Abstract

It is likely that about one out of four large companies systematically monitors the computer, internet, or email use of its employees. There are over fifty different products available today that will let employers see what their employees do at work on their "personal" computers, in their email, and on the internet.

But what do such numbers really mean? What does employer monitoring of employee email, internet, and computer usage actually look like? What sorts of things can an employer see employees do at their computers, and what sorts of computer activities are currently invisible to workplace monitoring? These admittedly sketchy notes attempt to show, as concretely as possible given a minimum of technical terminology, what "employee monitoring" of internet and computer usage looks like: its extent, the key companies involved, the forces driving its adoption, some important distinctions between different types of monitoring products, and some possible future trends.

Acknowledgment

A shorter version of this paper was presented at a conference in Hong Kong on "E-Privacy in the New Economy", hosted by the Office of the Privacy Commissioner for Personal Data, Hong Kong SAR. Privacy Commissioner Mr. Stephen Lau's permission to re-use the paper is gratefully acknowledged.

Earlier versions of this paper have appeared in, or will be appearing in: Corporate Governance International (Hong Kong), e-law asia (Hong Kong), and Privacy Law and Policy Reporter (Australia).

How much computer and internet monitoring is there, really?

The following section is largely superseded by a report from the Privacy Foundation (US), "The Extent of Systematic Monitoring of Employee E-mail and Internet Use" (9 July 2001). The study found that 14 million employees in the US, or about 1/3 of the online workforce (that is, those employees with regular internet access at work), have their web surfing or e-mail monitored using a product like Websense or MIMEsweeper. Globally, the figure is about 27 million, or about 1/4 of the global online workforce. The report received extensive press coverage; for example:
A much-quoted recent survey by the American Management Association (AMA) found that over three-quarters of major US firms record and review employee communications and activities on the job ("More Companies Watching Employees, American Management Association Annual Survey Reports" [18 April 2001]; see also "2001 AMA Survey: Workplace Monitoring & Surveillance: Summary of Key Findings").

It is important to note that the AMA study includes monitoring of telephone use (43% of respondent firms), voice mail messages (7%), and video surveillance for security purposes (37%). In this paper, I'll be focusing almost entirely on the monitoring of computer, internet, and email use. Even here, though, the AMA numbers are staggering:

- Storage & review of computer files: 36% in 2001, compared with 13% in 1997
- Storage & review of email messages: 47% in 2001, compared with 15% in 1997
- Monitoring internet connections: 63% in 2001, up from 54% in 2000 (the first year this question was asked in the AMA survey)
- Blocking connections to unauthorized or inappropriate web sites: 40%, up from 29% in 2001
- Computer use (time logged on, keystroke counts, etc.): 19% in 2001, compared with 16% in 1997

Not to be outdone, the Society for Human Resource Management in the US says that a whopping 74% of surveyed HR professionals think their organizations monitor employee internet use ("Are You Being Watched?" [January 2001]).

However, a closer look at the AMA report reveals that "Most respondent firms carry on surveillance practices on an occasional basis in the manner of spot checks rather than constantly or on a regular routine." Systematic, constant or routine monitoring is usually what the word "monitoring" evokes, yet few citations of the AMA study have emphasized the point that most of the AMA's figures represent spot checks rather than full-scale surveillance.

The notion that such large-scale monitoring of computer, email, and internet use is really taking place seems to be contradicted by the state of the employee-monitoring (EM) industry. Companies monitoring employees -- in the sense of systematic surveillance, rather than random spot checks, or ad hoc responses to a specific situation -- presumably do so using commercial EM software. Yet the EM business, while growing, does not report the revenue figures or market penetration one might expect from the AMA survey, or at least from the way that the AMA survey is typically quoted.

One of the best ways to understand the scope of workplace surveillance is to look at the market for employee-monitoring products. Perhaps the largest EM company (though not the largest company involved in the EM business), Websense (Nasdaq:WBSN), recently reported its subscription-based revenues for Q1 2001 were $6.7 million (all figures are in $US), representing more than 8.25 million worldwide customer "seats," pre-paid on a subscription basis ("Websense Inc. Announces First Quarter 2001 Results, Reports Strong Visibility, Progress Toward Profitability", April 24, 2001).

Aside from indicating that Websense apparently makes as little as $3.25 per monitored employee per year (though, as noted below, the company itself estimates an average cost to employers of $15 per employee), the coverage of 8.25 million workers worldwide by perhaps the largest EM vendor is hardly consistent with the notion that most employees with computers at "large" companies in the US are constantly surveilled. At the same, the 8.25 million figure -- which includes Websense's recent largest-sale ever, 200,000 subscriptions to the US Army, for $1.8 million -- is obviously very significant, and provides a useful starting point for understanding the true scope of employee monitoring.

The 8.25 million figure is an overestimate for the number of employees monitored using Websense, because, in its default configuration, this product merely blocks certain web sites, and does not keep any record of attempts to visit these sites, much less of successful visits to non-blocked sites. It is the recording, rather than the blocking, that would constitute monitoring or surveillance. Websense has a separate module, Websense Reporter, which records all web accesses (not only attempted accesses blocked by Websense, but also all non-prohibited web surfing) -- and, significantly, 70% of Websense's customers choose to install this Reporter module, according to a company spokesperson. So instead of 8.25 million workers monitored by Websense, we have perhaps 5.75 million.

(On the other hand, the same Websense spokesperson noted at a different time that "Since many of Websense's customers are mid-to-large size companies, they generally do not drill down to the employee level. They're not concerned with individual Internet use as much as they are concerned with department Internet use. Our research shows that our customers run reports to find internal Internet use trends.")

Curiously, another large EM company, SurfControl (Easdaq:SRFC; London:SRF) says in its 2000 annual report that the Corporate Internet Access Control (CIAC) market has less than 1% penetration. Revenues for the SurfControl product in the year 2000 were about $8.75 million, about 3/4 from the US; its average order is $4,500 ("SurfControl sales rocket by 200%", The Register, 5 April 2001). Clearly, not all of this was for SurfControl's business products, the SuperScout Web Filter and SuperScout Email Filter; SurfControl also has CyberPatrol for the home and educational markets.

