UIC John Marshall Journal of Information Technology & Privacy Law

Volume 22
Issue 1 *Journal of Computer & Information Law - Fall 2003*

Article 9

Fall 2003

A Further Darkside to Unsolicited Commercial E-mail? An Assessment of Potential Employer Liability for Spam E-mail, 22 J. Marshall J. Computer & Info. L. 179 (2003)

Ben Dahl

A FURTHER DARKSIDE TO UNSOLICITED COMMERCIAL E-MAIL? AN ASSESSMENT OF POTENTIAL EMPLOYER LIABILITY FOR SPAM E-MAIL

BEN DAHL†

Imagine one day a "police officer" appears at a local office and wanders the hallway to a cubicle and begins to take off his clothes in front of a woman working at her desk. The woman gasps and then noisily evicts the semi-nude man from the office once she realizes it is a strip-o-gram. The following day a "maid" performs similarly in the lunchroom. Security escorts her out. After a couple of days, the CEO wisely instructs the office reception to prevent any individual appearing with an apparently inappropriate or Velcro-enclosed outfit from entering the company's offices. If the CEO fails to take remedial action, she likely will be subjecting her company to a sexual harassment claim based on a hostile work environment.

Although the concept of a daily strip-o-gram described above may be facially fanciful, quite similar behavior appears in offices everyday around the country in the form of unsolicited pornographic e-mail, also known as "porn spam." The barrage of advertisements containing graphic images through unsolicited e-mail creates an environment with similar attributes as described above. That risk is substantial.[1]

† Ben is the COO and Co-Founder of Unspam, LLC, a consulting company for businesses and governments trying to solve the problems created by the flood of unsolicited, unwanted e-mail, also known as spam. Unspam's mission has been to combine a legal and technological approach to mitigating spam. Prior to co-founding Unspam, Ben worked to create Echo, Inc., a digital music licensing and distribution consortium backed by, among others, Best Buy, Virgin Entertainment Group, and Borders, through a recapitalization of a failed dot-com. Ben also practiced corporate law at Cooley Godward LLP, advising public and private technology companies as well as venture capital funds. Ben has a J.D. from the University of California, Berkeley School of Law (Boalt Hall) and is a member of the California Bar Association. Ben also has an A.B. in History from Princeton University.

1. Although this article only extensively covers receipt of pornographic spam, the risk is not confined merely to receipt. Employees also may be successfully lured by the advertisements that make their way into the workplace. This "clicking through" provides a risk

One need only look to the case settled on August 12, 2003 for $435,000 filed by twelve librarians in Minnesota to understand the potential specter of liability for employers.[2] The librarians alleged that they were subjected to a hostile work environment as a result of the unfettered Internet access afforded patrons.[3] The Equal Employment Opportunity Commission ("EEOC") agreed with the librarians.[4] The EEOC further concluded that the Minnesota public library should settle the case for $75,000 per librarian, for a total of $900,000.[5] Although the attorney for the librarians, Robert Halagan, contends that the EEOC decision and subsequent settlement do not have far reaching implications,[6] wise employers should see this as a harbinger of future lawsuits and administrative actions, particularly as it applies to porn spam.

This article endeavors to provide practical, rubber-meets-the-road advice to corporate leaders to assess and address the sexual harassment challenges posed by unsolicited e-mail. The first part of this article focuses on the potential liability that employers could face as a result of the receipt of pornographic spam in the workplace. The second part focuses on methods that corporate leaders can employ to reduce their risk of exposure to the legal pitfalls of spam.

The bottom line is that the proliferation of unsolicited commercial e-mail in the workplace means extra risk for businesses. The inherent threat in these communications has yet to be taken into account adequately by the business community. As will be outlined in this article, there is the double potential harm for employers of legal liability and business disruption, particularly given the legal and social backdrop of this problem. However, businesses can protect their bottom lines by low-

---

in its own right, potentially bringing more offensive material into the workplace and/or creating a sexually charged employment atmosphere. Even absent substantial specific discussion of this issue, it looms in the background. "Clicking through" multiplies the effect of spam receipt by employees.

