

Email, Adult Content, and Employment Law: Reducing Corporate Liability With Filtering and Policy Tools

By Michael R. Overly, Esq.
Foley & Lardner

Summary of Contents

- > Employers have been found liable for failing to protect employees from offensive electronic imagery and failing to prevent inappropriate use of email.
- > Ignoring the significant risks posed by such email can result in potential officer and director liability.
- > Companies can gain substantial protection by proactively working to reduce the threat of inappropriate email.

>> Protecting Your Company From Unsolicited Pornographic Email <<

The overwhelming majority of corporate email addresses today receive unsolicited commercial email, or spam. For a growing number of recipients, this includes spam with adult content or pornography known as unsolicited pornographic email (UPE). UPE poses serious legal risks to corporations, wastes valuable corporate computing resources, and reduces employee productivity.

Based on recent court and regulatory rulings, it's clear that UPE leaves companies vulnerable to charges of creating a "hostile work environment," and all the associated liabilities that implies. Already, employers have been found directly and indirectly liable under these rules for failure to protect their employees from offensive imagery, and failing to monitor and prevent inappropriate use of email when notified by employees of the problem.

Though email is often treated casually, it carries with it potentially significant consequences. It has become an almost constant target of discovery in litigation (some corporate attorneys say email is a factor in all of their litigation). Ignoring the significant risks posed by such email can result in potential officer and director liability for failure to exercise reasonable business judgment in addressing the problem.

While there is a range of possible responses to UPE, nearly all observers concur that organizations must take steps to address the problem, and that costs of prevention are trivial compared to the liability and damages that may result.

Developing an appropriate solution to UPE requires an understanding of email technology, employment law, email policies, and available email filtering solutions. Only a unified approach can provide a solution to this problem, but fortunately, employers can establish an "affirmative defense" to potential claims by establishing both policies and processes that address UPE.

This booklet is designed to explain the potential legal liabilities faced by corporations, provide precedence of similar cases, and provide suggested actions to minimize the risk of liability. It begins with an overview of the legal situation, explains how email policies can help, and then examines the role of email filtering and perimeter protection services that can help enforce these policies.

>> Unsolicited Pornographic Email and Hostile Work Environments <<

Receipt of UPE may subject an employer to liability for harassment based on a “hostile work environment.” This type of environment is present when, as noted in *Harris v. Forklift Systems, Inc.*, 510 U.S. 17, 114 S.Ct. 367, 370, 126 L. Ed.2d 295 (1993)

“ 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, or makes a habit of forwarding racially or sexually offensive email. 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 fails to adequately address and correct behavior or activity that creates a hostile work environment. For example, an employer who is on notice that its employees are receiving UPE may be indirectly liable for allowing such email into the workplace (i.e., not taking reasonable steps to prevent the email from being received by its employees) because technical solutions to this problem are now available.

Employers have also been found liable for failing to monitor and prevent inappropriate use of email when put on notice by employees. In *Blakey v. Continental Airlines, Inc.* (June 1, 2000), the New Jersey Supreme Court unanimously ruled that items 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 that harassment because it had received notice that employees were posting defamatory and harassing messages on the electronic bulletin board.

In itself, receipt of UPE is not grounds for an employee’s lawsuit. **But once the issue has been raised by an employee, it is incumbent upon corporate managers to take prompt remedial action.**

Adopting a well-developed email policy provides one part of the solution, but a mechanism should be deployed to enforce that policy and to quickly address future instances of offensive spam. Given the volume of email most businesses receive and the need for rapid action, many businesses are turning to technology to provide that mechanism.

The good news is that **if an organization does take prompt, appropriate, and effective action, it can avoid or substantially mitigate liability even in cases where sexual harassment actually occurred.**

Some examples of effective and ineffective responses are discussed in the next section.

>> New Defense in Sexual Harassment Cases <<

Laws related to employment and email are in a state of flux, but several relatively recent decisions provide some guidance.

An employer may establish an “affirmative defense” by showing that it had a specific policy concerning email and that it responded promptly to potential harassment and discrimination claims. Use of filtering and perimeter protection services can help establish a record of prompt response. The availability of this affirmative defense gives employers an incentive to prevent and eliminate harassment and discrimination. And by requiring employees to take advantage of the preventive or remedial apparatus in place, employers are protecting themselves as well.

> In *Schwenn v. Anheuser-Busch, Inc.*

an employee who received sexually harassing email messages from fellow employees failed to establish a claim of hostile work environment because, in large part, her employer had an email policy in place and promptly conducted meetings with the employees involved to reiterate the company’s sexual harassment policy.

> In *Daniels v. WorldCom*

employees claimed that their employer was negligent for allowing “racially harassing” email on its computer system. The employer successfully defended itself, in part because it produced a written policy that both included comprehensive remedy procedures and was actively supported by management.

> In *Faragher v. City of Boca Raton and Burlington Industries, Inc.*

the 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.