Perhaps SurfControl's 1% figure is meant to emphasize the potential for growth. Indeed, another widely-cited study, by International Data Corp., maintains that the EM market should grow at an annual growth rate of 55% (International Data Corp., "Employee Internet Management" [Sponsored by Websense]) -- a figure clearly inconsistent with the nearly-saturated market implied by the notion that
three-quarters of employers already engage in this type of surveillance.

Or, perhaps employers don’t really need products such as SurfControl or Websense to monitor their employees. Some could be using standard Unix or Linux tools such as syslog (see the section on “Log files and other forms of monitoring” in Kurt Seifried, “Linux Administrator’s Security Guide”, 1999). It’s worth noting that many cases of employees fired or suspended for “inappropriate” internet or email use (see the "Job Loss Monitor" maintained by the Privacy Foundation's Workplace Surveillance project) have not involved systematic monitoring.

For example, an article on the firing or suspension of twenty state employees in South Dakota notes that the state government "doesn’t have any systematic filtering or monitoring system in place to keep tabs on its 13,000 employees. The current investigation has relied on one Web log report of the 100 users with the most hits over a three-week period" (Jeffrey Benner, South Dakota: Fire, Don’t Filter", Wired News, 7 June 2001). Similarly, an in-depth account of 20 New York Times workers fired for sexually offensive emails notes that "the investigation started with something far more mundane: old-fashioned snail mail" (Ann Carns, "Bawdy email backfires on NYT staff", Wall St. Journal, 4 Feb. 2000).

As a counterexample, though, an article on 40 Xerox workers fired for surfing forbidden web sites states that they were "nabbed not by managers or fellow employees but by software designed to monitor their online indiscretions. The software recorded every Web site they had visited (many of which, it turned out, were related to shopping or pornography) and every minute they had spent at those sites.... they were not the only ones being subjected to the watchful eye of the monitoring software. In fact, the Web use of every one of Xerox’s 92,000 employees -- in countries around the world -- is routinely monitored by the company" (Lisa Guernsey, "On the Job, the Boss Can Watch Your Every Online Move, and You Have Few Defenses", New York Times, 16 December 1999). Indeed, Mike Gerdes, manager of information security at Xerox, has been quoted in the press several times on the subject of employee monitoring (e.g., "CyberSlacking", Newsweek, 29 November 1999), but declines to specify the products used.

Still, it's important to keep a clear distinction between systematic monitoring on the one hand, and ad hoc investigations or spot checks on the other.

Taking Websense's perhaps 5.75 million monitored seats, figuring a similar figure for SurfControl (see below), and adding in the other publicly-traded companies with EM products -- Telemate.Net (TMNT), Eiron (ELRN), Tumbleweed (TMWD), N2H2 (NTWO), and Baltimore Technologies (BALT) -- plus the several dozen smaller companies with EM products, we are probably talking about 20 to 25 million employees worldwide whose internet, computer, and email usage is being tracked in the constant way that the word "surveillance" usually conveys. (Jupiter Research has reported that 43 million workers in the US currently have online access, and that the US represents about one-third of the global internet population.)

All in all, it seems most reasonable to say that perhaps as many as one-quarter of employers monitor the computer and internet use of their employees.

Indeed, a recent survey by the office of the Privacy Commissioner for Personal Data (Hong Kong) found that 27% of responding organizations monitor employee computer use, 23% monitor web browsing, and 21% monitor employee email (Private Thoughts: Newsletter of the PCPD, August 2000). On the other hand, the Hong Kong survey did not specify whether "monitor" included spot checks in addition to systematic monitoring; it did however refer to "devices for monitoring," perhaps as distinct from a spot-check perusal of an employee's computer in response to a specific suspicion.

Some additional data points:

- A poll of corporate chief information officers (CIOs) in the US, conducted by CIO magazine, found that only 17% of CIOs conduct sporadic employee email checks, 16% never monitor employee email, 11% check only on "problem employees," and 38% check only after there's been a complaint or productivity issue ("CIOs Say Personal Email/Internet Use Increases Productivity", 25 April 2001).
- In the UK, KPMG conducted a small survey in late 2000, and found that around 50% of the surveyed companies monitor internet use "infrequently," around 20% monitor on a monthly basis, and only 11% monitor on a daily basis ("The Uneasy World of E - KLegal Internet Survey", 19 Jan. 2001).
- A Vault.com "Internet Use Survey" in Fall 2000 asked "Do you restrict/monitor your employee internet/e-mail use?"; 41.5% of the 670 surveyed employers said Yes ("Results of Vault.com Survey of Internet Use in the Workplace"). Its Sept. 1999 survey had only 31% of the 1,438 surveyed employers say Yes. Interestingly, of 451 employees surveyed in Fall 2000, 53.5% thought their employers monitored, and of 1,244 employees surveyed in Sept. 1999, 45.5% thought their employers monitored.
- A study by market analysts Frost & Sullivan, reported in PC Magazine ("US Business Pours Money into Content Filtering", 10 May 2001), states that "content filtering" generated $119 million in revenue in 2000, 77% of it from corporate customers: in other words, a corporate market for content filtering of about $92 million.
- If we take "content filtering" to be roughly synonymous with employee monitoring (as noted earlier, Websense says that approximately 70% of its customers install the Websense Reporter module, which logs all web accesses), how many monitored employees does this $92 million represent? Websense has an "ROI [return on investment] Calculator" at its web site, whose JavaScript source uses a figure of $15 per employee; similarly, SurfControl has an ROI Calculator at its site, whose JavaScript source uses a sliding scale, from $1195 for 50 or fewer employees, to $45,000 for 10,000 employees, but with an average of $10 per employee. If we take the lower figure of $10 per employee, the $92 million in corporate revenue in 2000 then represents about 9 million employees -- either newly monitored, or with annual monitoring subscriptions renewed. The number would be larger if you figured in a reseller discount of something like 30% (see below).
It does seem probable that something like three-quarters of employers have checked up on at least one employee's computer, email, or internet usage at one time or another. But again, this needs to be distinguished from monitoring. In some ways, to set aside spot checks (which are, arguably, merely a form of supervision), and focus entirely on systematic monitoring, employing an EM product, simply emphasizes the scope of true employee monitoring: as suggested above, we're talking about 20 to 25 million employees whose computer, internet, and email is constantly surveilled.