2. Gary Young, *No Smut at Work, Please*, Natl. L. J. (Sep. 15, 2003) <http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1063212018621> (accessed Feb. 18, 2004); *Library Settles with Workers Who Sued Over Hostile Work Environment* <http://wcco.com/localnews/local_story_227152529.html> (last updated Aug. 15, 2003); Tim Lemke, *Email Porn a Problem at Work,* Washington Times, (Oct. 16, 2003) <http://washingtontimes.com/business/20031015-093057-6953r.htm> (accessed Feb. 18, 2004).

3. For a copy of a complaint, *see Librarian Complaint to the EEOC Alleging "Hostile Environment" in Library without Censorware,* <http://www.eff.org/Censorship/Censorware/20010502_eeoc_complaint.html> (accessed Feb. 18, 2004).

4. *EEOC Determination. Re: Unrestricted Internet Access Policy of Minneapolis Public Library Creates Sexually Hostile Work Environment,* Tech. L. J., (May 23, 2001) <http://www.techlawjournal.com/internet/20010523eeocdet.asp> (accessed Feb. 18, 2004).

5. Michael Rogers and Norman Oder, *Library Journal: Feds Back Minnesota Staffers' Complaint* (July 1, 2001) <http://www.libraryjournal.com/article/CA90448> (accessed Feb. 18, 2004).

6. Young, *supra* n. 2, at ¶ 10.

ering their risk profile through applying several relatively simple techniques used to: 1) reduce the prevalence of unsolicited commercial e-mail in the workplace; 2) mute the potential harm of offensive e-mail; and 3) create a paper trail indicating diligence in the fight to protect employees.

I. BACKGROUND

The Internet has brought forth a revolution in how business is conducted and relationships work. The "killer app" of e-mail allows easy, quick, and cheap communication between friends, co-workers, and business contacts. The effectiveness and increased speed of communication have been cited as main drivers of the recent productivity gains in the United States.[7] However, enhanced communication has come with the dark side of unsolicited commercial e-mail, also known as "spam."[8] When spam is an offer to refinance a house or purchase nutritional supplements, consumers and businesses may be annoyed by the time or the resources required either to delete the message or route it to the rubbish.[9] However, when spam contains pornographic pictures, employers have another concern, namely liability. With over one third of companies (thirty-seven percent) without any policy or procedure regarding spam, there is great potential for looming liability.[10]

While there have been indications in the press, as well as marketing materials from e-mail filtration companies that employers face risk,[11] an overall analysis has been lacking. Employers need to know the legal risks that they face. They also need to be aware of the attitudes of their employees and how those attitudes relate to the legal risks. And beyond the marketing materials of filtration companies, employers need a road map for a complete approach to limiting potential liability from pornographic spam in the workplace.

---

7. John Rutledge, *Telecom Deregulation, It's Time for That Call*, Investors Bus. Daily A20 (Nov. 24, 2003); James Flanigan, *To Ease Fear About Jobs, Put Imagination to Work*, L.A. Times C1 (Jan. 4, 2004).

8. *See* Deborah Fallows, *Spam: How it is Hurting E-mail and Degrading Life on the Internet*, Pew Internet & American Life Project (Oct 22, 2003) <http://www.pewinternet.org/reports/ toc.asp?Report= 102> (accessed Feb. 18, 2004) (quoting Orson Swindle, Federal Trade Commission commissioner, "Spam is about to kill the 'killer app' of the Internet").

9. *Id.* (page seven of the PDF file indicates that the most popular way of dealing with spam was to click the "delete" key).

10. *See Survey finds 37% of Respondents Have No Spam Policy in Place* <http://www.clearswift.com/news/pressreleases/206.aspx> (accessed Feb. 18, 2004).

11. *See Why is Email Security So Critical* <http://www.postini.com/services/why_security_critical.html> (accessed Feb. 18, 2004); *Business Benefits*, <http://www.brightmail.com/enterprise-benefits.html> (accessed Feb. 18, 2004); *Monitoring Email, Privacy Issues*, <http://enterprisesecurity.symantec.com/article.cfm?articleid=91&PID=na> (accessed Feb. 18, 2004); *Virtual Image Agent*, http://www.surfcontrol.com/products/content/art_of_filtering/virtual_image_agent/default.aspx> (accessed Feb. 18, 2004).

