Washington Journal of Law, Technology & Arts

Volume 1 | Issue 2 Article 3

2-1-2005

Risky Business: What Must Employers Do to Shield Against Liability for Employee Wrongdoings in the Internet Age?

Nicole J. Nyman

Corporate & Commercial
Cite as: Nicole J. Nyman, *Risky Business: What Must Employers Do to Shield Against Liability for Employee Wrongdoings in the Internet Age?*, 1 Shidler J. L. Com. & Tech. 7 (Feb. 2, 2005), *at* <http://www.lctjournal.washington.edu/Vol1/a007Nyman.html>

RISKY BUSINESS: WHAT MUST EMPLOYERS DO TO SHIELD AGAINST LIABILITY FOR EMPLOYEE WRONGDOINGS IN THE INTERNET AGE?

By Nicole J. Nyman[1]

ABSTRACT

Recent suits filed by the recording industry have raised the issue of employer liability for copyright infringement by employees. In fact, legal consequences for an employer do not end with copyright infringement liability, but extend into many other areas. This Article discusses several legal concerns raised by employee Internet use and examines steps an employer should take to minimize or avoid liability for inappropriate employee actions, including a discussion of benefits and drawbacks to various approaches.

TABLE OF CONTENTS

INTRODUCTION

<1> Employers may be held liable for the wrongdoings of employees, an issue raised by some highly publicized copyright infringement actions recently initiated. In April 2003, the Recording Industry Association of America ("RIAA") announced an out-of-court settlement of one million dollars with Integrated Information Systems ("IIS"). IIS is a technology company that, ironically, offers software for the secure electronic transmission of copyrighted material. The company allegedly allowed employees to share MP3 files over its internal network and ran a dedicated server for this purpose.

<2> The RIAA's policy appears to involve pursuit of companies connected in any way with copyright infringement. According to its senior vice president of business and legal affairs, the IIS settlement "sends a clear message that there are consequences if companies allow their resources to further copyright infringement."[2] This settlement, in combination with the confirmation by RIAA that it has identified business accounts in the search for pirates, has made employers more aware of possible liabilities that may arise from the Internet activities of employees.

<3> When employees download MP3 files at work, employers may face vicarious liability for copyright infringement. This, however, is only one of many legal problems that employers may face when employees interact with the World Wide Web. Employers should educate themselves regarding the various legal risks that arise and how to effectively avoid liability for employee misconduct. Employers should re-evaluate the company policy regarding Internet usage, including privacy issues that might arise as a result of the adoption of new technologies, and implement software solutions to monitor and enforce the company policy. These steps are likely to shield the employer from charges for an employee's illegal actions.

RISKS EMPLOYERS FACE DUE TO EMPLOYEE INTERNET ACTIVITIES

<4> In addition to employee file sharing of music, employers face possible liability for employee

misconduct in several other areas. The Internet puts numerous copyrighted resources at the fingertips of employees, including streaming video, music files, power point presentations, articles, software, logos, artwork, and pictures.

<5> When an employee infringes copyrights, the employer may be held liable under two theories: contributory and vicarious infringement. Contributory infringement requires the employer have "knowledge of the infringement" and have made "material contribution to the infringement."[3] Actual knowledge, however, is not always necessary. "Willful blindness is knowledge, in copyright law (where indeed it may be enough that the defendant *should* have known of the direct infringement)."[4] Thus, the fact that an employer was unaware of the illegal conduct of its employee does not fully preclude liability. In addition, the second theory, vicarious infringement, contains no knowledge requirement, but only requires that the employer receive "a direct financial benefit" and have "a right and ability to supervise the infringers."[5] In the employment setting, the second element is virtually always found, leaving the question of financial benefit to control the inquiry.

<6> Thus, unauthorized use of any copyrighted material may give rise to employer liability, especially when: (i) the employer enjoys a benefit because of the employee's infringement, (ii) the copyrighted material is shared using company time and equipment, or (iii) the employer has taken no steps to prevent such infringement and has turned a blind eye to the infringing activities.[6] When a third party brings charges for copyright infringement, which carries hefty fines of up to $150,000 per violation, the employer becomes a more profitable target than the employee because of the depth of employer pockets.[7]

<7> Employer liability extends beyond copyright infringement into several other areas. Defamatory or libelous statements made by employees in e-mail communications or Internet postings may give rise to employer liability.[8] Employers may also be liable to their employees for claims of sexual harassment or employment discrimination when other employees create a hostile work environment by downloading and distributing inappropriate materials.[9] Finally, even without the attribution of liability to other parties, employers should be concerned about employee Internet activity because it can contribute to a loss in employee productivity, significantly decreased bandwidth, and increased exposure to the viruses, worms, and spy-ware associated with downloading materials from untrusted and unknown Internet sources.[10]

FUNDAMENTALS AND LIMITATIONS OF THE COMPANY INTERNET POLICY

<8> To take a proactive part in the battle against inappropriate employee Internet activity, employers should put procedures into place to educate and monitor employees. If it can be demonstrated that the employer took affirmative steps to prohibit illegal activity, liability for employee actions is much less likely.