It is also clear that employee monitoring is growing. For example, while Websense currently claims 8.25 million "seats," as recently as July 2000 it claimed only 5.4 million, and for July 1999, only 3.3 million (see "Websense Inc. Announces Second Quarter 2000 Financial Results", 25 July 2000).

Almost every month, a new vendor seems to enter this market. The number of effected workers could also jump dramatically if Microsoft, for example, decided to "integrate" (i.e., bundle) employee-monitoring capabilities into future versions of its operating systems (Microsoft already promotes a long list of "reporting" and "access control" partners for to its Internet Security & Acceleration Server; see "Partners: Reporting" [3 May 2001] and "Partners: Access Control" [3 May 2001]).

Important distinctions

Having already noted the distinction between spot checking on the one hand, and systematic monitoring on the other, several additional important distinctions should be made when discussing employee monitoring:

- Monitoring email, vs. monitoring web surfing, vs. monitoring other internet activities such as "chat" and instant messaging, vs. monitoring computer activities such as files accessed, programs run, and keystrokes entered.
- Monitor/log/record vs. filter/block -- Some products can actually block access to a web site, or prevent the sending or receipt of an email, as opposed to simply making a record of the access. From a privacy perspective, filtering/blocking is preferable to monitoring/logging/recording. From an anti-censorship perspective, of course, it might be the other way around. Many products do both: prevent access to particular sites or email, and make a record of the attempted access.
- Log everything vs. log exceptions -- Some products by default make a record of everything they see, while also highlighting or raising an alert for violations such as accessing an "inappropriate" web site. Other products only record infractions, or at least have this as their default behavior.
- Content/body vs. traffic data/headers -- Some products will inspect the entire contents of an email message or web site to determine its appropriateness; others only inspect the email header (sender, recipient, subject, size, etc.) or the web site's address (URL). Similarly, note the difference between counting the number of keystrokes and recording the actual keystrokes themselves.
- Client vs. server/network -- See "Client-Based vs. Server-Based Interception" below
- Continuous vs. random vs. spot check/response -- See "How Much Computer and Internet Monitoring is There, Really?" above.
- Aggregate vs. individual/specific -- When records are kept of employee activities, do the logs tie specific activities to specific employees (e.g., "Joe made 5 visits to playboy.com"), or does the employer only keep aggregate statistics (e.g., "We had 10 visits to playboy.com last month")? Similarly, do the records include details such as complete URLs ("Joe visited these specific pages at playboy.com"), or do they provide an aggregate per individual ("Joe spent a total of 30 minutes at playboy.com" or, less detailed, "Joe spent 30 minutes at a site on our prohibited list"). One approach might be to conduct aggregate monitoring to first see if there's even a problem that warrants closer inspection.
- Inspecting storage vs. intercepting "on the fly" -- Some monitoring involves nothing more than inspecting files on the PC used by an employee, or inspecting copies kept in the employer's backup server, or mail server, or inspecting log files kept by a web proxy server. An EM product is not even required for this; it seems likely that most reported employee firings and suspensions over internet, computer, or email usage have involved this type of after-the-fact inspection. Some EM products simply create additional records which can then be inspected in the same way. Many products, though, actually catch (intercept) employee activities in "real time," for example by blocking access to web sites or inspecting and filtering emails after they have left an employee's computer, but before they've been sent over the internet.
- Vendor defaults vs. customized triggers -- Probably all of these products are customizable by employers. But how much customization actually goes on? Are employers generally simply going with the defaults set by the vendor? (This may be of particular concern when government agencies outside the US install EM products whose database of "inappropriate" sites has been compiled in the US; see for example Electronic Frontiers Australia, "Government approved Net filters attempt to silence critics" [29 June 2000].)

The issues

There are numerous reasons, both good and bad, for employers to monitor the personal-computer (PC) and internet activities (including email and web surfing) of employees. Two of the driving forces behind this monitoring are simply the decreased cost and increased ease of use of workplace-surveillance software. Amusingly, some of these products were originally intended for parents and schools to monitor the online activities of children ("nannyware"), or for spouses to monitor each other ("adulteryware"; see "Snoop software: Unhealthy at home?" [MSNBC, 9 May 2001]). Could this be what businesses mean when they describe their workforce as "part of the family"?

Employers can monitor the PC and internet activities of employees either by intercepting data in "real time" (which also allows prohibited
Employers can install interception devices on the PC used by the employee, and/or on the network. Where the employer plants this "bug" or "wiretap" (as it were) determines the sort of information that the employer can gather.

Software installed on an employee's PC, such as WinWhatWhere Investigator or Webroot WinGuardian, can capture the keystrokes (even deleted ones) that an employee types; it can also "see" what the user does in programs, such as Microsoft Word, that are located on the PC. In contrast, products installed on the network, such as eSniff, or SurfControl, are best for monitoring employee email and web surfing -- and are certainly more suitable if the employer wants to monitor the activities of a large group of users at the same time. Some programs (such as Trisys Insight) take a hybrid approach, installing a small "agent" program on the PC that communicates with the main program, installed on the network.

An employer primarily interested in monitoring employee productivity, for example, might prefer a very different type of surveillance device from an employer whose main concern is, say, preventing (or at least detecting) sexual harassment in the workplace. Detecting trade-secret leakage may require different technology from preventing visits to web sites that specialize in pornography or gambling.

Another way to monitor employees is to examine stored data. This might include perusal of log files maintained by the employer's proxy server, or it might be as simple as the human resources (HR) department using a web search engine to see if they can find out anything about the personal web postings of employees or prospective employees.

