Big Brother At The Office: Friend or Foe?

Clint M. Satterwhite

Abstract

There are many aspects of employee monitoring that must be taken into account before determining if it is right for your organization. This paper outlines most of the issues and attempts to present an objective presentation of the information from both the employee and employer's perspectives. You will have to evaluate all of the available resources, weigh the benefits versus the disadvantages of monitoring and determine if it is right for your organization.

While monitoring is often times directed or led by the human resources departments of many organizations, network and security administrators generally carry out the orders. Security professionals can gain from monitoring by some of the possible benefits including: prevention of data theft and the reduction in the risk associated with employees visiting 'hacker', 'warez' and other questionable content websites.

Table of Contents

Do we really need monitoring?

The short answer is a resounding maybe.

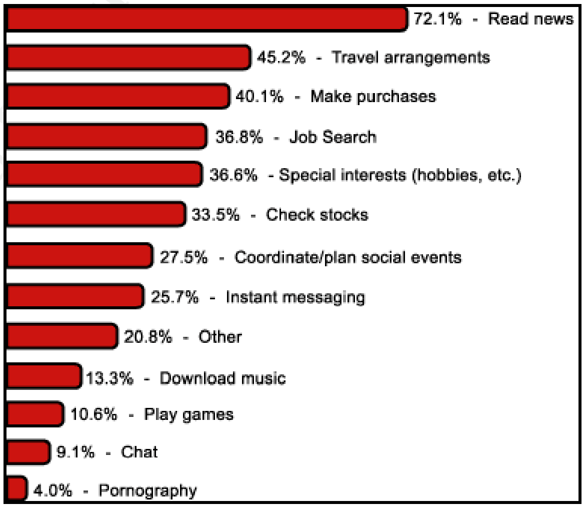
Now that we have that cleared up, let's outline some of the possible reasons for needing monitoring:

1. Employees tend to waste productivity when they are given access to the Internet. [1]
2. You may be paying for a substantial amount of wasted bandwidth due to non-business-related web sites and e-mail. [2]
3. Employers face a risk of sexual harassment cases when inappropriate materials are distributed via e-mail or viewed on their screens.[3]
4. Companies may incur losses and liabilities related to employee copyright and intellectual property violations. [4]

Wasted Productivity

Human nature leads us to be curious. The term 'surfing' is quite appropriate when you consider how the average American utilizes the Internet. With the number of domains worldwide growing from 3.3 million in January of 1998 to over 33 million in January of 2001[4], the possibilities of finding a site that will interest an employee is staggering. Since most non-business related sites are linked to each other, it is quite easy to unconsciously waste a large amount of time.

Non-work related Internet access at the office:



Source: Vault.com Internet Use Survey of 451 Employees, Fall 2000

At an average hourly wage of $14.29 per hour[5], the average American worker can easily cost their employers billions of dollars while casually surfing the Internet. According to Nielsen//NetRatings, the average Internet user spends around six hours and eleven minutes per week while at work versus only three hours and thirteen minutes per week while at home[6]. Why?

Generally, most corporate connections to the Internet are of higher speed than those at home. While this is slowly changing with the gradual proliferation of broadband connections to the general public, it may be too late to change the habits that American workers have learned over the past few years.

Finally, many workers have grown apathetic. Point in case: the mere existence of http://www.ishouldbeworking.com/. This website is devoted to slacking off at work and providing the needed resources to accomplishing that goal. This site averages 20,000 to 40,000 hits a day and has earned the creator between $35,000 and $40,000 a year in click-through revenue[7]. How is it that someone else can profit from an employee wasting paid productivity hours on your dime? Think about that for a while.

Lost Bandwidth

Bandwidth usage at the office historically was quite minimal for the average user. Inter-company e-mail, and remote reporting, job control operations and other low bandwidth operations were all that average users would have used corporate network connections for fifteen years ago. Today, we send twenty-megabyte sales presentations, large print-ready product brochures and other worthwhile business related items over our network connections. While these are all valid uses of the corporate network and it's Internet connection, there are many other non-business related activities which use just as much bandwidth.

