

Over Your Shoulder: The Debate Over Internet and E-mail Surveillance in the Workplace

Ben Malisow 2001-05-23

Over Your Shoulder: The Debate Over Internet and E-mail Surveillance in the Workplace

by *Ben Malisow*

last updated May 23, 2001

One aspect of the Internet that has been a continual source of lively debate is the crackdown of employers on the use of web-surfing and e-mail applications in the workplace. This has caused much concern for civil libertarians and privacy mavens who strongly believe that surveillance of workplace Internet activities constitutes an intrusion on the democratic freedoms of employees and, as such, necessarily detracts from the benefits of living in such a democratic society. In addition to their concerns for the constitutional protection against unwarranted search and seizure, their rationale is rather simple and straightforward: taxpayers funded the development and construction of the information superhighway, they support the market environment where it (along with the many companies that profit from it) flourishes, and they continue to pay for the privilege of utilizing it. They should therefore be entitled to use it whenever and however they please, without pesky state troopers and private rent-a-cops abrogating that right.

Opponents of this perspective might object on the grounds that, in addition to paying employees for the constructive use of their time, employers are also the rightful owners and/or providers of workplace Internet equipment. Using a tired analogy, they ask whether workers should be allowed to go for a spin to the local porn shop in the company car. The subject has strong arguments on both sides. How can this issue be resolved in a practical manner to the satisfaction of both employers and their workers?

Concerns of Employers

Employers have several valid concerns regarding employees' use of the Internet and e-mail, which they use to justify the supervision of employees.

Decreased Production

One of the primary fears held by employers is that unrestrained access to the outside world will have a negative effect on productivity. This is continually proven to be groundless. According to

numerous U.S. Department of Labor reports, 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. While use of the Internet for personal activity might detract momentarily from business concerns, it is unlikely that such behavior will result in pathological levels of goldbricking from employees not otherwise so predisposed. (That said, anecdotal evidence of individuals getting carried away suggests that these same persons would find some way to shirk even in 18th-century Lowell factory townships.)

Tarnished Corporate Image

Another reason businesses regard unrestricted access to the Internet as worrisome is the risk of negative publicity. The employee's concern is that inappropriate use of the Internet by individual workers can reflect badly upon the image of the company as a whole. When Microsoft asks "where do you want to go today?" and your Accounting Department responds "HotYoungTeenLust.com," management may tend to get edgy about the next shareholders' meeting. American Puritanical hypocrisy aside, it could be very bad for business if consumers and business partners were to find out that they're paying (indirectly) for employees to indulge their prurient interests.

This, too, may be a slightly overblown concern. Reports in August, 2000 that White House staff were using government networks to gather pornography resulted in very little public outcry. Although this story made the front page of the Washington Post (Aug. 11), it didn't cause much uproar. This might signal that Americans are now blasé about sexual shenanigans in the home of the Executive Branch; however, it might also indicate a general apathy, if not acceptance, towards such behavior in society in general.

This attitude does not necessarily apply to the private sector: whereas the government only stands to lose votes - businesses stand to lose market share, and are therefore (justifiably) more paranoid. In July, 2000, 50 employees of Dow Chemical were fired, and another 200 terminated for using company e-mail to circulate "inappropriate images." (See [Dow Chemical fires 50 over e-mail abuse](#).) 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 say that juries

are simply not sympathetic to employees who are caught collecting dirty pictures on company machines, are dismissed, and subsequently file a wrongful termination suit.

And truthfully, such threats can be effectively lessened without employee surveillance by the implementation 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.

Security

There is a third sound reason that gives companies pause when considering the risks 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. The more users who are using the Internet and e-mail in an unsupervised manner, the higher the risk that these applications will be used in such a way as to place the network as a whole at risk. Of particular relevance at the moment are shareware applications such as Napster.

Another risk to the security of an enterprise is the disclosure of proprietary company information by employees. Certainly it is not outrageous to suggest that employers have the right to ensure that their networks are not being used to communicate information which might prove injurious to the well-being of the company.