Employee surveillance software can employ different "triggers" when determining whether to raise an alert. Some products scan all emails for certain keywords, much as Echelon and the US FBI's Carnivore were reported to do. Others check all attempted web accesses against a list of unapproved sites. Some vendors claim that their products use "artificial intelligence" or "neural networks" to spot problems (i.e., "given this piece of email I don't like, figure out all the other emails I won't like, and block them"). Some products simply log all employee activities in excruciating detail, and leave it to a human (or perhaps another program) to figure out which items, if any, are cause for concern.

Many (and possibly most) of these products, in addition to monitoring (that is, recording entries in a log file), proactively block or filter, for example refusing to establish a connection with a pornographic web site, or refusing to allow the sending of an email with a viral attachment. Issues of censorship and free speech (or rather, freedom to receive speech) have been raised regarding these products, for example when installed at public libraries or public schools in the US.

The privacy concern, however, involves the monitoring rather than the blocking/filtering aspect of these products, which can, over time, assemble a comprehensive profile of an employee's web surfing, email, applications, and so on, all associated with the employee's identity (such as a workstation ID assigned by the employer).

Some worrisome implications:

- What about monitoring of public employees? For example, in the US, do the log files produced by EM software installed in federal, state, and local government offices become "public records" that are subject to Freedom of Information Act (FOIA) requests?
- As email and email attachments become the "lifeblood" of companies, is it really the employer's intent to memorialize every email conversation by keeping detailed employee-monitoring logs? How long will these logs be kept? There's a danger that the previously ephemeral (the equivalent of casual conversations at the water cooler) will now be fixed in a permanent record. The technology is available to record pretty much everything that happens at work (Shoshana Zuboff's fascinating early look at employee monitoring, In the Age of the Smart Machine: The Future of Work and Power[Basic Books, 1988] refers to this possibility as the "textualization of work"). Of course, this isn't just an issue with employee monitoring; note for example the Deja.com archive of Usenet postings, recently acquired by Google (see "Privacy Concerns for Google Archive", New York Times, 7 May 2001).
- Are there any intellectual property issues here?
- Assuming that almost all employees commit some infraction of computer and internet usage policies at one time or another, will stockpiles of employee-monitoring logs be used later as a "wishing well" by supervisors and employers seeking, for example, to disguise layoffs as disciplinary actions?
- Will the log files created by employee-monitoring software become a "honeypot" for litigation? (See below)
- Is monitoring essentially an editorial function, in effect turning the employer into a "publisher," rather than a mere distributor, of any material that appears on its system, and thus potentially more liable than it would be without monitoring for any contents that pass through its system? Note for instance the "pervasive disincentive" created in the US by the 1995 decision in Stratton Oakmont v. Prodigy, which led in part to a"Good Samaritan" provision in the subsequently-overturned Communications Decency Act (see Michael R. Overly, e-policy, pp. 50-51: "The greater the control a business has over the content of a communication, the more likely it will be found to be a publisher"). As another example, some employees are counseling companies to encourage employees to use personal web-based email, such as Hotmail or Yahoo: "A company might have an easier time proving that it did not contribute to an unhealthy working environment if an employee sent sexist jokes or racist commentary through his personal email address instead of the corporate email address" (Web-based email services offer employees little privacy", CNET, 3 Oct. 2000).

While employers presumably install workplace surveillance to reduce risk, liability, and costs, this surveillance introduces new risks, liabilities, and costs. Installing an email-monitoring system which tries to filter out objectionable email could, for example, leave the employer that much more responsible for any objectionable email that the system fails to prevent, or may simply serve as a new storage mechanism -- a "honeypot" -- for "smoking gun" documents to be discovered later during litigation. And, of course, it may open the employer up to employee complaints of intrusion.
Why monitor employees?

There are numerous reasons why employers might monitor the computer and internet activities of employees, but all these reasons should address the following two questions:

- What risks are we trying to prevent or detect or manage here?
- What policy is this monitoring intended to enforce?

A 1993 survey of employers gave the following reasons for monitoring (Charles Piller, "Bosses with X-Ray Eyes," *MacWorld*, June 1993):

- Monitor work flow: 29.2%
- Investigate theft: 29.2%
- Investigate espionage: 21.5%
- Review performance: 9.2%
- Prevent harassment: 6.2%
- Seek missing data: 3.1%
- Seek illegal software: 3.1%
- Prevent personal use: 3.1%

A survey in the November 1997 issue of *PC World* ("The Need for Monitoring") gives the following survey results:

- Crack down on recreational use: 58%
- Put an end to downloads of pirated software: 47%
- Avoid sluggish internet connections due to recreational browsing or excessive downloads: 33%

At the same time, monitoring employee PC and internet activity -- and thus possibly intruding on employee privacy -- can actually provide benefits, including privacy benefits, to some groups besides the employer. Employee monitoring may help enforce restrictions on access to customer personal data. For example, the US Health Insurance Portability and Accountability Act (HIPPA) mandates the use of "audit trails" to protect the privacy of patient data. According to one medical security specialist, "Privacy should be protected in health care by 'tagging' all health data with the names of every single person who viewed it.... Any patient who wants to see their record should be given immediate access to it. Then they would be able to see exactly who has been viewing their data, which, many people don't realize, can total hundreds and hundreds of individuals" (quoted in *Health Data Management*, October 1998, p. 60). These individuals are, needless to say, monitored employees. Thus, privacy (for one group, such as patients or consumers) may be bought at the price of privacy (for another group, employees).

As the HIPPA example suggests, some employers are essentially required to monitor employees. To take another example, some form of employee monitoring would seem to be required for compliance with US Securities and Exchange Commission (SEC) record-keeping rules 17a-3 and 17a-4, and with amendments to NASD rules 3010 (supervision) and 3110 (books and records) (see "NASDR Adopts Rule Amendments Regarding Public Correspondence", 17 April 1998; "NASD expects members to prohibit correspondence with customers from employees' home computers or through third-party systems unless the firm is capable of monitoring such communications"). This is reflected in the AMA survey, which shows much higher monitoring in the financial sector than in any other. Some products, such as the SRA Assentor email-monitoring product, specifically target financial institutions (SRA has also built a product that Nasdaq uses to monitor stock chat boards).