<9> Examining the existing company Internet policy is a good starting place for employers because, no matter how advanced, no software exists that is one hundred percent successful in preventing wrongful Internet actions by employees. Although a well drafted policy is a useful tool and a good first step, it alone is not likely sufficient. Withstanding charges of vicarious liability for copyright infringement requires more than a well written company policy.

<10> In a 2003 federal district court case, *Lowry's Reports, Inc. v. Legg Mason, Inc.*,[11] the publisher of a newsletter brought copyright infringement charges against a company subscriber because copies of the newsletter were sent via e-mail to many company employees and the letter was posted on the company's intranet. In defense, the company, Legg Mason, put forth the argument that such infringement violated the company's express use policy. The court responded that "reliance on company policies and orders is misplaced [for] [t]he law of copyright *liability* takes no cognizance of a defendant's knowledge or intent."[12]

<11> The court also noted that Legg Mason had the right and the ability to supervise its employees, who had infringed the newsletter copyright at company offices, through company equipment, and on company time.[13] While the court said company policy might be relevant in determining punitive damages, it unequivocally does not bear on the issue of employer liability.[14]

<12> In light of such a decision, an employer should do more than ensure the company Internet policy forbids inappropriate employee action. The subsequent steps of employee education and enforcement of company Internet policies are necessary. It is crucial that employees are aware

of company policies, the consequences of noncompliance, and the chosen methods of enforcement. Employee education should include specific examples of communications and uses that are appropriate and those that are not. Education should be done on a regular basis, and documentation evidencing such education and agreement to the policy should be compiled.

<13> To encourage compliance, employers should alert their employees to the problems that arise with inappropriate Internet activity so they understand the purpose of the company policy. When employees understand the risks facing the company and themselves, they are less likely to see the policy as a privacy intrusion and more likely to acknowledge the benefits and protection of compliance.[15]

<14> Another way to encourage employee compliance is to create a realistic policy, balancing the monitoring needs of the employer with the realities of the workplace. While a complete ban of private communications may be unrealistic, the employer should make it clear that even allowed private communications using company resources are subject to the same monitoring policy as all work-related communications, even if the use is after work and they are "off-the-clock," or if they have a company laptop that may be used outside of the office.

PRIVACY INTEREST CONCERNS OF EMPLOYEES

<15> Employers may attempt to enforce an Internet usage policy by monitoring their employees' Internet activities through software designed to monitor the files and actions of employees. Companies must be cognizant of the privacy issues raised by such monitoring. There have been several reported cases in which employees have sued employers for violations of privacy when the company monitored their online activity.

<16> In *Smyth v. Pillsbury*,[16] an employee brought an action for wrongful discharge against his employer when he was terminated as a result of an inappropriate e-mail sent over the company e-mail system. The employee, while at home, received and replied to an e-mail from his supervisor. Contrary to assurances by the company that such transmissions were private and confidential, the e-mail messages were intercepted by the company and, upon discovery of their content, the employee was terminated.

<17> The court found that there is no "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management."[17] The court noted that an employee's voluntary action itself forfeits the reasonable expectation of privacy. Further, the court stated that even if there was a reasonable expectation of privacy, the employer's actions were not "substantial and highly offensive invasion[s] of [the employee's] privacy. . . . Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[18]

<18> Most cases have followed the logic in *Smyth*, and it appears that, as a general rule, employees legally cannot claim an expectation of privacy for communications and activities conducted over the employer's infrastructure.[19] However, the court did note that when a privacy intrusion was "substantial" and would be "highly offensive" to a reasonable person, the result might be different.[20] In fact, there are several cases holding an employer liable for an invasion of privacy, many placing great weight on the fact that the employees were not informed of company monitoring of e-mails and other Internet activity.[21] While the balancing test between the company's need to monitor inappropriate activities and the privacy interests of the employee seems to weigh in favor of the employer, employers should still address employee privacy concerns when enforcing an Internet policy. Employers should educate employees regarding the monitoring policy in order to avoid employee expectations of privacy and the employer should monitor all employees equally as to avoid "highly offensive" intrusions.