In May of 2000, nearly 2 million people used almost 360 gigabytes of bandwidth in less than 25 minutes[8]. What was so important to cause such a large usage of bandwidth? Victoria's Secret premiered a web cast of their new product line, and they did it during normal business hours.

While audio and video files are entertaining, downloading them at work is a waste of company network resources. While the usage of Napster has decreased significantly since it's implementation of filters, it is a prime example of bandwidth intensive applications. Some companies have found that over 60 percent of their traffic was being generated by Napster[9]. Just because Napster appears to have become a non-issue, we should not assume that the next killer application isn't waiting around the corner to take its place. Years before Napster was around, there was the streaming 'push-technology' application PointCast.

AdCritic.com is another entertaining, yet wasteful bandwidth hog. If you are in the advertising profession, you probably have a valid reason to go to their site during business hours. However, with over 100,000 unique visitors a day, imagine how many of those could be your employees.

Day trading, and stock watching has become an obsession with many Americans. Besides the possible health risks associated with day trading such as nervous fits, outbursts of obscenities and the urge to jump out of windows, it can also consume a lot of bandwidth. Most real-time financial tracking applications require a 56Kbps modem connection as the absolute minimum. Most state that ISDN, Cable or DSL are preferred to ensure current information. We can assume that users are going to turn on all of the bells and whistles in the application because they have you to thank for providing them with a large connection to the Internet. If the application averages 56Kbps, just 24 users could saturate your T-1 line. What happens then? You get lots of angry phone calls because people can't access the Internet to watch their children on the day care's web cam[10].

Sexual Harassment and Libel

There have been a number of highly publicized cases over the past few years that have brought the importance of monitoring employee communications to the forefront. A few of these examples are cited in the following paragraphs.

A Federal court in New York allowed a case, which was based on racist e-mail distributed by employees, to be called as a class-action discrimination suite. The plaintiffs were seeking $60 million in damages[11]. While settled out of court in a confidential agreement, this case no doubt cost Morgan Stanley & Co. a lot of money in legal fees, bad press and the actual undisclosed settlement.

Newsweek reported that Chevron settled a sexual harassment lawsuit for $2.2 million based on e-mail postings including: "25 reasons why beer is better than women" [12].

A long-time employee of a major insurance company was fired for "gross misconduct". When an e-mail stating the reason that the employee was distributed to associates of the employee, it was then in turn forwarded to others. The former employee was able to bring suit against the insurance company and received over $1.25 million in compensatory and punitive damages based upon a defamation claim[12].

The New York Times dismissed 23 employees at a Norfolk, Virginia Administrative center on November 30, 1999 at a cost of over $1.9 million, for violating the company's e-mail policy. Cited were "offensive or disruptive messages, including photographs, graphics and audio materials." [13]

Copyright and Intellectual Property

Software piracy can cost a company thousands, or even millions, of dollars in penalties and legal fees. The Software & Information Industry Association (SIIA) actively files legal suits against companies and individuals suspected of software piracy. Violations are subject to a maximum penalty of $150,000 per software title infringed. For this reason alone, it is important to inventory PCs for software that has been installed, and prevent access to 'Warez' sites where commercial software may be illegally downloaded.

Because of decentralize purchasing, autonomous accounting practices and an unfortunate acceptance of software piracy among many employees, many users may be more aware of the problem than management. The SIIA provides a simple, anonymous way to report violations on their website[14]. This has become a favorite site for disgruntled ex-employees.

You should also be concerned with copyright and intellectual property as it relates to your own property, and that of customers and vendors. In order to conduct daily business, we often engage in non-disclosure agreements. Many organizations require that candidates sign these agreements before becoming employees. While having a policy in place is an absolute requirement, it becomes worthless if it is not enforced. The only way to enforce a policy is to monitor the activity of the concerned parties.

What harm can come from monitoring?

If all of the above arguments can be made for using monitoring, why shouldn't you just go ahead and do it?