II. AN ASSESSMENT OF EMPLOYER RISK

A survey of the large volume of legal literature addressing sexual harassment brings one to the inevitable conclusion that most employees must stock shelves in adult bookstores, serve cocktails in skimpy outfits, or constantly struggle with the decision to hang a Playboy centerfold instead of a Degas bather.[12] Although such situations provide fodder for intellectual discussion, they do little to aid general counsels and corporate leaders in taking practical steps to forestall or minimize sexual harassment problems in the workplace.

Although there is lively and interesting debate regarding the difficulties posed by potential proscription of First Amendment speech as a result of prevailing sexual harassment law,[13] corporate leaders do not have the luxury of engaging in this ivory tower debate. They must focus on three separate goals: 1) limiting sexual harassment liability; 2) maintaining a positive work environment; and 3) preserving a solid reputation among peer institutions and potential employees. These three goals are all served by creating an environment that will limit the efficacy of hostile work environment claims brought by employees. In order to examine whether the company has any risk, we must first look at the current state of sexual harassment law.

At first blush, many may see spam as being of little risk to employers. Everyone's computer has a "delete" key. The quick use of the delete key should make further action unneeded on behalf of employers. However, there are both legal and practical indications that risk looms in the form of potential hostile work environment claims. The first part of the analysis is whether a colorable legal claim can be made that spam contributes to a hostile work environment. Although more than a colorable claim is needed to prevail as a plaintiff in final adjudication, it may be all that is necessary to cost an employer hundreds of thousands of dollars directly, not to mention the indirect costs of the derailment of hiring and recruiting efforts. After the brief analysis of relevant sexual harassment law, the next two sections look at the risk in both the encouragement of plaintiffs by certain government agency and advocacy groups and the at-

12. *See* generally, Eugene Volokh, *Thinking Ahead About Freedom of Speech and Hostile Work Environment Harassment*, 17 Berkeley J. Emp. & Lab. L. 305 (1996); David Benjamin Oppenheimer, *Workplace Harassment and the First Amendment, A Reply to Professor Volokh*, 17 Berkeley J. Emp. & Lab. L. 321 (1996).

13. *Id. See* also David E. Bernstein, *Sex Discrimination Laws Versus Civil Liberties*, 1999 U. Chi. Leg. Forum 133 (1999) (significant tension exists between the First Amendment and sexual discrimination laws); Richard A. Epstein, *Liberty, Patriarchy, and Feminism*, 1999 U. Chi. Leg. Forum 89 (1999) (differences between men and women exist, greatest protection of workers comes from information and freedom to enter the market); Andrew Koppelman, *Feminism and Libertarianism: A Response to Richard Epstein*, 1999 U. Chi. Leg. Forum 115 (1999).

titudes of the public at large regarding spam and employers' risks associated with its receipt.

A. Summary of Relevant Sexual Harassment Law

The legal question of whether spam could create a hostile work environment claim requires the answering of two main questions: 1) Can pornography contribute to a hostile work environment? and 2) Can the pornographic spamming by a third-party be attributed to an employer?

1. *Can Pornography Contribute to a Hostile Work Environment Sufficient to Support a Claim of Sexual Harassment?*

Employer liability for sexual harassment must be measured under both the EEOC guideline and the general Title VII standard that provides its underpinning. The overall Title VII standard proscribes discrimination on the basis of an individual's sex. That discrimination can manifest in "compensation, terms, conditions, or privileges of employment."[14]

The EEOC guidelines enumerate three separate types of harassment claims that specifically fall under the Title VII standard:

> Unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature constitute sexual harassment when (1) submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment, (2) submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual, or (3) such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive work environment.[15]

Courts, for quite some time, made a delineation between the following two different types of sexual harassment cases: 1) cases based on a quid pro quo theory; and 2) cases based on a hostile work environment.[16] Quid pro quo cases presented scenarios where promotions or job maintenance were explicitly made contingent by supervisors or employees on sexual acquiescence by employees.[17] These explicit trade-offs created an alteration in the terms of employment.[18] Hostile work environment cases did not provide that explicit trade-offs be elucidated.[19] Instead such claims required that indirect sexual harassment conduct had to be severe or pervasive enough to implicitly alter the terms of the employ-