SOFTWARE SOLUTIONS TO ENFORCE AN EMPLOYER'S INTERNET POLICY

<19> Because employers have the right and ability to supervise employees, they are required to do more than have a well-written company Internet policy – they must also enforce it. There are various software solutions that allow an employer to enforce Internet use policies.

<20> The first and most simple solution is to address these issues when configuring the company firewall. Firewalls can be configured to block traffic on certain ports, which eliminates

traffic from most of the widely known peer-to-peer operations. A firewall can block specific web site addresses, which prevents access to some of the biggest problem web sites.

<21> Also, a firewall can forbid the transmission of files with known problematic extensions, such as .mp3 and .wav. Firewall configuration is an excellent measure because it prevents inappropriate employee conduct and does not cost employer time to review a paper trail for misconduct that has already occurred. Also, because it is entirely preventative, firewall configuration does not raise concerns of invasion of employee privacy rights that often arise with monitoring software.

<22> Beyond firewall configuration, many software products are on the market to help employers respond to inappropriate employee Internet activities. The least controversial is software that scans company computers for illegal files. This activity raises fewer privacy concerns since the computers and company network are the property of the employer. This fact, when coupled with an Internet policy, make it less likely that courts would find a reasonable expectation of privacy by the employee concerning information stored on company property.[22]

<23> Regularly scanning company computers can be a very time intensive project, but could be accomplished over the company intranet during hours when the offices are closed and employee work is not hindered by the search.

<24> More sophisticated and more controversial software is available to help companies monitor and record employee Internet activities while they are actually online – recording e-mail messages, file downloads, web site screen shots, and amount of time spent within each browser window. Employers can use certain products within this category to record every employee keystroke, giving them access to each key typed by employees and statistics regarding the efficiency of the employee.[23] These monitoring techniques are invisible to the employee, yet are capable of obtaining communications, passwords, and personal identification numbers (PINs), which the employee would be very reluctant to divulge. Because of the high sensitivity of data that may be gathered by keystroke logging, there is an elevated duty of the employer to guard this data against security breaches. Appropriate safeguards must be established so that information is not accessible by any individuals other than those responsible for monitoring.

<25> Since keystroke monitoring software is so invisible to the employee, it raises more privacy issues. Some keystroke monitoring software includes an optional notification banner which companies may display to inform employees of the continual monitoring. Another drawback of this type of monitoring is an employer's elevated risk of employee claims of discriminatory enforcement. Avoiding these claims requires that employers be very consistent in monitoring and enforcing their Internet policy through these means.[24]

<26> Unfortunately, none of the software options discussed above will bring a certain end to problematic employee Internet use, since, for the determined employee, there are always ways to circumvent the safeguards. However, employing some methods that will eliminate most illegal employee activities shows that the employer is not turning a blind eye to the activities, but is, instead, making a good faith attempt to supervise the actions of its employees.

<27> To further establish the efforts of the employer, an enforcement plan should be well documented, listing the officers with the specific responsibility to police activities that violate the company policy, defining the frequency of the monitoring, and detailed procedures and documentation of any follow-up activities that follow a policy violation. Such documentation shows that not only does company policy forbid certain uses, as was the case in *Lowry*, but also that the employer took additional steps to enforce the policy, which is likely to be a cushion against employer liability.

CONCLUSION

<28> As demonstrated by the recent RIAA enforcement proceedings, there are inherent legal risks to employers when their employees access the Internet. There are, however, concrete steps that employers can take to protect themselves from liability for employee actions. Employers must regularly re-evaluate the company Internet policy and educate employees as to the policy and its specific implications. The employer then has a duty to monitor employees and must take at least some steps to ensure compliance—which may necessitate a technological solution. And finally, the employer should consistently enforce the policy.