Well, the primary disadvantage is the loss of morale that is created by monitoring activities. Monitoring activities convey a sense of mistrust. Many workers can become nervous, overly fatigued, and experienced various other physical and psychological problems due to monitoring. S.A.M. Advanced Management Journal cites some examples as follows[15]:

> *Disadvantages for Employees*
>
> *Although the advantages are important and helpful to employees, the disadvantages that go along with employee monitoring may outweigh the benefits. While employers argue that monitoring is an inexpensive way to increase productivity and customer service, others argue it is really the modern method of exerting control and power over labor. Monitoring has been used to determine pay and promotion decisions as well as to reinforce disciplinary actions. The AFL-CIO objects to monitoring because it "invades workers' privacy, erodes their sense of dignity and frustrates their efforts to do high quality work by a single-minded emphasis on speed and other purely quantitative measurements" (Lund, 1992, p. 54).*
>
> *Objections to computer monitoring include the issue of privacy. Monitoring is intrusive and the potential for abuse exists. For example, computer data banks, telephone and video monitoring, active badges, and other monitoring techniques make the private lives of workers easier to delve into without detection. Data concerning employees' security clearance, computer applications preferred, right/left handedness, and "even how the user takes his coffee" can be maintained -- which go beyond how an employee is performing on the job (Levy, 1993, p. 3). How information gathered on employees will be used and who has access to it are questions at the center of the debate. Technology has made it too easy to gather private information and to potentially use it against the employee. For example, information can be used to discriminate or retaliate against employees by using it "to identify or harass whistleblowers, union organizers, or other dissidents within a firm or agency" (U.S. Congress, 1987, p. 2). Private information may also find its way to co-workers or prospective employers.*
>
> *Other objections center around the question of fairness in how the*

monitoring is implemented, whether the standards are viewed as reasonable, whether the information gathered is work-related and necessary, and, finally, the effects on employees ' quality of work life (Levy, 1994). The creation of "electronic sweatshops" leads to unneeded employee pressure and stress. Stressful working conditions related to monitoring include a heavy workload, repetitive tasks, social isolation, fear of job loss, and a lack of job involvement and personal control (Levy, 1994). In a study of worker stress for the Communication Workers of America, Smith (1992, p. 21) indicated that "the monitored employees reported higher workload, less workload variation and greater workload dissatisfaction than the unmonitored employees. The monitored employees also reported less control over their jobs.., less fairness of their work standards and more frequent interactions with difficult customers."

These pressures and stressors have also been considered a major contributor to employee psychological and physical health complaints. In the Smith (1992) study above, monitored workers indicated more somatic health complaints, such as stiff/sore wrists; pain/stiffness in the shoulders, arms, legs, neck, and back; racing heart; acid indigestion and stomach pains; headaches; depression; severe fatigue/ exhaustion; extreme anxiety and high tension. "At AT&T, where computer monitoring is used extensively, at least 25% of the workforce is involved in job counseling for work-related emotional disorders" (Pai, 1997). In another example, a TWA reservation agent who has worked for the same company for 30 years says things have drastically changed. The reservation agent said that after years of stress from constant monitoring, her work and health suffered. She commented that, "I suffered nausea, severe sleep disturbance, weakened eyesight, mental confusion, headaches, muscle aches, exhaustion, and lymph node pain" (Worsnop, 1993, p. 1025). In addition, a study by the University of Wisconsin's Department of Industrial Engineering concluded that "electronic monitoring was seen as a major cause of psychological and physical health complaints among workers" (Worsnop, 1993, p. 1025). "Monitoring makes us feel like prisoners hooked up to a computer; mistreated, guilty, paranoid, enslaved, violated, angry, and driven at a relentless pace" (Worsnop, 1993, p. 1025).

There are also cases known as "bathroom break harassment" where workers' stress becomes unbearable because employees fail to take needed bathroom breaks out of fear of termination. In one example, a telephone service worker suffered a nervous breakdown (9 to 5, 1986). In another example, a United Airlines' employee was threatened with firing when her supervisor told her she went over her

> *allotted time while she was in the bathroom and coworkers had to take extra calls to make up for her "abusive" work habits (flight reservationists are permitted 12 minutes for bathroom breaks during a 7.5 hour period) (9to5, 1986). The National Association of Working Women summed it all up by saying, "the work lives of monitored employees can be characterized by three words: invasion, stress, and fear" (Worsnop, 1993, p. 1013).*

Having a bunch of employees that think you are out to get them, are watching their every move, and generally don't trust them is not a very enjoyable way to run a business. If you were in a communist country and could shoot employees for disloyalty, this may work, but not in America.