Monitoring may also be necessary to reduce a sexually or racially "hostile environment" in the workplace, which is at least arguably a privacy issue (but see, for example, the argument against overbroad use of the term "privacy" in Raymond Wacks, *Law, Morality, and the Private Realm* [Hong Kong University Press, 2000]).

The following is a list, in no particular order, of some concerns that have been related to employee monitoring:

- Productivity (e.g., measuring raw keystrokes/minutes; preventing access to time-wasting web sites: games, porn, personal finance, sports, music)
- Bandwidth (Conserving network resources by reducing access to non-productive sites; a somewhat different issue from monitoring employee productivity)
- Cost center (for billing based on client codes, or to assess timesheets)
- Intellectual property (enforcing software licenses for a specified number of "seats"; reducing company liability for software piracy by employees; the Business Software Alliance encourages employers to monitor for compliance)
- Trade secrets (detecting copying of employer’s trade secrets in emails, to floppy or zip disks)
- Security (detecting viruses in emails or email attachments; preventing employees from unintentionally downloading trojan-horse programs)
- Insubordination (employees and former employees venting their "bad attitude" in chat rooms and on "gripe" boards, posting internal company documents to FuckedCompany.com, etc.; see "By the Water Cooler in Cyberspace, the Talk Turns Ugly", *New York Times*, 29 April 2001)
- Job seeking (Employees visiting Monster.com, HotJobs.com, etc., or using Microsoft Word to work on my_resume.doc)
- Cyber-moonlighting (working a second job while at work; working on a personal web site at work)
PC and internet monitoring: driving forces

(Back to top)

Indeed, employee-monitoring software may sometimes be installed, less with a clear purpose of enforcing specific policies and managing specific risks, and more because the software is "there": readily available, at an apparent low cost:

- Trisy Insight: $85 per monitored computer, for 50-99 users.
- WinWhatWhere Investigator: $34 per "seat" for 100-149 licenses.
- Adavi SilentWatch: $35 per "seat."
- WebSense: $5,000 for 1,000 users. (As noted earlier, Websense revenues represent about $3.25 per user per annual subscription, its large sale to the US Army was for about $9 per user [though this sale also included cache engines and Ethernet switches], and its ROI calculator estimates $15 per user. The discrepancies are partially accounted for by reseller discounts; Websense "channel partners" get a 30% discount.)
- SurfWatch@Work: $995 for 50 users.
- SmartFilter for Microsoft Proxy Server: $3,250 for 1,000 users
- LittleBrother Pro: $495 for 10 users.
- CyberPatrol for Microsoft Proxy Server: $1,395 for 100 users
- SurfControl: as noted earlier, its "ROI calculator" on the web prices 50 or fewer employees at $1,195 ($24 per employee), and 10,000 employees at $45,000 ($4.50 per employee); the average is about $10 per employee.

In other words, the initial cost of purchasing employee-monitoring software is generally far less than $100 per user, and in large organizations may be as little as $5 per user. (Of course, the actual total cost of ownership is likely much greater, when you consider that someone must not only install and maintain the software but must, most importantly, be ready to respond appropriately to the personnel issues raised by the output that employee-monitoring software produces.)

This apparent low cost is probably driving the adoption of employee monitoring in the same way that the low cost of cameras has promoted increased use of visual surveillance.

In a sense, we're dealing here with the technical possibility of "Carnivore on the Desktop": ubiquitous, fine-granularity surveillance in the hands of every employer. On the other hand, it is crucial to recall the figures given earlier: right now probably no more than 25 percent of employers systematically monitor their employees.

As noted earlier, some of the "spy on your employees" products started off life as "cybernanny" products for the home/school market. Having difficulty selling to schools and consumers, many of these companies looked around to see what else they could do with their cybernanny products, and realized that other businesses might be a better market. As the head of Websense has noted, "After four years, they all realized schools don't have much money to spend"; the head of N2H2 agrees: "Most of them have left education and are now gearing toward the business enterprise market" (quoted in "Desk Top Cops", Internet World, 15 August 2000). Thus, another driving
Companies are gradually realizing that the whole idea of a "personal computer" creates workplace problems. Especially with essential resources increasingly located on the internet rather than on the PC, there is perhaps a trend to treat the PC more as a centrally-administered terminal than as a "personal computer." IT departments may see employee monitoring as a way to regain some control over the desktop. If so, there is a danger that technical considerations may end up being allowed to drive policy. One interesting question is whether IT departments, rather than HR, are generally being left responsible for employee monitoring.

Client-based vs. server-based interception

All available employee-monitoring products are essentially programs that report on (and in some cases constrain) how you use other programs. Having installed an employee-monitoring program, an employer can -- depending on the type of program -- see how much time employees (individually and/or in aggregate) spend playing Solitaire, or what web sites they visit, or even read email messages that they typed but then deleted and didn't send. The employer may also be able to prevent employees from visiting certain web sites, or from sending or receiving certain emails.

One way to understand these products is to consider where they are installed. There are basically two types: server-based monitors, designed to be installed on the employer's network; and client-based monitors, designed to be installed right on the personal computer (PC) used by the employee.

First, we'll look at the network (server), then at the PC (client). To see the difference, let's imagine a typical employee, whiling away the time playing Solitaire. Wes Cherry, the Microsoft programmer who wrote the Solitaire game included with Windows, has noted that he has single-handedly "wasted more corporate time than any other developer" (though employers might recall that many employees first learned to use a mouse by playing Solitaire). The question is, Can the corporation tell (short of looking over his or her shoulder) whether an employee is playing Solitaire?

To hear the vendors' claims, the answer is yes, they can see everything. Naturally, privacy advocates, whose chilling reports in turn sometimes help reinforce vendor hype, rely upon these Orwellian claims.