14. 42 U.S.C. § 2000e-2(a) (2004).
15. 29 C.F.R. § 1604.11(a) (2004).
16. *See Burlington Industries Inc. v. Ellerth*, 524 U.S. 742, 751-754 (1998).
17. *See Meritor Savings Bank, FSB v. Vinson et. al.*, 477 U.S. 57, 65 (1986).
18. *Id.* at 66.
19. *Id.* at 67.

ment contract.[20]

The United States Supreme Court in two cases decided on the same day *Burlington Industries Inc. v. Ellerth*[21] and *Faragher v. City of Boca Raton*[22] determined that these two types of claims could not be so clearly delineated. Essentially, the Court held that the key was not whether the behavior by the supervisor or the employer fell into this bucket or that bucket, but rather whether the conditions of employment were altered sufficiently to change the nature of the employment contract.[23] Under *Burlington* and *Faragher*, explicit sexual advances no longer needed to be tied to explicit employment actions.[24] Along with the employee favorable blurring of the line between quid pro quo claims and the hostile work environment claims, the Court offered defendant employers a new affirmative defense. The affirmative defense at base was an analysis of whether the employer had, under the circumstances, taken reasonable steps to prevent the harassment.[25] The Court indicated in *Burlington* and *Faragher* that the adequacy of the defense should be analyzed under a two-prong test: 1) did the employer exercise reasonable care to prevent and correct promptly the sexually harassing behavior? and 2) did the employee unreasonably fail to take advantage of employer's preventive or corrective action?[26] Therefore, while the strict requirements for employees to claim sexual harassment were reduced, employers were given a significant, new tool to protect themselves.

Despite the effective theoretical combination of quid pro quo harassment and hostile work environment harassment, the term "hostile work environment" continues to be used by commentators and courts to describe the general employment context in which employees find themselves. These hostile work environment cases are generally not monolithic, i.e. there are a number of factors contributing to an environment sexually charged enough to alter implicitly the conditions of employment. Although there have been scant circumstances where pornography in the workplace alone has been determined to be adequate to sustain a hostile work environment claim in and of itself, it has been a part of numerous successful claims.

> Although many, if not most, women find pornography, particularly in workplace settings, to be insulting, intimidating, and degrading, courts generally have not held that pornography in the workplace, even when unwelcome and pervasive, constitutes hostile environment sexual har-

20. *Id.*
21. *Burlington*, 524 U.S. at 742.
22. *Faragher v. Boca Raton*, 524 U.S. 775 (1998).
23. *Burlington*, 524 U.S. at 754; *Faragher*, 524 U.S. at 786.
24. *Burlington*, 524 U.S. at 754; *Faragher*, 524 U.S. at 786.
25. *Id. Burlington*, 524 U.S. at 756; *Faragher*, 524 U.S. at 808.
26. *Burlington*, 524 U.S. at 756; *Faragher*, 524 U.S. at 808.

> assment per se. Rather, most courts have cited pornography in the workplace as mere *evidence* of a hostile environment, if they found pornography mentioning at all, and have focused primarily on other aspects of harassing behavior, such as offensive comments and sexist pranks.[27]

There is some support among commentators and case law to make pornography in and of itself enough to support a claim for sexual harassment.[28] Because of the charged nature of sexual harassment discussions, some commentators vehemently argue for the expansion of claims for sexual harassment,[29] while others see a doomsday erosion of free speech in the workplace.[30] Because of this disagreement it is necessary to look directly at the case law to see that, in general, mere pornography in the workplace has not been enough to sustain harassment claims.[31] Although the cases available currently point generally to the inadequacy of pornography standing alone as a basis for a claim, there has been a noticeable expansion of what courts have determined to be adequate for sexual harassment suits.[32] In light of the United States Supreme Court's establishment of an employer affirmative defense,[33] courts will likely continue to allow a broader definition of the types of conduct for which employers will be held responsible.[34]

---

27. Note: *Pornography, Equality, and a Discrimination-Free Workplace: A Comparative Perspective*, 106 Harv. L. Rev. 1075, 1087 (1993).

28. *Id.* at 1090; *see also Robinson v. Jacksonville Shipyards, Inc.*, 760 F. Supp. 1486, 1542 (M.D. Fla. 1991).

29. *See Pornography, supra* n. 27, at 1090.

30. *See Volokh, supra* n. 12, at 319.