With all of the things that companies do to lure employees to their organization including benefits, hiring bonuses, perks and stock options, it only makes sense to make the work environment as employee-friendly as possible. Monitoring can be done while maintaining a sense of pride in the workplace. How? Read on.

How to monitor

It is possible to monitor everything an employee does from the time they enter company property to the time they leave, but it is not practical, and as you have read earlier, can cause serious side effects.

Policies

You must consider what is most important to you. Like establishing a good security plan, you must first determine what to set as your objectives. Generally, you are attempting to safeguard the well-being of your employees, maintain efficient productivity levels and protect yourself from un-due financial hardship.

Your policies should state in clear terms what you will monitor, what is considered inappropriate usage and what corrective actions will be taken. Do not take the approach of '…we're going to get you… so keep your noses clean…". Your policies will be better received if they are presented in a manner that explains how the employee can benefit and how the company (and therefore the source of their livelihood) can benefit.

Area managers, not just executives, should present the policies. If the employees cannot see that their direct supervisors are going to embrace the policies, it is unlikely that you can expect much more from the employees themselves.

It is critical that you enforce the policies without prejudice, and in a completely objective manner. If you, or an employee, are ever forced to resort to legal action, and the employee can prove that the policies were not enforced across the board, you will lose. If an employee sees that the policies are always enforced, they will be much more likely to follow their guidelines.

E-Mail

E-mail can be monitored, logged and filtered by a number of products. One such product, SuperScout E-Mail Filter from SurfControl, can provide various levels of protection for your company. The capabilities of SuperScout are pretty representative of other products on the market. For that reason we will cover it's features for simplicity sake: [16]

> ***Increase Security***
>
> *Provides Anti-Virus Scanning at the Gateway - Use your current anti-virus solution, giving you the choice of best of breed products, for enhanced virus protection.*
>
> *Prevents Confidential Data Loss - Block, isolate, or delay until*

approved, the unauthorized transmission of email containing intellectual property or other confidential data.

Implement Encryption Policy - Block, isolate, allow, or strip desktop encrypted messages from unauthorized personnel within the organization.

Limit Legal Liability

Prevent Sexual Harassment - Provide a safe and productive work environment for employees, by filtering out offensive/inappropriate email from the Internet.

Avoid Libel Litigation - Protect company image and liability with corporate disclaimers, where appropriate, or by preventing internal users from sending offensive or otherwise inappropriate email to the outside world.

Improve Productivity

Enhance Email Server Productivity - Schedule non-essential email to transmit after normal business hours, ensuring priority to business-critical email during the workday.

Improve Employee Productivity - Prevent spam and other junk email, as well as minimize, delay, or discourage excessive personal use of email depending on your organization's specific email policy.

Other products in this category include:

2. MailMarshal from Marshal Software – http://www.mailmarshal.com
3. MIMESweeper from Baltimore Technologies – http://www.mimesweeper.com
4. eSafe Mail from Aladdin Knowledge Systems – http://www.ealaddin.com
5. Mail essentials from GFI Communications – http://www.gfi.com
6. ScanMail and ScanMail eManager from Trend Micro – http://www.antivirus.com
7. Mail-Gear from Symantec – http://www.symantec.com
8. ES2000 from 8e6 Technologies – http://www.8e6technologies.com

Web Surfing

The web has everything. If you don't think so, try to think of any obscure or dark subject and enter it into a search engine like http://www.google.com and see how many hits you get. Here are a few interesting statistics:

Websites[17]:

Warez – 613,000 Google results

Sex bondage – 1,100,000 Google results

Phreaking – 57,700 Google results

Serial number generator – 81,500 Google results

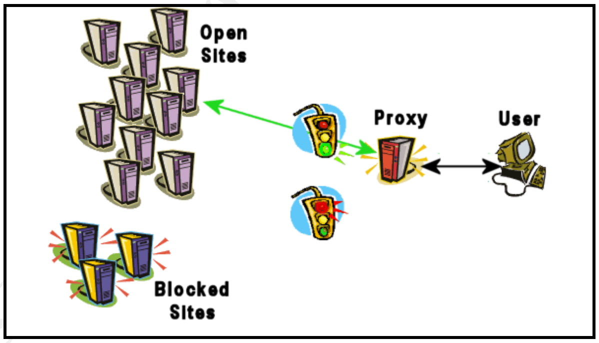
Newsgroups[18]:

