Employee Use of Technology in the Workplace: Corporate Liability for Sexual Harassment Claims

CONTENTS

SONICWALL

Abstract: Use of technology in the workplace has grown exponentially over the past few years. We are at a time when literally every employee has access to the Internet and the corporate e-mail system. That access affords employees use of a communications medium that may result in substantial liability for their employers.

E-mail and Internet use has already served as "smoking gun" evidence in lawsuits involving breach of contract, discrimination, harassment, fraud, defamation, and many other claims. It has become almost commonplace to find articles on the front pages of the business sections of many newspapers to find articles detailing the latest corporate liability stemming from electronic evidence. This White Paper addresses one particular aspect of that liability: sexual harassment and discrimination claims. The reason for focusing on this particular area of liability is that it is one of the most common sources of claims involving employee use of their employer's Internet and e-mail systems and carries with it some of the greatest liability.

For example, it was reported that an e-mail message, "25 reasons beer is better than women," was part of the evidence retrieved from a large oil company's computer system in a sex discrimination lawsuit in 1995. It was the key evidence leading to a settlement that cost the petroleum giant $2.2 million.

A few statistics will further highlight the problem:

- *1 in 5 men and 1 in 8 women admitted using their work computers to access sexually explicit material online*
- *More than 25% of workers surveyed said they "sometimes" or "often" receive sexually explicit or otherwise improper e-mails*
- *A 2000 study revealed that 1 in 3 companies had terminated employees for abusing Internet access*
- *A survey conducted by Elron Software Inc. found the following: Of the 86% of people who said they send or receive personal e-mail at work, 70% said their e-mail contains "adult content"*

Many employers have had to take drastic action to address this problem:

- *Dow Chemical fired more than 75 employees for forwarding inappropriate or harassing jokes to coworkers by e-mail*
- *The New York Times fired 22 staff members for sending or forwarding dirty jokes*
- *Several Computer Associates employees were fired for e-mailing sexually explicit jokes*

HOSTILE WORK ENVIRONMENT

The most common form of corporate liability for harassment is for claims based on a "hostile work environment." This type of environment is present when "the workplace is permeated with discriminatory intimidation, ridicule, and insult ... that is sufficiently severe or pervasive to alter the conditions of the victim's employment and create an abusive work environment ...."

Employers can be directly or indirectly liable for sexual harassment based on a hostile work environment. Direct liability results when, for example, the employer's supervisor harasses a subordinate. In this type of case, the wrongful conduct of the supervisor is imputed to the employer on the theory that the employer should be responsible for the supervisor's actions. Indirect liability results when an employer is liable for failing to adequately address and correct behavior or activity that creates a hostile work environment. An employer who is on notice that its employees are receiving highly offensive, sexually explicit e-mail or accessing inappropriate sites on the Internet, including downloading sexually explicit images and other

materials, may be indirectly liable for allowing such conduct to occur in the workplace (i.e., not taking reasonable steps to prevent employees from engaging in this activity).

The most frequent form of this liability arises when an employee downloads sexually explicit jokes, graphics, and stories from the Internet and then forwards them around the company by e-mail. There have been instances where employees have downloaded literally hundreds of megabytes of this material and stored them on their employer's computer systems. In addition to potential liability for sexual harassment, the presence of this material on the employer's computer systems may give rise to liability for copyright infringement (i.e., the images and other content will likely be copyrighted), prosecution for trafficking in child pornography or committing hate speech, and potential seizure of the company's computer system because it was used in the commission of a crime. In addition, these types of materials frequently contain illicit code (e.g., viruses, worms, Trojan horses) that may cause substantial harm to the employer's systems.

Separate and apart from potential liability issues is the very real problem of lost employee productivity as a result of these activities. As indicated by the studies referenced above, the amount of time spent by employees surfing non-business related sites on the Internet and, in particular, sites with sexually explicit content is at an all time high. Most businesses now view the loss of employee productivity as so substantial that the use of blocking software and other technological measures to limit access to inappropriate sites has now become the rule, rather than the exception, in business.

An employer may be liable for failing to monitor and prevent inappropriate use of e-mail and the Internet when it has notice of the offensive use. In *Blakey v. Continental Airlines, Inc.* (June 1, 2000), the New Jersey Supreme Court ruled that postings on a work-related electronic bulletin board constituted a hostile work environment for which the employer could be held liable. The court ruled that the employer had a duty to remedy the harassment because it had notice employees were posting defamatory and harassing messages on the electronic bulletin board.

NEW DEFENSE IN SEXUAL HARASSMENT CASES

Until recently, employers had little guidance with regard to the measures they should take to mitigate potential liability for harassment claims. Several relatively recent decisions, however, have finally provided some guidance for businesses.

An employer may establish an "affirmative defense" to a claim of harassment by showing that it had a specific policy concerning employee use of technology, including the Internet and e-mail, and that it responded promptly to potential harassment and discrimination claims. That is, the employer must show that it was proactive in addressing the problem (e.g., the use of written technology policies and employee training, use of Internet and e-mail content monitoring technology) and that it took swift action as soon as it became aware of inappropriate activity.

In *Faragher v. City of Boca Raton* and *Burlington Industries, Inc.*, the United States Supreme Court recognized a new affirmative defense that may be raised by employers in sexual harassment cases. The defense has two elements: (1) that the employer had exercised reasonable care in preventing and promptly correcting any sexually harassing behavior, and (2) the employee unreasonably had failed to take advantage of the employer's preventive or corrective procedures or otherwise avoid harm.