31. *Rabidue v. Osceola Refining Co.*, 805 F.2d 611, 622 (6th Cir. 1986) (porn had small effect on harassment); *Andrews v. City of Philadelphia*, 895 F.2d 1469, 1485 (3d Cir. 1990) (porn pinned up was evidence of a hostile workplace); *Waltman v. International Paper Co.*, 875 F.2d 468, 476-77 (5th Cir. 1989); *but see Robinson v. Jacksonville*, 760 F. Supp. at 1542.

32. Kim Houghton, *Internet Pornography in the Library: Can the Public Employer Be Liable of Third Party Sexual Harassment When a Client Displays Internet Pornography to Staff?* 65 Brook L. Rev. 827, 861 (1999). The accompanying notes provide a good basis for an in-depth examination of the expansion of hostile work environment claims based on "dirty pictures." An in-depth examination of this trend is not necessary for this article, because this article focuses primarily on risk reduction techniques rather than on the current evolution of hostile work environment sexual harassment theories.

33. *Burlington*, 524 U.S. at 756; *Faragher*, 524 U.S. at 808.

34. Two examples are instructive of this trend. The first is the recently settled case regarding the Minnesota librarians being harassed by patrons cited in the introduction to this article indicating an expansion of employer duties. In that case the EEOC determined that the employer did owe a duty to the employees to take reasonable steps to limit the ability of patrons to harass employees. The second oft-cited cases are the cases against Hooters restaurants by waitresses against the employer for harassment by patrons. Hooters restaurants are establishments themed on "female sex appeal" which includes a signature provocative uniform consisting of short-shorts and tight T-shirts. *See Hooters of America, Company, About Hooters*, <http://www.hooters.com/company/about_hooters/> (accessed Feb. 18, 2004). These cases were brought by waitresses around the country based

A hostile work environment claim must meet two requirements in order to be actionable.[35] First, that the complained-of conduct would not have occurred but-for the employee's gender.[36] Second, the conduct must be severe or pervasive enough to make a reasonable woman believe that the conditions of employment are altered and the working environment is hostile or abusive.[37]

The first requirement in the case of spam would seem a difficult burden for an employee plaintiff to fulfill. All employees that receive pornographic spam are arguably equally affected. Male or female, there is no indication that pornographic spam is directed only at women or that women receive more pornographic spam.[38] However, some courts have looked at impact as being *de facto* evidence of harassment.[39] Under such a loose standard, a defendant need not prove that the behavior has been directed intentionally or solely at women, but rather must show that such material has an adverse impact on women. In *Lehmann*, even

---

on the behavior of patrons. Although these cases ended in negotiated settlements, they represent increased employer risk for third party action. *See* Sarah L. Sanville, *Employment Law—Employer Liability For Third-Party Sexual Harassment: Does Costilla Take the Hoot out of Hooters?* 25 Wm. Mitchell L. Rev. 351 (1998). Given the arguable assumption of risk that waitresses assume by becoming waitresses at Hooters, the employer settling these cases is indicative of the perceived trend that employer duties are expanding under the law.

35. *Lehmann v. Toys 'R' Us*, 626 A.2d 445, 453 (N.J. 1993). In *Lehmann*, the court actually divides these two requirements into four prongs, the court's decision indicates that the last three prongs are interdependent and therefore cannot be perfectly unpacked. For the purposes of this article it is more appropriate to combine those three prongs into one requirement.

36. *Id.*

37. *Id.* Although there is much debate regarding whether the standard for harassment should be a *reasonable woman* or a *reasonable person* standard, it is relatively inconsequential in this context as will be seen below in the generally similar reaction of both males and females to the problem of pornographic spam. However, in terms of analyzing potential liability as an employer, the more prudent standard to assume is the reasonable woman standard. In the context of either standard, there is an objective reasonability standpoint. This objectivity prevents particularly frail plaintiffs that may be easily offended or harassed from successfully suing on relatively innocuous content.