Different Monitoring Philosophies

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.

Unilateral Snooping

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.

The Trust Model

There is another, less draconian philosophy emerging in the security industry, one that might better lend itself to the modern workplace environment: trust the employees. Effective security practice can no longer be based on a unilateral initiative, if it ever was. Employees can teach the workers, train them, and keep them current on security policy and procedure, they can even threaten them with dire consequences for security breaches, 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.

The information economy is redefining the relationship between employers and workers. In the Information Technology economy, labor is a sellers' market. Personnel have a greater opportunity to define the situations in which they choose to work, as such they can and will choose to leave companies with repressive security practices. Workers are more likely to join 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 continue to have good reason to implement some overarching surveillance techniques. However, employees who find an employer they can trust will be more likely to acquiesce when asked to consent to monitoring. This is true for two reasons. In the first place, in by trusting the workers, the company implicitly recognizes the workers autonomy, which will likely be rewarded with conscientious, responsible decision making by the worker. Secondly, the employers will realize such activity protects themselves, too. If an employee is suspected of unacceptable behaviour, reports of surveillance may be used to exonerate him or her. Furthermore, employees with a vested interest in the success of the company -those with stock options, profit sharing, etc.- will be even more amenable to actions that benefit the company as a whole, including what would otherwise be considered "intrusive" security practices.

Legislative Options

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 examine the browsing activities of company computers just as they can check the odometer on company vehicles. However, governments have yet to definitively address how they will address the issue of workplace monitoring through legislation. According to the online [Privacy Rights Clearinghouse](http://www.privacyrights.org/fs/fs7-work.htm), workplace monitoring is "virtually unregulated" (<http://www.privacyrights.org/fs/fs7-work.htm>.)

The Role of Third Party Providers

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.

So how will this issue be affected by the ongoing increase in telecommuters and remote employees? This debate will surely intensify as more members of the workforce opt 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?

It can be argued that it is only a matter of time before cases involving these very questions will demonstrate that companies will indeed be granted such power. 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 a right to ensure that the actions of its representative are in concert with the best interests of that organization, whatever the locale. .

Finding a Solution - Consensual Surveillance

Most of us understand that, if we are paid to do a job, we owe our employers a like measure of effort in recompense, and that utilizing the resources of the employer for personal amusement is contrary to this codicil. While 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, 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.

Employers who provide the means for the Internet and e-mail and who are subsidizing the time of their employees are justified in implementing some form of employee surveillance. On the other hand, as has been pointed out in this discussion, employees who are trusted and treated

with the respect that they deserve are not only more likely to be productive, they are also more likely to accept workplace monitoring.

So perhaps the best way to engage in network-oriented surveillance activities is to seek the approval of those who will be monitored. By notifying employees that their online activities are being monitored and by clearly explaining why that surveillance is being implemented employers can facilitate the understanding and cooperation of workers with a minimal disruption to company morale. Buy-in from personnel will go a long way towards ensuring that the provisions -and ultimate security- of the company are upheld. The education, awareness and involvement of employees in the security program is therefore highly-advised. The benefit of surveillance is only fractionally diminished if it is overt: in fact, it could be argued that overt surveillance is a markedly more effective preventative measure, as it acts as a known deterrent of unwanted behaviour that can be counter-productive for the company and embarrassing, if not terminal, for the worker.

Of course, it may seem that 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.

Ben Malisow, MBA, CISSP, is a Virginia-based security consultant with C-CUBED Corporation, Managing Editor of the humor site www.edodo.com, and all-around wonderful person who both surveils and resents being surveiled.

Relevant Links

[EFF "Privacy, Security, Crypto, & Surveillance" Archive](#)
Electronic Frontier Foundation

[Electronic Privacy Information Center](#)

[E-Mail and Privacy in the Workplace](#)
Stephen Entwisle

[Privacy Rights Clearinghouse](#)

[Privacy Statement](#)

