

Legal Liabilities of Employee Internet Use

Table of Contents

Overview.....3

Employee Privacy3

Sexual Harassment and Discrimination.....4

Child Pornography.....4

Internet Security.....4

Conclusion.....5

About The Author.....5

About Burstek.....5

Legal Liabilities of Employee Internet Use

Overview

Almost every employer provides its employees with Internet access on the job. This indispensable tool contains the seeds of business growth as well as business destruction. Most employers have already learned the importance of protecting their IT investment from technical threats presented by viruses, hackers, blended threats and SPAM. However, because of its human interface, Internet security involves more than a good firewall or antivirus software. That same employee who might accidentally download a virus is also a target, or even a source, of other insidious human -based infections, including illegal activity. As with all such challenges, the first step is to recognize the problem.

The notion that laws do not apply to the “free” Internet entered society almost as rapidly as the love of the Internet expanded. This freedom has been tested in the areas of music and movie downloads, among others. Closely related to this notion of freedom is the idea of privacy. These notions are dashing against the hard rocks of reality, and the pounding of this surf continues as courts and legislatures around the world are being asked these questions. Generally, the answers are consistent with legal concepts developed before the Internet. At the same time, the variations of human activity which are having negative impacts on employee access to the Internet have a uniqueness that makes them seem overwhelming sometimes. The following is a brief description of some of the legal issues raised by employee access to the internet on company -owned computer networks.

Employee Privacy

The suggestion that an employee has an expectation of privacy in email conversations created and stored on an employer’s computer network has been pretty much put to rest. As early as 2001, the American Management Association reported that three-quarters of its firms regularly monitor, record, and review employee emails and computer files. Courts agree that it is now a “social norm” that employees are not entitled to expect privacy in the use of workplace computers. It has been found that the employer’s interests are reasonable and deserve protection. Ownership of the equipment is not the sole reason. On-the-job misuse of computers poses significant dangers in terms of diminished productivity and employer liability. There is also a growing use of written “ [Acceptable Use Policies](#) ” by savvy employers. A well written AUP will explain to the employee in clear language that there is no expectation of privacy. Such [AUPs](#) may even allow some private use of the employer -provided internet access, but such use is typically subject to the employer’s right to monitor its employees’ files, and inspect website usage and emails. In the U.S., laws controlling electronic eavesdropping vary from state to state, but it can generally be said that an employer who obtains the employee’s acknowledgment or consent regarding the monitoring of electronic communications will be safe from claims under such laws.

Legal Liabilities of Employee Internet Use

Sexual Harassment and Discrimination

Pornography has produced many Internet millionaires and accounts for a significant percentage of all Internet activity. Think of the number of jokes and digital videos that get passed without a second thought from one buddy list to the next. The presence of Internet -based porn or racial slurs in the workplace has ramifications well beyond lost productivity. The concern here is creation of a workplace environment of sexual harassment or discrimination that exposes the employer to liability. If a female reports that a male coworker is viewing porn on company computers, even a basic HR policy will require the employer to take immediate action. This makes it essential for employers to be vigilant, not only to prevent harassment, but to address the conduct and avoid or minimize legal liability. Evidence offered in discrimination and harassment suits has ranged from improper wallpaper/screen saver images to offensive jokes. This potential proof of a hostile work environment can turn the "free" email into a steeply expensive harassment or discrimination lawsuit. Prevention is the best way to avoid these risks and expenses. The case law suggests that a clear AUP and other affirmative steps, such as [security blocking and reporting software](#), provide evidence of an employer's good faith and lack of harassment that can help defeat claims that arise out of a rogue employee's misuse of the internet. Software that monitors employee Internet and email use is an excellent liability prevention tool, and is recommended by the American Bar Association Section of Business Law.

Child Pornography

Most AUPs have a general prohibition against illegal activity. Unfortunately, child pornography is a specific form of illegal activity that merits special mention in your AUP. In the U.S and other countries, politicians are promising to boost child pornography enforcement efforts. Law enforcement agencies at all levels are getting involved. Local sheriffs are arresting people through Internet sting operations. Current laws in every U.S. state impose a strict duty to report child pornography, and an employer who discovers it has to act instantly. A company in New Jersey noted suspicious activity, but failed to pursue an inquiry and was later found partially liable for an employee's child pornography activities. Obviously, there is a line to walk between over-zealous monitoring and employee culture. There is no doubt, however, that the discovery of child pornography usage on company IT resources imposes a duty to investigate and report, regardless of what the company's AUP may or may not say.

Internet Security

This topic involves more than protecting your network from viruses, hackers, adware, spyware, or an inundation of unwanted SPAM. Many employers have a legitimate concern about employees trafficking improperly in trade secrets or other confidential information. Patient records protection in the health care industry is only one example. Organizations concerned with such proprietary information as customer lists, product and service pricing, even growth strategies for the next year, or negotiation strategies on obtaining a competitive bid should take note: [Monitoring employees](#) is even more important now that such information is so easily accessible and so easily transmitted. This does not mean you will have to inspect each employee's key chain flash drive at the end of every workday. Fortunately, software exists that can help prevent this activity from occurring in the first place, and can automatically put employee activity reporting directly into management's inboxes so that behavior can be managed. This type of behavior should not be ignored, and employers should understand that they have the right to monitor it and enforce their zero tolerance policies.



Legal Liabilities of Employee Internet Use

Conclusion

A well-written AUP is a good first step, and the right filtering and reporting software are indispensable, but as with many employer initiatives, the key is management commitment. That commitment does not have to be expressed in militaristic or oppressive terms. After all, company culture is an important ingredient to business success and Orwellian policies may not be accepted, much less followed. The best AUP will include the involvement of key department heads and leaders within your organization in addition to your legal department or counsel in order to customize it to your organization's culture and business needs. Employee education and communication of your Acceptable Use Policy are critical. Employees obviously need to buy into the policy and understand its reasons and its fairness. This has the added effect of eliminating employee expectations of privacy. The employer does not have to turn employees into spies. The goal is the same as any other proper workplace policy – proper behavior has a sound purpose, and misbehavior is not allowed, not only because of its impact on profits and productivity, but because what is wrong should not be tolerated.

Burstek offers a free white paper on [creating Acceptable Use Policies](#).

About the Author Jim Lussier



James R. Lussier is a Shareholder, at Mateer Harbert, P.A. located in Orlando and Ocala, Florida. He practices Intellectual property law, corporate law and civil litigation. Jim is a third generation Floridian and received his JD at the University of Florida.

Mateer Harbert - www.mateerharbert.com/

Email - jlussier@mateerharbert.com

About Burstek

As an industry leader in the development and deployment of Enterprise Internet Management solutions, Burstek has been on the forefront of Internet security since 1997. Burstek's core products, bt-WebFilter and bt-LogAnalyzer have won numerous awards and accolades and are the first Internet content filtering and reporting applications developed specifically for Microsoft server technology. By combining leading edge software solutions with the most competent technical support in the industry, Burstek has built a loyal customer base of education, industrial, financial, legal, government, and military organizations across the globe, including many Fortune 100 companies. Burstek is part of Burst Technology, Inc. © 2007.