Network-based (server) products

eSniff, who make workplace-surveillance hardware, claim: "If an employee goes outside of your eboundaries, eSniff provides an exact copy of everything that was on their screens; sites visited, chat room activity, email ... everything."

Now, eSniff provides network-based surveillance. That is, like a wiretap, it listens in "real time" to everything that employees do on the network. According to the company, "The eSniff device uses patent pending linguistic and mathematical techniques to analyze the content and context of all TCP/IP traffic. All traffic is analyzed; Web, e-mail, chat, ftp, telnet, print jobs, absolutely all traffic that crosses the wire."

Another example of network-based monitoring is SurfControl's amusingly-named LittleBrother (oddly, there doesn't yet seem to be an employee-monitoring program called BigSister). The products made by the largest employee-monitoring vendor, Websense, are also network-based, plugging into an employer's firewall, proxy, or cache server.

These server-based products produce reports that would show if an employee was playing a web-based version of Solitaire. But not the Solitaire (nor FreeCell or MineSweeper) that come bundled with Windows, because these games run entirely on the PC, without making a network connection. When a network-based surveillance product like eSniff claims they can monitor "everything," they mean everything on the network. (And actually, "everything on the network" isn't quite right either, because many of these products can't do much about encrypted content, such as web pages that use the https:// rather than the http:// protocol.)

This approach is good for detecting (and, with some products, perhaps even preventing) employees from visiting pornographic sites, from whiling away the day at web-based gaming sites like Pogo.com, from taking on a second job as a "day trader" (though recent events on Wall St. may do more to curb this activity), from venting a bad attitude about the company at a site whose unprintable name is FuckedCompany.com, or from sexually harassing their coworkers via email.

PC-based (client) products

But it can't catch them viewing porn that they've already downloaded to their computer, nor can it see how much time they waste playing games off a CD ROM (unless the game "phones home" over the network), nor could it see them copy company secrets to a floppy disk, or polish their resume in Word. These are all activities that happen on a PC, generally without accessing the network.

To see those sorts of things, employers need something more akin to a camera, located right on the PC used by the employee, rather than a listening device (so to speak) like eSniff that sits on the network.
A good example of such a client-based product is **WinWhatWhere Investigator**. This product records the names of programs you run, the titles of the windows that are open on your computer, and -- most significantly -- the keystrokes that you type, including ones that you subsequently delete. (For sample "screen shots," see "Examples from Investigator Reports".)

For example, while WinWhatWhere Investigator was running on my PC, I wrote an email to a friend that contained the text, "I think I have herpes" (this text comes from a recent advertisement for **SafeWeb**, an anonymizing product which promises to protect employees from monitoring by "anyone -- including your boss"). I then deleted the line, and typed, "I'm fine." Then I decided not to send the message, after all.

WinWhatWhere's report showed the following: "I think I have herpes. I'm fine." In other words, my ephemeral thoughts have now been permanently recorded (this fixing of "deleted" contents may raise some interesting intellectual property issues). The report also showed: "Message has not been sent." It also showed the nickname (but not the actual email address) of the aborted email's intended recipient. (On the preservation of ostensibly "deleted" material, see the following thought-provoking article by a federal judge in Minnesota: James M. Rosenbaum, "In Defense of the DELETE Key", *Green Bag*, Summer 2000; though also see "Billg's dream? Honey, I disappeared the emails...", *The Register*, 1 June 2001.)

I've also seen WinWhatWhere record personal information (such as passwords) that I've entered onto "secure" web pages, encrypted with https://, such as the customer information page at Amazon.com. Even if the employee uses the SafeWeb anonymizing service, WinWhatWhere can still capture keystrokes and window titles (which often describe web sites visited).

Even WinWhatWhere's author, Richard Eaton, says, "A lot of things this program does cause me great consternation." According to Internet Week ("Keystroke Logging Software Spies on Chats, IMs," 7 November 2000), "Eaton is having second thoughts about a feature that can sweep up passwords. "If you tab across a password field, it picks all that up," he said. "I haven't decided if that is good or bad." He's referring to WinWhatWhere's ability to go into a form on a web page, and pick up the contents of text fields that already contain information -- such as a password dialog box which already contains the user's saved password.

On the other hand, WinWhatWhere does not appear to detect the typing of a passphrase in the Windows version of PGP (Pretty Good Privacy) encryption software; PGP uses Windows "console" input which, like DOS input, is missed by client-based monitors due to the technique they happen to use to "hook" the keyboard (for what it's worth, a more compulsive monitor would use a low-level "virtual device driver" rather than employing the higher-level SetWindowsHook() API).

Because the surveillance occurs right on "your" PC -- actually, it's not literally surveillance at this point, just logging of your activities to a file or database, for later perusal -- rather than on a central server, it is obvious that more of your activities can be monitored than from a network-based program. And it can be done whether you are connected to a network or not.

You can configure these programs to hide their presence from most users, though the vendors generally recommend that employers make the monitors' presence known (though not in a way that allows the monitor to be easily disabled).

But since the program runs on a PC used by an employee, how is the employer going to see the report that WinWhatWhere so compulsively keeps? An employer (or an HR or IT person assigned this task) could walk up to the PC itself, press a special key sequence, and view the report. Or the program can be configured to periodically "stealth email" the report to a designated address.

In contrast to the server-based monitors, this obviously isn't monitoring in "real time," nor does this level of detail seem conducive to large-scale surveillance of many users at the same time from a single location (think of Montgomery Burns looking at his multiple monitors in the cartoon, "The Simpsons"). However, WinWhatWhere can be configured to save its log files to a network file server, with logs from multiple PCs poured into a single database, and the entries from each individual PC distinguished by user name. Coupled with WinWhatWhere's configuration options to turn off some forms of monitoring, such as keystroke logging, this could perhaps be made into a system-wide monitoring tool.

Another client-based monitor is **Webroot WinGuardian**. In addition to capturing keystrokes and logging programs run and web sites visited, WinGuardian can capture "screenshots" (i.e. graphic images of the entire computer screen) at specified intervals (down to once per minute), and then email them out for remote viewing. The screenshots can then be "played back" on another computer to see what the employee was doing, literally every minute of the day.

