by the institution of appropriate-use policies and the purchase of basic web-monitoring software. While even the best and most popular site-blocking applications cannot truly prevent access to "naughty" Internet destinations (as the majority of these rely on the diligence of underpaid grad students surfing for prohibited material, and the purveyors of prohibited materials have a profit motive encouraging creativity and proliferation), the ease of reaching such sites is hampered enough to take the fun out of that recreational endeavor for the average employee.

There is a third reason, this one fairly sound, that gives companies pause when considering the

vagaries of employees contacting the outside world through technological means: security.

Communication, by definition, is a two-way street, and while website cookies may be a relatively risk-free minor nuisance resulting from unhampered external contact, the likelihood of much more malicious intrusions also necessarily increases dramatically. E-mail laden with worms, viruses, and Trojan Horses are but the tip of the proverbial nightmare-iceberg for security specialists who have to protect systems from attack when users are granted unrestricted communications access.

## **Differing Minds**

Security professionals, and the companies they serve, have distinct perspectives on the means to lessen the risks to networks caused by exposure to external threats through the actions of employees - malicious, negligent, or otherwise.

One camp is rooted firmly in the Cold War security mentality: they believe that eternal vigilance, including snooping on cowed personnel, is the sole means of making sure nobody does anything wrong. General Dynamics Electronic Systems would seem to subscribe to this view: last summer, the gargantuan defense contractor launched PostMaster, an e-mail scanning application that can be used to detect policy infractions.

Another philosophy is emerging in the security industry, one that might better lend itself to the modern workplace environment: trust your employees. You can teach them, train them, and keep them current on security policy and procedure, but when all is said and done, no amount of direct action will prevent security mishap without cooperation from the personnel who actually use the system. Effective security practice can no longer be based on a unilateral initiative, if it ever was.

A growth economy exacerbates this situation: today, moreso than any other time in the past three decades, labor is a sellers' market, and personnel can and will choose to leave companies with repressive security practices. Like consumers who are skeptical of e-business claims when their personal privacy is in dubious care, workers will opt to join those companies that will offer them a semblance of trust - and demonstrate good faith in nurturing that trust.

Yet even when adhering to the trust model, employers do, and will continue to, have good reason to implement some overarching surveillance techniques; to not do so would be foolish.

Employees who find an employer they can trust will be more likely to acquiesce when asked to consent to monitoring, as they realize such activity protects themselves, too. The employees with a vested interest in the success of the company -those with stock options, profit sharing, etc.- will be even more amenable to what would otherwise be considered "intrusive" security practices. The rationale is simple: if I'm going to make more money if everyone is doing their job, tolerating colleagues who use company property as their personal playground during office hours is not the optimum choice.

## **The Long Arm of John Law**

Governments seem to understand this premise as well. While the network-intensive snooping performed by law enforcement is, for the time being, as restricted as other forms of surveillance such as wiretaps and surreptitious recording, there is little American legislation preventing such behavior by employers on their own equipment. Ownership bestows as many rights: employers can check the odometer on company vehicles just as they can examine the browsing activities of company computers.

In Europe, where the proposed Safe Haven legislation is heavily in favor of personal privacy, recent laws limiting the ability of companies to inspect their employees have been temporarily delayed (until October 24th) pending further clarification. This was in response to employer protest, and rightly so - if a company cannot assure the proper use of its assets, risk is magnified in untold proportions, troubling both investors and clientele alike.

What happens when the concerns of law enforcement and private business seem to conflict? Internet service providers (ISPs) have been asked to hand over data about their customers to law enforcement agencies on numerous occasions (with and without warrants), information that would otherwise conflict with the providers' own privacy policies and assurances. These instances will only increase as even more individuals, criminals and law-abiding alike, use ISPs to facilitate their activity.

ISPs, for the most part, have capitulated to such requests, on the premise that such companies want no part of abetting illicit activity. America On-Line, still the largest domestic ISP, has an entire office dedicated solely to processing such queries from law enforcement organizations.

