

## Article

### Worker Beware

#### Why Employees Should Be Careful About What They Do With Their Workplace Computer

That hot website you've been looking at while surfing on the Internet may be giving your employer just the information they need to terminate you. Workers today should know that everything they do with their work computer is subject to scrutiny. Technology exists to provide companies an unparalleled ability to monitor employees day to day, minute-to-minute actions.

"I had no idea that my employer was watching my every move on my computer. I thought I was protected from being terminated, since my last few reviews all had high marks. Because I used my computer for personal use, my employer had just the ammunition they needed to fire me without severance. I know they did this because times are tough, but it really stinks that I wasn't even able to claim unemployment. This experience will really make me think twice about ever using my workplace computer for personal business."

— Name not disclosed.

#### Proxy Server / Firewall Usage Reports

Most companies today utilize a proxy server/firewall that provides convenient reporting showing aggregate website visits, time spent at each site, and other information relating to surfing the web. These reports are limited in tracking the specific information passed from the desktop client to the website and back, but can be indicative of potential sources of computer abuse.

Accordingly, most companies will perform periodic audits system wide to determine if any employee is abusing popular sites that have nothing to do with business. Sites such as members.aol.com, or mail.yahoo.com may be checked to see if an individual is spending a significant amount of time on entertainment or shopping websites. Employees should not make assumptions about what permitted uses are for work computers; otherwise they might find themselves in a termination situation. In most

cases, employers tolerate a reasonable amount of use of computers for personal usage, but this is generally restricted to the lunchtime or other break time established by the employer.

## Corporate Email Monitoring

Ever since Enron's collapse, email monitoring has captured headlines in the news. Companies today can create agents that scout through corporate mail servers looking for email containing content or keywords that are classified as sensitive. This can relate to everything from sensitive contracts, to adult-oriented material. When the email agent finds an instance of such word or phrase, the administrator is alerted to check the email. Other methods of email monitoring that exist include, Pop account mirroring, periodic mail file system scans, and many others.

## Computer Forensics

Computer Forensics relates to tracking the digital footprints that exist in electronic messages to determine information relating to the source, create date, method of transmission and various other META data relating to usage of computers for communications and work. In some cases, workers leaving companies have attempted to steal sensitive information such as prospect lists, proprietary secrets or other corporate assets. Companies today can bring in computer forensic experts to reconstruct what actions took place on a computer. Even if a computer has been reformatted completely, it is still possible to reconstruct the original information and determine the state of the computer prior to its modification.

## Employee Computer Surveillance

Surveillance monitoring involves installing software on a desktop machine that resides undetected but captures information specific to the computer's usage. This enables employers to create employee profiles based upon an employee's entire work day. Information captured includes text transcripts of input devices used, such as keyword keys, or mouse motion and click usage rates. Surveillance monitoring can allow employers to see personal emails accessed outside of the corporate email system.

In one case, an employee of a company used their AOL account to email contact lists to a competitor. Because the employee used their personal account while at work, they gave up some of their personal privacy rights as it relates to their personal email account. Employees need to presume that if they can see it on their monitor, then so can their employers.

## Packet Sniffers

Packet sniffers are tools used to monitor information transmitted by a computer on a specific port, such as 5190, the port used for AOL instant messaging. A packet sniffer can log all text conversations, the IP address that identifies the internal computer user, along with the text transcripts of conversations, all without any modifications to any of the computers on a business network.

In fact, there have been cases of corporate espionage, whereby a computer is plugged into a private network to log transmissions on specific ports, including those that transmit email. If a technical individual knows the IP address of your corporate LAN that is exposed to the Internet, this individual could monitor all email and instant messaging communications via a port sniffer from outside the internal network.

## Conclusion

The law is very much on the side of the employer regarding privacy disputes relating to business property use. Employees should presume that anything they type or receive might become subject to discovery in the case of termination, promotion or lawsuits. Employees need to be smart and anticipate how their supervisor or a court of law might interpret their behavior. In general, it is recommended not to do anything with your computer that you wouldn't do publicly at a company presentation. Employers everywhere have begun instituting computer productivity monitoring.

Usually, these actions are not publicly discussed or known by the employees. Note the following case in point:

"My colleague and I used to use AOL to IM (Instant Messaging) each other to discuss who we thought was attractive in our office. When Marcia was let go because of the recent cut backs, she sued the company on the basis of sexual harassment and won because of Instant Messaging traffic log monitoring that had been installed on the corporate network. These logs were subpoenaed by her attorney to help her prove sexual harassment. Unfortunately, I lost my job because I was part of those IM conversations"

— Real name not disclosed.

## What About Business Property Used At Home?

Another area of perceived privacy by employees is in the area of corporate-owned laptops used from a personal dwelling. The courts have upheld the rights of corporations to hold employees accountable for inappropriate use of their business computer when used at their personal dwelling. This may pose serious problems for some who use their work computer for personal dating or other personal entertainment endeavors.

Employers frequently use this information out of the courts to get employees to agree to leave without the threat of litigation or at reduced severance payouts. In most cases, the employer does not want internal or external publicity relating to their usage of advanced monitoring tools. Because of this, most employees do not suspect their actions might result in public scrutiny.

Employees everywhere need to be informed and protect themselves and their companies against potentially harmful allegations. Keeping business separate from personal endeavors is a good first start. Limiting usage of business-owned property to conform to your work place policy is a must.

If you have not read your employee handbook, request a copy. Those who notice a lack of a stated computer usage policy should request one in writing if in doubt. This can help protect the employee and employer from any potential disputes.