Hack – 83 newsgroups

Erotic – 553 newsgroups

Binaries (files excluding erotic) – 449 newsgroups

Several companies offer software that will filter content based upon keywords, MIME file types, URL or IP address or category. Many offer a subscription service that keeps the database of websites with questionable or inappropriate contents up to date automatically. Most of these products are installed on a dedicated server, which acts as a proxy for the user.



How a proxy works: When a client system requests access to a resource, it makes the request to the Proxy rather than directly. The proxy can then determine if it is acceptable based upon rule-sets. If it is, the proxy handles all transactions. The client never directly contacts the destination.

Some of the currently available products in this category include:

1. SuperScout Web Filter by Surf Control – http://www.surfcontrol.com
2. AllegroSurf from RhinoSoft – http://www.allegrosurf.com
3. N2H2 Filtering from N2H2 – http://www.n2h2.com
4. I-Gear from Symantec – http://www.symantec.com

5. Various products from WebSense – http://www.websense.com
6. R2000L from 8e6 Technologies – http://www.8e6technologies.com
7. LANguard from GFI Communications – http://www.gfi.com

EVERY KEYSTROKE???

This is the extreme. There are a few instances where this may have legitimate usage. One case would be in a word or data processing operation when key-entry speed and accuracy verification is an important measurement. This type of information could be used to facilitate employee evaluations.

Is this legal? Generally, yes. If you decide you need this level of surveillance, be sure to perform it across the board, not selectively. Also make sure that you indicate the practice in your policies. There are a couple of groups which may be exempt from keystroke monitoring: certain union members and public sector employees[19].

Employee and human-rights organizations scrutinize this type of monitoring heavily. As with any of the monitoring techniques outlined in this document, seek legal counsel before implementing any policies or practices.

Due to the sensitive nature of keystroke monitoring, a listing of available products will not be provided here. Reputable companies produce some of these products, while others are developed by obsessed spouses intent on catching their mates in some lurid activity. Products can be found by searching for 'keystroke monitoring' in your favorite Internet search engine.

Employee Rights

There are a number of organizations that provide guidelines, arbitration and other assistance to employees when they have cause to believe their privacy rights have been violated.

Center for Democracy and Technology
1634 I St. N.W. #1100, Washington, DC 20006.
Voice: 202-637-9800.
Fax: 202-637-0968.
E-mail: info@cdt.org
Web: www.cdt.org

Computer Professionals for Social Responsibility
P.O Box 717, Palo Alto, CA 94302
Voice: 415-322-3778
Fax: 415-322-4748
E-mail: cpsr@cpsr.org
Web: www.cpsr.org

Electronic Frontier Foundation
1550 Bryant Street #725, San Francisco, CA 94103
Voice: 415-436-9333
Fax: 415-436-9993
E-mail: eff@eff.org
Web: www.eff.org

Electronic Privacy Information Center
666 Pennsylvania Ave. SE #301, Washington, DC 20003
Voice: 202-544-9240
E-mail: info@epic.org
Web: www.epic.org

Privacy Rights Clearinghouse
1717 Kettner Ave. #105, San Diego, CA 92101
Voice: 619-298-3396
Fax: 619-298-5681
E-mail: prc@privacyrights.org
Web: www.privacyrights.org

National Work Rights Institute
166 Wall St.
Princeton, NJ 08540
(609) 683-0313
Web: www.workrights.org

9 to 5, the National Association of Working Women
231 W. Wisconsin Ave. No. 900
Milwaukee, WI 53203
(414) 274-0925
Hotline (800) 522-0925
Web: www.9to5.org

National Employee Rights Institute
414 Walnut St., Suite 911
Cincinnati, OH 45202
(800) 469-6374
Web: www.nerinet.org