These cases make clear that **companies can gain substantial protection by proactively working to reduce the threat of inappropriate email.**

>> How Companies Can Reduce Their Potential Liability <<

Reducing liability requires that companies implement a unified approach to UPE. The approach should have three components:

- > An appropriate email policy.
- > Training for employees.
- > Mechanisms and computer-based tools and filters for enforcing the policy.

To be effective, an email policy must clearly describe each employee's rights and obligations regarding use of his or her employer's email system. 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 content for email. 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 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 email 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 email address on the Internet may lead to the receipt of unsolicited email containing offensive content. Users accessing the Internet do so at their own risk.

> 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.

Complete guidelines on developing a corporate email policy are beyond the scope of this paper, and companies should consult their legal counsel as part of that process, but several resources are now available that can help companies understand these issues and develop their own policies. Among them are www.email-policy.com, and the book *E-policy: How to Develop Computer, E-Policy, and Internet Guidelines to Protect Your Company and Its Assets* by Michael Overly.

What's important to stress here is that having a policy is generally not enough to establish a defense to a claim of harassment. Employers must also enforce the policy and proactively take steps to prevent employees from being exposed to harassing material. Non-enforcement implies non-commitment or, worse, disregard for accepted working conditions, while the implementation of filtering systems and perimeter protection services count as important indicators of corporate intent to enforce stated policies.

The three-pronged foundation of policy, training, and enforcement greatly reduces the potential for employment-related claims. In the event of litigation, this foundation will strengthen the employer's position in requesting a summary judgment or other motion to terminate litigation at any early stage – saving legal costs in hundreds of thousands of dollars and substantial damages.

>> The Cost of “Winning” Legally <<

It's worth noting that prevailing in the courtroom is not the same as “winning.” As noted in a recent article in *Risk and Insurance* http://www.riskandinsurance.com/0902_news_1.asp, even if a company prevails in court, companies will still “spend tens of thousands of dollars on attorneys' fees, internal investigations, employee unhappiness, and lots of nonproductive time.”

In addition, companies that follow through in enforcing their email policy may find themselves forced to terminate large numbers of employees. For example, *New York Times* fired 23 employees and disciplined 20 others for exchanging inappropriate email with co-workers, Dow Chemical fired 50 employees and 200 others faced suspension for transmitting by email offensive, pornographic, and explicitly violent material, and Edward Jones & Company terminated 19 employees for failing to admit they sent pornography or off-color jokes over the company's email system. **Clearly, prevention of the problem by intercepting offensive messages before they reach employee inboxes is a more desirable way to go.**

>> Technical Approaches to Reducing Liability <<

Key to retaining the protections of an email policy, and the affirmative defense available for actively policing the policy, is having a set of tools that allows email administrators, HR directors, CIOs, and corporate general counsels to take action.

While there are a few products now available that remove adult content from inbound email, not all of them meet both the legal and technical requirements necessary to solve the problem in an acceptable way. To be effective, systems that filter adult content must meet a demanding set of requirements imposed by several different constituencies, including IT, upper management, and end users.

First, these systems must handle large volumes of inbound email, avoid generating false positives, and be capable of immediate adjustment in the event of employee complaints. They must also work with an organization's existing email infrastructure, and must not interfere with the way users read, write or send messages – users have shown that they are unwilling to adjust their practices to comply with policy. Ideally, they should be server or perimeter (outside the firewall)-based, rather than client-based so that UPE never reaches employees' desktops.

Demands on administrator time must be minimized. Administrators can't be expected to spend time scanning through quarantined messages or responding to user inquiries. And simple monitoring is not enough. Administrators need a single point of command and control across all of the email resources via a centralized console that gives the administrator the ability to manage and control email traffic – based on source information and the target recipient.

Finally, the system must offer a substantial and provable return on investment. In most cases that means a system that deals with a wide range of other threats such as spam, viruses, and Directory Harvest Attacks.

>> Summary of Recommended Actions <<

Effective strategies for reducing liability are well understood, but most companies have not yet implemented the policies or tools they should to reduce their legal risks. Based on the current state of the law and commercially available technology, companies can reduce their potential liability if they:

- > Develop clearly stated email policies, as well as administrative means to communicate and enforce those policies.
- > Implement tools that allow automated policy enforcement and prompt remedial action.
- > Use reasonable efforts to prevent UPE from ever reaching employees.

Fortunately, cost-effective products and services to automatically enforce corporate email policies and to eliminate UPE are available now. Organizations that opt to implement these systems can gain a variety of other benefits, including conservation of valuable computer resources and the prevention of other harmful content such as viruses.

>> 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 book *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), and *Document Retention in The Electronic Workplace* (Pike & Fischer 2001).



Brought to you by:
Postini Corporation
510 Veterans Blvd.
Redwood City, CA 94063
USA
Tel 650-482-5130
Fax 650-482-3109
www.postini.com