SheppardMullin

Articles

Read My Mind - The Perils of Surfing the Web at Work

06.26.2000

As more employees obtain desktop Internet access, employers must balance potential liability and loss of productivity issues against the employees' rights to privacy. Internet abuse at work is a serious problem. "The most commonly abused Web sites at work are porn," says Dr. David Greenfield, with the Center for Internet Addiction in West Hartford, Conn. According to the June 12, 2000 issue of Business Week, as much as 70% of the traffic on pornography sites occurs during working hours. Sex Tracker, a service that monitors Internet traffic to adult sites claims one in five white collar male workers are accessing pornography at work.

Not surprisingly, pornography is not the only Internet abuse in the workplace. A survey by Internet Analysts International Data Corporation reveals that 60% of all on-line purchases are made during working hours, and 40% of all Internet surfing performed at work is not work related. The June 12, 2000 edition of the Express reports that the average office worker with Internet access spends one to two hours per day browsing the Web to trade stocks, look at pornography, play games, chat, look for other employment, or perform other non-work related activities on the Web.

Employees are also discovering on-line music. With the advent of Napster, a service that creates a virtual forum for Internet users to share their often pirated music with each other, employee productivity, as well as network bandwidth, suffers. According to a Media Matrix study, 335,000 at-work employees visited Napster.com during the month of March alone.

What is the cost of all this, you ask? Websense, the maker of Internet monitoring software, estimates that employee abuse of the Internet costs employers $54 billion annually. Despite the magnitude of the problem, experts estimate that nearly one-half of the Fortune 100 companies have yet to adopt adequate Internet usage policies. Employers' reluctance to adopt stringent policies may be attributable, at least in part, to the fear of alienating privacy sensitive employees in a tight labor market.

In response to employee Internet abuses, an increasing number of employers are installing web-monitoring software. Using this software, management can block employee access to categories of Web sites. More troubling from a legal and ethical standpoint, management can choose instead to passively monitor corporate network traffic and log employee activities based upon parameters chosen by management. Many of these packages record e-mail sent and received; some will even record the very thought processes of employees by capturing employee keystrokes, including the ones that are deleted. By generating a report, management can discover whether an employee is, for example, spending long hours looking at pornographic websites, checking stock quotes regularly, looking for another job, or selling company secrets.

Many civil rights activists express concern that employee monitoring is yet another example of infringement of employee privacy. Employers, in response, argue that uncontrolled or unmonitored Internet access not only wastes corporate resources such as employee time and network bandwidth, but employee behavior which may be inappropriate for the workplace environment potentially exposes the employer to legal liability for sexual harassment.

Although the most well known of all privacy protection laws, the Fourth Amendment to the U.S. Constitution, guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," the Fourth Amendment does not apply to non-government actors such as private employers. The California Constitution in article I, section I, however, does. It provides that: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." In the seminal California case, Hill v. NCAA, the Supreme Court held that article I, section I of the California Constitution applies not only to the government, but to private actors as well, including employers. The Court in Hill also enumerated a test to determine whether an invasion of privacy has occurred. An employee alleging an invasion of privacy in violation of the California Constitution must establish all of the following: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; (3) conduct by defendant constituting a serious invasion of privacy. California also protects all citizens, including employees at work, from illegal wiretapping and eavesdropping. Under Penal Codes § 631 and § 632, it is a crime for any person to, intentionally and without the consent of all parties, eavesdrop on or record a confidential communication by means of any electronic amplification or recording device.

As related to computer usage, in the few unpublished superior court decisions relating to e-mail, California courts have refused to apply either the California Constitution's guarantee of privacy or California's anti-wiretapping law to employee monitoring efforts.

One might distinguish monitoring e-mail from monitoring Internet usage on the grounds that an employee's use of the Internet has a greater expectation of privacy than an employee's use of e-mail sent through the company's computer network. While e-mail involves a two-way conversation, Internet browsing is more like reading a magazine behind closed doors. Monitoring Internet use by employees would enable an employer to gather information concerning the employee's personal interests and subjective thought processes.

Courts have not yet drawn such a distinction. In a recent Fourth Circuit Federal criminal case, the first of its kind, a court upheld a government agency's right to monitor the Internet usage of its employees. In United States v. Simons, Mark Simons, a government employee was charged with receiving illegal child pornography over the Internet while at work. His activities were discovered when a network specialist, monitoring Internet employee usage from a remote location, discovered that Simons visited a large number of pornographic websites. After the supervisor had the contents of the employee's computer downloaded and discovered files containing illegal child pornography, the employee was arrested.

In upholding the monitoring and remote search of Simon's computer, the Fourth Circuit stated that in light of the agency's Internet usage policy, which clearly stated that the employer would "audit, inspect and/or monitor employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages as deemed appropriate," Simons lacked a legitimate expectation of privacy in his Internet usage in light of the government policy.

If California courts accept the reasoning of the Fourth Circuit -- and it seems likely that they will -- a court would probably find that the use of Internet monitoring software is neither an invasion of privacy under the California Constitution nor a violation of California's anti-wiretapping or anti-eavesdropping laws. This would be especially true if the company has a clear policy regarding the Internet usage.

An employer wishing to maximize its chances of winning a lawsuit should have a specific Internet and electronic communication policy which not only advises employees that the corporate computers and network resources are to be used solely for company business, but also that the employer reserves the right to inspect and monitor employee usage of the Internet. For employers who choose monitoring, this approach increases the chances of successfully defending claims asserting violations of California's right to privacy or California's anti-wiretapping, anti-eavesdropping laws.

Practice Areas

Litigation