

Proper Internet Usage in the Workplace

By Benjamin Wright, JD

Employee Internet abuse can cost employers. It can spawn a lawsuit. The costs can be imposed on large and small employers alike. Prudent employers will take practical steps against computer abuse.

Hostile Workplace Lawsuits in the Internet Age

In the workplace, electronic pornography is legal poison. In a "hostile environment" lawsuit against a business, the existence of porn on work computers or in work e-mail systems can be highly prejudicial. Even though the business objected to porn and enforced an explicit policy against it, its presence can reflect horribly on the business as a case goes to the courtroom.

In *Williams v. City of Chicago*¹ e-pornography backed the police department into an indefensible position. After a female police officer complained about pornography in department computers, the department took action in accordance with its policy against pornography and hostile work environment. Still, officer Williams sued, and the court said the case should go to a jury for decision. The basic question for the jury would be whether the porn in department computers was so pervasive that it injured officer Williams.

Wow. How can the police department withstand a jury trial focused on the amount of pornography on the department's computers? Such a public trial would be highly embarrassing, even if the department eventually won the case! The local media would have a field day. At this point, the city has strong incentive to settle with Ms. Williams and pay her a lot of money.

The presence of pornography is hard to defend in a lawsuit.

¹(US Dist Ct, N.D. Illinois, E Div 03C2994, Jul 13, 2004),
<http://www.internetlawguide.info/tiki-index.php?page=Williams+v+Chicago>

Behold the city's unenviable position. Even after it settles, its problem remains. The continued presence of Internet pornography can prejudice the city in future cases brought by future employee-plaintiffs, just as it did in Ms. Williams' case.

This police department has good reason to use technical measures – filters and blocks – to mitigate its problem.

Another case ensnared a trucking company -- *Smith v. C.H. Robinson Worldwide, Inc.*² The employer asked the judge to dismiss a sexual harassment case. But the court said the case should continue because:

[Plaintiff] Smith claims that [co-workers] exposed her to lewd internet images. . . . [M]ost of the internet images seen by Smith were not specifically brought to her attention by [co-workers]. Smith claims that due to the close proximity of cubicles in the office, it was impossible to avoid seeing the internet images that she thought inappropriate. . . . While the incidents of pornography viewing may seem inconsequential . . . such conduct should not be considered individually, but in the aggregate.

In other words, Internet abuse in the workplace can contribute to an overall finding of hostile work environment for which an employer might be liable and have to pay money.

²Minnesota District Court, Fourth Judicial District, File No. 27-CV-06-19663, September 14, 2007. <http://www.sprengerlang.com/files/9.14.07%20SJ%20Denial%20LS.pdf>

Reasonable Steps by Employer

In *Burlington Industries Inc. v. Ellerth*³ and *Faragher v. City of Boca Raton*⁴ the US Supreme Court said an employer will often be able to avoid liability for sexual harassment if it takes reasonable steps to prevent the harassment. One reasonable step, logically, would be to monitor and block offensive computer use.⁵

Internet monitoring and blocking are logical steps to combat harassment.

Employer's Duty to Investigate

Employment law suggests an employer has a duty to investigate if it sees dangerous activities by an employee. One approach is for an employer to close its eyes, and hope it sees nothing that would give rise to an obligation to investigate. But that approach is dangerous. After disaster happens, proving that the employer saw nothing is hard – especially when the clues are records stored on the employer's computers. It's better to be generally aware of what employees are doing through their computers. Employers have reason to monitor Internet usage for both pornography and other dangers.

*Jane Doe v. XYZ Corporation*⁶ said an employer could be held responsible for injury to a child, where an employee was using his work computer to access child pornography on the Web. The New Jersey Supreme Court said the employer should have known of the employee's illicit surfing and therefore should have informed the police. Had the police been informed, then the employee's abuse of his step daughter at home might have been prevented.

³524 U.S. 742 (1998).

⁴524 U.S. 775 (1998).

⁵Sindy J. Policy, "Keeping an eye on Net use and e-mails can prevent litigation," Business Law Today. <http://www.abanet.org/buslaw/blt/ndpolicy.html>

⁶887 A.2d 1156 (N.J. 2005).

In addition to pornography, an employer has incentive to monitor for other dangerous matters like illegal drugs or weapons.

Surfing to any unsavory site can pose a security risk for the employer's computers and network.

Employee Acceptable Use Policy

An employer is often wise to publish an acceptable use policy for employees. Generally, the policy should forbid the use of work equipment for pornography and other offensive or non-business purposes. It might specifically warn against wasting of time at places like gambling, shopping or social networking sites.⁷ And it might warn that violation of the policy could be grounds for reprimand or termination. An example policy: <http://www.abanet.org/labor/lel-aba-annual/papers/2004.oneill.pdf>

Policy on Monitoring of Employee Communications

An employer may also be wise to tell employees that the employer may monitor employee communications through employer equipment. A prudent employer might warn employees they have no privacy in work equipment, and any suspicious information may be disclosed.

Smart employers might communicate this information to employees multiple times. In *Quon v. Arch Wireless*⁸ a supervisor's careless words over-rode the employer's written policy that it could read an employee's electronic messages. Because it is hard to prevent a boss from ever saying something contrary to policy, policy might be repeated over and over and over. One way to repeat policy might be to have it appear every time an employee logs onto a network or sends a message.

⁷At least one court has upheld the termination of an employee for excessive web surfing. <http://www.nysun.com/new-york/court-upholds-citys-decision-to-fire-employee/73049/> Proper disciplining of employees is beyond the scope of this paper.

⁸hack-igations.blogspot.com/2008/06/employee-imtexte-mailvoiccomputerinter.html

Conclusion

As the Internet has become commonplace in modern work life, new technology is necessary to keep the workplace safe. Deployment of Internet monitoring and filtering software can be evidence of good faith efforts to foster a safe work environment.

~ ~ : ~ ~



A Dallas-based attorney, Benjamin Wright is the author of leading books on technology law, including *The Law of Electronic Commerce*. He maintains a popular blog at <http://legal-beagle.typepad.com>. This paper provides only general education under US law. It does not provide legal advice for any particular situation. If you need legal advice, you should consult your lawyer. November 2008.



[CyberPatrol](http://www.cyberpatrol.com)[®] provides technical solutions for monitoring Internet activity at home, in the workplace or in an organization like a church or school. CyberPatrol software can filter or block unwanted parts of the Internet such as pornography sites and offensive chat sessions.