In *Schwenn v. Anheuser-Busch, Inc.*, an employee received sexually harassing e-mail messages from fellow employees. The employee failed to establish a claim of hostile work environment because, in large part, her employer had an e-mail policy in place and promptly responded to her claims by meeting with employees responsible for sending the inappropriate e-mail to advise them of the company's policy against such messages.

In *Daniels v. WorldCom*, employees claimed that their employer was negligent for allowing "racially harassing" e-mail to be circulated on its computer system. The employer successfully defended itself, due in part because it produced a written policy against such activity and proof that it responded quickly to claims of harassment.

REDUCING POTENTIAL LIABILITY

As the cases described above make clear, employers can substantially mitigate potential liability by adopting a three-pronged approach to employee use of technology: (1) adopt an appropriate technology use policy, (2) conduct training for employees to ensure they understand their rights and obligations regarding their use of corporate computer resources, and (3) promptly enforce the policy, including the implementation of appropriate technological measures (e.g., e-mail content monitoring applications and Internet monitoring and blocking programs). The use of technological measures, in particular, has become a key element of many businesses' approach to preventing sexual harassment claims. By using content monitoring technology, these businesses can prevent access and distribution of sexually explicit materials before they give rise to a harassment claim. Use of such technology would likely have prevented many of the harassment claims filed to date involving employee use of e-mail and the Internet.

To be effective, the technology policy must clearly describe each employee's rights and obligations regarding use of the corporate computer systems. In the context of potential harassment claims, a basic policy should include the following:

- A statement regarding the employer's position against harassment, including examples of inappropriate uses. For example:

  Material that is harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate, including any comments that would offend someone on the basis of race, age, sex, sexual orientation, religion, or political beliefs, national origin, or disability, must not be sent by e-mail or other form of electronic communication, viewed on or downloaded from the Internet or other online service, or displayed on or stored in our computer systems. Users encountering or receiving such material must immediately report the incident to their Supervisor. For more information, please see our Policy Against Sexual Harassment.

- A strong notice to employees that no one controls the Internet and that having an e-mail account will likely result in the receipt by the employee of spam, including messages with highly offensive, sexually explicit content. A typical disclaimer would read as follows:

  WE ARE NOT RESPONSIBLE FOR MATERIAL VIEWED OR DOWNLOADED BY USERS FROM THE INTERNET. THE INTERNET IS A WORLDWIDE NETWORK OF COMPUTERS THAT CONTAINS MILLIONS OF PAGES OF INFORMATION. USERS ARE CAUTIONED THAT MANY OF THESE PAGES INCLUDE OFFENSIVE, SEXUALLY EXPLICIT, AND INAPPROPRIATE MATERIAL. HAVING AN E-MAIL ADDRESS ON THE INTERNET MAY LEAD TO THE RECEIPT OF UNSOLICITED E-MAIL CONTAINING OFFENSIVE CONTENT. USERS ACCESSING THE INTERNET DO SO AT THEIR OWN RISK.

- A reference to the employer's general non-discrimination/harassment policy:

  Use of our computer systems, including Internet and e-mail, is subject to the provisions of our [title of non-discrimination/harassment policy].

- A statement that violations of the policy may subject employees to disciplinary action and potential termination of their employment. For example:

  Violations of this Policy may result in disciplinary action, up to and including possible termination, and potential civil and criminal liability.

In *Faragher v. City of Boca Raton*, the City of Boca Raton was found not to have exercised reasonable care to prevent harassment, particularly when management made no attempt to keep track of a supervisor's inappropriate conduct or enforce its published policy. Similarly, in *Burlington Industries v. Ellerth*, the Supreme Court stated that an employer is negligent and therefore subject to liability if it knew or should have known about sexual harassment and failed to stop it. In

Schwenn v. Anheuser-Busch, in addition to threats of discipline, the employer warned employees that it would audit e-mail messages to enforce policy.

Given the potential damages and adverse publicity businesses face from harassment lawsuits, they should not delay in implementing the three-pronged approach outlined above. By taking action now, before a claim ever arises, businesses can potentially avoid dramatic damages later. The costs involved in implementing this approach are minimal compared to the potential damages that may result from even a single lawsuit. There is no longer any reason to delay. Businesses should act immediately to address this problem.

ABOUT THE AUTHOR

Michael R. Overly is a partner in the e-Business and Information Technology Group in the Los Angeles office of Foley & Lardner. As an attorney, Certified Information Systems Security Professional (CISSP), and former electrical engineer, his practice focuses on counseling clients regarding technology licensing, information security, electronic commerce, and Internet and multimedia law. Mr. Overly writes and speaks frequently on technology licensing, information security, the legal issues of doing business on the Internet, and technology in the workplace. Mr. Overly has written numerous articles on these subjects and has authored chapters in several treatises. He is the author of the best selling e-policy: How to Develop Computer, E-mail, and Internet Guidelines to Protect Your Company and Its Assets (AMACOM 1998), Overly on Electronic Evidence (West Publishing 1999), Document Retention in The Electronic Workplace (Pike & Fischer 2001), and The Open Source Handbook (Pike & Fischer 2003).