American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004-2400
(212) 549-2500
Publications Ordering: 1-800-775-ACLU (2258)
Web: www.aclu.org

Conclusion

Should you use monitoring and filtering techniques in your environment? Based on the our current society, the proliferation of legal action, the age of political correctness and many other factors, the answer seems to be yes. There are many more legal aspects that should be examined. You should seek legal advice from a professional with experience in the area of employee surveillance and privacy rights. You should clearly define policies. You should ensure that your employees understand and agree to the policies. You should enforce the policies with fairness and without bias. Pick a suite of products that will allow you to maintain the effectiveness of your policies. If you add a bit of luck, your company should be able to successfully live with surveillance in the digital age.

References

1 – Seminerio, M., Nov. 29, 1999, “Content Filters Don't Just Spy Risqué Surfing”, *PC Week*, 73, http://www.zdnet.com/eweek/acrobat/1999/99pcweek/nov29mb.pdf.

2 – UNCREDITED, unknown, “Reducing the Risks of Internet Abuse with Internet Usage Management Solutions”, *NetSpective.com*, http://www.getnetspective.com/pressroom/whitepapers/stopwatch.asp.

3 – Beall II, R.; Lynch, M., 2000, “READ MY MIND - THE PERILS OF SURFING THE WEB AT WORK”, *Sheppard Mullin Richter & Hampton LLP*, http://www.smrh.com/Publications/PublicationDetail.asp?PublicationID=123.

4 – Duree, D., 2000, “INTELLECTUAL PROPERTY – INTERNET”, *Trademarks, Copyrights and the Internet*, http://www.ipilaw.net/.

5 – USDoL, 2001, “Average hourly earnings of production or nonsupervisory workers on private nonfarm payrolls by industry, seasonally adjusted”, *Bureau of Labor Statistics, U.S. Department of Labor*, http://stats.bls.gov/webapps/legacy/cesbtab4.htm?H5.

6 – Nielsen//NetRatings, July 1, 2001, “Weekly Web Usage, United States”, *Nielsen//NetRatings*, http://www.nielsen-netratings.com/hot_of_the_net.htm .

7 – Vault: Internet, September 1, 2000, “Daytime Surfing, News & Research”, *Vault > the insider career network™*, 3, http://www.vault.com/nr/newsmain.jsp?nr_page=3&ch_id=263&article_id=19333&listelement=1&cat_id=1181.

8 – Lantech, September 1, 2000, “Managing Responsible Internet Usage”, *Lantech of America, Inc.*, http://www.ltoa.com/netaccessmgmt.htm.

9 – 8e6 Technologies, date unknown, “Internet Access Management White Paper”, *8e6 Technologies*, 2, http://www.8e6technologies.com/solutions/white_paper_hr.pdf.

10 – JM Technology Solutions, date unknown, “How it works”, *Daycare Webcam*, http://www.daycarewebcam.com/.

11 – Owens and Hutton v Morgan Stanley & Co., INC. Case no. 96 CIV 9747, http://www.contilaw.com/articles/owensvmorgan.html.

12 – Adler, Jerry, “When e-mail bites back”, *Newsweek*, Nov 23, 1998.

13 – Staff Writer, Dec 1, 1999, “Times Company Dismisses 23 Over E-Mail”, *The New York Times*

14 – The Software & Information Industry Association, “Report Piracy”, http://www.siia.net/piracy/report/default.asp.

15 – Mishra, Jitendra M.; Crampton, Suzanne M., Summer 1998, “Employee monitoring: Privacy in the workplace?”, *S.A.M. Advanced Management Journal*, Vol. 63 Issue 3, p4.

16 – SurfControl, date unknown, “SuperScout E-Mail Filter, Managing Content Security”, *SurfControl Products for Business*, http://www.surfcontrol.com/products/superscout_for_business/email_filter/index.html.

17 – Keyword search results, http://www.google.com.

18 – Newsgroup search from publicly available groups master list downloaded from AT&T@Home service.

19 – Privacy Rights Clearing House, April 2001, “Fact Sheet 7: Privacy in the Workplace”, http://www.privacyrights.org/fs/fs7-work.htm.