Yet another such product is Spector, from **SpectorSoft**. I've spoken with one HR director who installed Spector on an employee's PC after repeated complaints (by other employees), and after his own repeated denials, that he was spending hours every work day viewing pornography. This is probably a representative example of non-systematic monitoring, conducted in response to a specific situation. The HR director said that Spector covertly saved away frequent screenshots of the employee's activity, and that viewing these screenshots later, after the employee had left for the day, was (a) necessary under the circumstances; and (b) extremely creepy, "like looking at someone else's screen through their own eyes." Spector's own web site makes these promises for this $69.95 product: "Automatically record everything your spouse, children & employees do online.... Spector SECRETLY takes hundreds of screen snapshots every hour, very much like a surveillance camera. With Spector, you will be able to see EVERY chat conversation, EVERY instant message, EVERY e-mail, EVERY web site visited and EVERY keystroke typed."

To eliminate the awkward need for viewing saved records on the employee's PC, SpectorSoft also makes **eBlaster**, which, for an additional $69.95, sends out detailed email reports: "eBlaster delivers detailed activity reports, including all web sites visited, all applications run, and all keystrokes typed, right to your e-mail address, as frequently as every 30 minutes."

These client-based monitors begin to sound like what is known as a RAT (Remote Admin Trojan), similar to Symantec's pcAnywhere, or
the notorious hacker tool "Back Orifice." These "trojan horse" programs typically include both keystroke logging and screenshot capture, and so could conceivably be used for employee monitoring.

Having just looked at client-based employee monitoring, it is crucial to note that few EM products currently use this technique in a system-wide fashion. WebSense, SurfControl, Elron Internet Manager, and MIMESweeper, for example, are all server-based. Practically all the EM software installed at major companies is server-based. However, client-based monitoring does make a good illustration of what's technically possible with employee-monitoring software available today; one just has to remember that this particularly-intrusive technique is not in widespread use. As the Spector example illustrates, though, HR departments may be using such products to deal with specific problem employees.

**Hybrid (client/server) products**

Some workplace surveillance products, like Trisys Insight, are hybrids. (See [http://www.born2e.com/isgt/MainPage.asp](http://www.born2e.com/isgt/MainPage.asp) for a live online demo; you get to snoop on selected Trisys employees.) This involves a small "agent" program on the PC used by the employee, which sends messages to a server program. This company even offers an "outsourced" service, whereby Trisys itself will monitor your employees' activities for you. Trisys doesn't monitor specifics like keystrokes or the text of email messages. Instead, it concentrates on measuring the amount of time spent at web sites or using specific applications.

Another hybrid program is Wards Creek GameWarden. According to the company, "Its client/server technology allows for monitoring and enforcing company policies on playing local games such as Solitaire and Minesweeper or multi-player network games like Doom, Descent or X-Wing/Tie Fighter."

There appears to be a trend towards hybrid client/server monitoring. Two recent products, Actis Net Intelligence (see "Is this the end of corporate porn?", *The Register*, 19 April 2001) and Cerberian (see [http://deseretnews.com/dn/view/0,1249,250011010,00.html](http://deseretnews.com/dn/view/0,1249,250011010,00.html), Deseret News, 14 Feb. 2001) each include an "agent" that sits on the employee's PC and reports back to a server program. As noted earlier, many server-based products are not able to fully handle web pages encrypted with the https:// protocol, and having a small "agent" program on the PC would help with this too; for example, employee monitoring vendors might look into this approach as a way to defeat web anonymizers such as SafeWeb.

**Future trends**

Having speculated earlier in this paper that it might be natural for Microsoft to indirectly enter the employee-monitoring business by way of adding additional management features to its operating systems, and having just suggested a trend towards doing more client-based monitoring via "agent" programs, here are some other possible future trends in employee monitoring:

- As storage becomes cheaper and processors faster, "recording everything" becomes a realistic possibility.
- A "universal inbox" (all company documents are delivered as email or email attachments) would make it possible to record all company workflow.
- "Convergence" of office equipment (voice mail, fax, copier all accessible from the network) may provide a single "integrated" site for monitoring.
- On the other hand, "divergence" away from the PC into wireless devices will force employee-monitoring vendors to keep up, perhaps by putting monitoring software into wireless networks; there may also be a call for integration with location tracking (GPS).
- With at least fifty different employee-monitoring products on the market, there will inevitably be some industry consolidation. Already, SurfControl has acquired the CyberPatrol, SurfWatch, and LittleBrother products, and Emu Tech in Australia. Telemate.Net is being acquired by Verso Technologies.

**Conclusion**

The phrases "employee monitoring" and "workplace surveillance" evoke Orwellian images of Big Brother sitting at a central computer console, watching everything his employees do at their computers -- every keystroke or mouse click, every email message, every web page -- and responding to "inappropriate" usage the moment it happens.

Truly, as noted above, relatively inexpensive software now makes these capabilities cheap and potentially ubiquitous.

However, it's important to appreciate the differences among workplace surveillance programs. There is generally a trade-off between real-time monitoring (the employer can watch what the employees do, as they do it), on the one hand, and the ability to take a perfect picture of employee activities, on the other. Right now, ubiquitous, fine-grained employee monitoring is technically feasible but not a widespread practice. As noted above, most companies that even employ employee-monitoring software (and recall that they are still in a minority) use the server-based approach, which can be intrusive enough, but which doesn't have quite the intrusive capabilities of client-based monitoring.
There probably isn't much of a privacy interest in goofing off at work. But there is a privacy interest in not having exact recordings kept of precisely what you were doing while taking a break, while working, or even while goofing off.