Again, this is not only justifiable, it's good business practice and acceptable community behavior; if a rented car is used in a hit-and-run, the rental agency wants to resolve the matter

as expeditiously as possible, even if it means turning over customer records. Should personal privacy extend to those using market resources to break the law?

There are those who say "yes," especially when the vendor explicitly states that any customer information tendered under the assumption that such data will not be released outside the purveyor's domain for any reason.

The lines between government and private sector are blurred in many of these instances, and companies affected have no interest in making a stand- understandably so. The company is in business to do business, not to provide a vehicle for the conduct of illegal behavior. While some customers may fear the eventual release of their own information, most admit the need for such action, and all stakeholders involved are mollified by the resolution of legal issues without the cost and redirection of resources of litigation.

Few of us work for companies interested in public protest in lieu of profit.

This kind of debate will intensify as more the workforce opts to perform business functions from home, often with personally-owned equipment. Will employers' efforts to monitor these devices, otherwise outside the scope of their influence and propriety, be sanctioned by the courts and legislators?

The safe assumption is that it is only a matter of time before cases involving these very questions will demonstrate that companies will indeed be granted such power. While the attempt to extend OSHA's power to home-based offices was aborted early after inception, the efforts of labor unions and traditionalists to diminish the attractiveness of telecommuting for both companies and employees will likely tip the hand of the government in favor of far-reaching security enforcement.

Moreover, simple logic demands such corporate permissions; when an individual, acting as agent of an organization in return for financial remuneration, that organization necessarily has a need and requirement to supervise that the actions of its representative are in concert with the best interests of that organization, whatever the locale. People who believe that intentionally blurring the lines between work and personal life is a good idea have not fully thought through the idea.

## **Psychological Impact**

Most of us understand that, should we be paid to do a job, we owe a like measure of effort in recompense, and that utilizing the resources (to include time) of the employer is contrary to this codicil, implicit or otherwise. We are, however, people and the vagaries of our behavior usually fulfil this unspoken agreement.

There are those who pad their expense accounts, steal office supplies, make personal phone calls on company time, and generally abuse their rights and privileges of employment. Anecdotal evidence would even suggest that we laud these efforts even as we tacitly agree that they are worthy of only disdain and good cause for any punishment forthcoming. Slacking might be secretly admired, but getting caught is an unforgivable transgression.

Yet even as we (or those around us) take advantage of our positions, we still readily delineate between acceptable behavior and that which is excessive; the demarcation between right and wrong is clear and lucid to most people.

Why, then, are we somewhat riled by the efforts of the wronged (the employer) to diminish such wrongdoing? Nobody likes to be spied upon, even if that surveillance is warranted. We have come to expect a freedom from any intrusion on our personal privacy, and equate any such activity with Gestapo or KGB tactics. Innocent people, perhaps most of all, resent being treated like suspects.

We are convinced a certain amount of low-level "goofing off" is vindicated, and, indeed, it has been suggested that those who feel like they're getting away with something are happier - and therefore, more productive. That the company should overlook a certain amount of personal phone calls, e-mailed jokes, and on-line shopping in the interest of creating a more efficient workplace environment is more than a little ironic.

So perhaps the best way to engage in network-oriented surveillance activities is to indeed seek the approval of those who will be monitored. Buy-in from personnel might go a long way towards ensuring that the provisions -and ultimate security- of the company are upheld. Education and awareness, maybe even involvement, of employees in the security program is therefore highly-advised even for those companies that want to keep tabs on the behavior of their workers. The benefit of surveillance is only fractionally diminished if it is overt.

Of course, employers who use such tacit acceptance to mandate Draconian measures are doing a disservice to their own interests. Nobody likes to hear "this is for your own good," as their

teeth are kicked in. But we'd all like to feel like we're part of the solution instead of the problem. And we'd all like to be trusted.

[Privacy Statement](#)

Copyright 2006, SecurityFocus