PRACTICE POINTERS

- Provide employees with concrete illustrations of both prohibited and allowed activities and list the specific consequences for each violation, so they better understand how the general guidelines will be applied.
- Enlist the help of employees through education regarding the purposes of the company policy and the benefits of compliance.
- Document that employees have been educated and notified regarding the company policy and that they have given consent to the monitoring of any communication transmitted over company equipment.
- Update the company policy frequently.
- Remind employees of the company policy on a regular basis and promptly notify employees when policy revisions are made.
- Include specific information within the policy regarding enforcement, including delegation of duties to various staff members and specification of which high-level personnel have overall oversight responsibility.
- Employ at least some technological methods to ensure compliance with the company policy, especially methods with a low cost, such as reconfiguring the company firewall.
- Monitor and enforce the company policy with regularity and equality, avoiding focus on select individuals.
- Take extra precautions with information obtained through the monitoring of employee activities to ensure that it is appropriately safeguarded.

<< Top

FOOTNOTES

1. Nicole J. Nyman, University of Washington School of Law, Class of 2005. Thanks to John Morgan for feedback on a draft of this Article.
2. Recording Indus. Ass'n of Am., *RIAA Collects $1 Million From Company Running Internal Server Offering Thousands of Songs*, http://www.riaa.com/news/newsletter/040902_2.asp (Apr. 9, 2002).
3. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1160 (9th Cir. 2004), *cert. granted*, 125 S. Ct. 686 (U.S. Dec. 10, 2004)(No. 04-480). The boundaries of these tests may be altered in 2005 when considered and addressed by the Supreme Court.
4. In re Aimster Copyright Litigation, 334 F.3d 643, 650 (7th Cir. 2003).
5. *Grokster.* 380 F.3d at 1164.
6. *See* Lowry's Reports, Inc. v. Legg Mason, Inc., 271 F. Supp. 2d 737, 745-746 (D. Md. 2003).
7. 17 U.S.C. § 504(c)(2) (1999) (other subsections of this statute ruled unconstitutional).
8. Marcelo Halpern, *Secure Email Use: Avoid the Pitfalls and Hazards of Email in the Workplace*, TechTV, *at* http://www.techtv.com/news/securityalert/story/0,24195,2470875,00.html (Mar. 21, 2000).
9. Marcelo Halpern, *Setting Boundaries on Net Use: Minimize the Risks Associated with Employee Internet Access*, TechTV, *at* http://www.techtv.com/news/securityalert/story/0,24195,2432470,00.html (Mar. 28, 2000).
10. Dan Hutzell and Jim Lynch, *RIAA Subpoenas Identify Business Accounts*, The Ass'n of Prof'l Office Managers, *at* http://www.apom.us/Articles/riaa.asp (Oct. 2003).

11. 271 F. Supp. 2d 737 (D. Md. 2003).
12. *Id.* at 746.
13. *Id.* at 745-46.
14. *Id* at 746.
15. Laura Hunt, *E-Mail Monitoring: Why You Should Pry*, SearchCIO.com, *at* http://searchcio.techtarget.com/qna/0,289202,sid19_gci817258,00.html (Apr. 16, 2002); Toni Bowers, *How toRroll out an IT Policy in your Organization*, TechRepublic, *at* http://techrepublic.com.com/5100-6315-1051507.html (July 31, 2002).
16. 914 F. Supp. 97 (E.D. Pa. 1996).
17. *Id.* at 101.
18. *Id.*
19. *See* Garrity v. John Hancock Mut. Life Ins. Co., 2002 WL 974676 (D. Mass.); Kelleher v. City Of Reading, 2002 WL 1067442 (E.D. Pa.); U.S. v. Monroe, 52 M.J. 326 (C.A.A.F. 2000); McLaren v. Microsoft Corp., 1999 WL 339015 (Tex. App.). *But see* U.S. v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).
20. 914 F. Supp. at 100.
21. Douglas M. Towns, *Legal Issues Involved in Monitoring Employees' Internet and E-Mail Usage*, GigaLaw.com, *at* http://www.gigalaw.com/articles/2002-all/towns-2002-01-all.html (Jan. 2002).
22. Joycelyn A. Stevenson, *Recent Cases Confirm Need for Employment Guidelines on Computer and Internet Use in the Workplace*, Boult Cummings E-News, *at* http://www.bccb.com/Publications/Files/RecentCasesConfirmNeedForEmploymentGuidelinesOnComputer.
(Mar. 14, 2002).
23. Stuart Glascock, *Keystroke Logging Software Spies on Chats, IMs*, TechWeb, *at* http://www.techweb.com/wire/story/TWB20001106S0012 (Nov. 6, 2000).
24. Nicholas D'Ambrosio, *Avoid the Most Common Mistakes When Dealing with Your Employees*, The Business Review, *at* http://www.bizjournals.com/albany/stories/2002/08/12/smallb3.html (Aug 9, 2002).

<< Top