**Bibliography**

*(Back to top)*

"1999 Utility Guide: Corporate Filtering" *(PC Magazine, May 4, 1999)* (extensive coverage of CyberPatrol for Microsoft Proxy Server, LittleBrother Pro, SmartFilter for Microsoft Proxy Server, SurfWatch@Work [Editor's Choice], WebSense)

Parry Aftab and Nancy Savitt (?), *Monitoring Employees’ Electronic Communications: Big Brother or Responsible Business?*

Ellen Alderman and Caroline Kennedy, *The Right to Privacy*, NY: Knopf, 1995 (pp. 275-320, 376-387 on "Privacy in the Workplace")

Lawrence Aragon, *E-Mail Is Not Beyond the Law*, *PC Week*, 6 October 1997 (role of IS departments in legal discovery)

Vijay Balakrishnan, *Why It Pays to Have a Network Usage Policy for Your Company*, Telemate.net, 1999

Doug Bedell, *Bye, Anonymous: Lawsuits surprise users of online pseudonyms as many seek to keep their identities hidden* *(Dallas Morning News*, 24 May 2001 (former employees)

Erik J. Belanoff and Evan J. Spelfogel, *Email: Property Rights vs. Privacy Rights in the Workplace*, Epstein Becker & Green PC, December 1999

David S. Bennahum, *Daemon seed: Old email never dies*, *Wired*, May 1999


Berkman Center for Internet & Society at Harvard Law School, *Digital Discovery*


Tom Brown, *Preservation: Analysis*, Harvard Law Digital Discovery (duty to preserve email)


"Computers and Work bibliography" (includes section on employee monitoring)

Andrew Conry-Murray, *The Pros and Cons of Employee Surveillance*, *Network Magazine*, 5 February 2001


Mark S. Dichter and Michael S. Burkhardt, "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age", Morgan, Lewis & Bockius LLP, 1999

Sean Doherty, *ESniff Noses Out Mischief Makers*, *Network Computing*, 25 June 2001 (lengthy review, not only of eSniff, but also of several other employee monitoring products: Elron Internet Manager, SurfControl SuperScout, Pearl Echo, and Trisys Insight)

Amitai Etzioni, *Some Privacy, Please, for E-Mail*, *New York Times*, Nov. 23, 1997 (even "communitarians" want privacy for employee email)

Susan E. Gindin, *Guide to E-Mail & the Internet in the Workplace*, 1999 (Only one section is available online; the full work is available from the Bureau of National Affairs)

Michael Hart, "An Employer's Staff Email and Internet Policy", Baker & McKenzie, London, 1996 (covers employee internet law in the UK, France, Italy, the Netherlands, Hong Kong, Japan, and the US)

Heather Harred, "And forgive us our trespasses: Agencies monitor employee Internet use to stem unauthorized surfing", Federal Computer Week, 5 Feb. 2001 (employee monitoring in US government offices)

"Internet Misuse in the News" (extensive set of links, put together by Websense, to articles on cyberslacking, cybermoonlighting, etc.)

Internet Product Watch, List of filtering & monitoring products

Larry Johnson, "Guerrilla Raids on the Honey Pot: Going Straight for Email", Fios, Inc., 2000

Tammy Joyner, "Big Boss is Watching", Atlanta Journal-Constitution, 25 July 2001 (GPS-based employee monitoring a key point in contract talks between BellSouth and the CWA).


Michael J. McCarthy, "Workers Return E-Mail Fire", Wall St. Journal, 26 April 2000 (Leinweber v. Timekeeping Systems; McLaren v. Microsoft)

Michael S. Moran, "Internet Access and Employer Risk", NY State Law Reporting Bureau (focuses on New York state law)


Privacy Foundation (US), Workplace Surveillance Project

Privacy International, "Technologies of Privacy", Privacy & Human Rights 1999 (has a long section on "workplace surveillance": performance monitoring, telephone monitoring, email and internet use monitoring, drug testing)

Janice Reynolds and Ellen Muraskin, "Logging, Monitoring Follow Call Centers", Computer Telephony, 1 May 2000

Proskauer Rose LLP, "Electronic Mail: Is It Labor's Latest Organizing Tactic?", August 1999 (NLRB)

Cheryl Buswell Robinson, "Surveillance and Nurses: The Use and Misuse of Electronic Monitoring", Research for Nursing Practice (location tracking via infrared and radio frequency)


James M. Rosenbaum, "In Defense of the Hard Drive", Green Bag, Winter 2001 (Chief Judge of US District Court for Minnesota questions the "uncritical acceptance" of the odd idea that just because a company owns a computer, they therefore have a right to examine all its contents)


Andrew Schulman, "The Extent of Systematic Monitoring of Employee E-mail and Internet Use", Privacy Foundation Workplace Surveillance Project, 9 July 2001

Andrew Schulman, "Fatline and AltaVista: 'Peer Pressure' Employee Monitoring?", Privacy Foundation Workplace Surveillance Project, 18 June 2001


Scott A. Sundstrom, "You've Got Mail! (And the Government Knows It!): Applying the Fourth Amendment to Workplace E-mail Monitoring", NYU Law Review, Dec. 1998 (mostly on public employees)


John Whalen, "You're Not Paranoid: They Really Are Watching You", Wired, March 1995 (covers employee theft, "time theft", etc.).

Jonathan Whelan, e-mail @ work, London: FT.com, 2000

Kenneth J. Withers, "Electronic Discovery Bibliography", 2000 ("... items relevant to the discovery of electronic evidence in civil litigation. This collection also includes subjects closely related to electronic discovery, such as electronic records management, computer forensics, the rules of evidence as applied to electronic data, and the use of e-mail in the workplace.")

Kenneth J. Withers, "Is Digital Different?: Electronic Disclosure and Discovery in Civil Litigation", 30 December 1999

Kenneth J. Withers, "Killing the vampire: Computer users, facing discovery, attempt to make the 'delete' key stick" Federal Discovery News

Anush Yegyazarian, "Nosy Bosses Face Limits on E-Mail Spying", PC World, September 2000 (NLRB)

Richard F. Ziegler and Seth A. Stuhl, "Spoliation Issues Arise In Digital Era", National Law Journal, 16 February 1998 (duty to preserve email and voice mail)