38. Unspam, LLC, *Recent Publication, Comprehensive Spam Survey*, <http://www.unspam.com/fight_spam/information/survey_oct2003.html> (Oct. 15, 2003) (supplementary information is on file with the author or available by subscription from Insight Express) (the survey covered 1,500 respondents and included respondents from all fifty states and the district of Columbia). The margin of error for the survey is +/- 2.65 percent. Women responded on average that 8.77 percent of spam they received in their work e-mail accounts work was pornographic, while 24.05 percent of spam they received in their personal account they considered pornographic. The percentages for men were 10.70 percent and 27.93 percent respectively. Thus, the results indicate that on a perception basis, men perceive there to be more porn spam—quantitatively—coming into their accounts.

39. *See* Houghton, *supra* n. 32, at 858-861.

though noting perhaps the moral difference between intentional and unintentional harassment, the court looked to the purpose of sexual discrimination law, i.e. to eliminate discrimination whether intentional or unintentional. The implication of the holding in *Lehmann* is that some courts will infer that conduct is directed towards women if such conduct has a disparate impact. The disparate impact of pornographic spam is apparent.[40] Women are more bothered by offensive content than men.[41] Further, in specific circumstances, pornographic spam can have a particularly devastating psychological impact on women. As one woman recipient of pornographic spam observed when surveyed regarding unsolicited commercial e-mail:

> Almost daily I get really nasty spam in my email account. . . [One] offers a '3 for 1' deal so that I can have access to 'real police videos' of sexual assaults. The email promises that I have 'never seen such cruel action.' As a rape survivor, this email upsets me greatly.[42]

The above statistics and anecdotal evidence such as the preceding quote indicate that a strong factual case can be made for disparate impact in the case of pornographic spam.

The second requirement of showing severity and/or pervasiveness to the level that a court would hold a company responsible is more difficult for potential plaintiffs. Would a court find that pornographic spam was severe or pervasive enough to alter the terms of employment? The most conclusive answer one can reach is maybe.[43] Although, as discussed in the previous paragraph, courts have been reluctant to find that pornography is severe or pervasive enough to be actionable in and of itself,[44] there are specific characteristics of e-mail that may make the receipt of pornographic spam particularly onerous for employees. First, for many businesses the timely receipt, review, and reply to e-mail is considered essential. Employees are held responsible if they "miss" an e-mail in their effort to weed out spam.[45] Second, for many employees the computer is a constant companion either at their desk or on the road. The ubiquity of computer input means that once porn spam arrives, absent

---

40. *See* Fallows *supra* n. 8, at 30 of PDF ("[s]ignificantly more women than men are bothered by offensive or obscene content of spam (83% v. 68%); by the deceptions and dishonesties in spam (82% v. 77%); by the sense that spam could mean their privacy has been compromised (79% v. 73%); and that spam could damage their computers (81% v. 76%").

41. *Id.*

42. *Id.* at 34. Another woman observed, "[i]magine the horror of being forced to sign up for numerous accounts in order to complete research directly related to my job, only to be sent unwanted spam relating to such topics as breast augmentation and increasing sexual stamina." *Id.* at 30.

43. *See* Houghton, *supra* n. 32, at 861-867; *see supra* n. 31.

44. *See* Houghton, *supra* n. 32; *Burlington*, 524 U.S. at 756; *Faragher*, 524 U.S. at 808.

45. Sharon Gaudin, *False Positives: Spam's Casualty of War Costing Billions*, <http://itmanagement.earthweb.com/secu/article.php/2245991> (accessed Feb. 18, 2004).

any technological blockage or other mitigation, it has the potential to invade all aspects of the work environment. These aspects of e-mail are factors that would have probative value in convincing a court that the conditions of employment have been altered as a result of unfettered receipt of pornographic spam.

2. *Can Third-party E-mail Sending be Imputed to the Employer?*

The relevant regulatory authority has provided that employers can be held responsible for actions of third parties.[46] The EEOC has established the following guideline in the Code of Federal Regulations:

> An employer may also be responsible for the acts of non-employees with respect to sexual harassment of employees in the workplace, where the employer (or its agents or supervisory employees) knows or should have known of the conduct and fails to take immediate and appropriate corrective action.[47]

Numerous cases have pointed to employer liability for actions of third parties.[48] These cases of employer liability for the actions of non-employees have been broadly categorized into three different varieties of cases:

> 1) [if the] employee's position places him under the 'control' of a non-employee, both employer and non-employee are potentially liable; 2) [an] employer's dress code that encourages patrons to sexually harass employee can create liability for employer because of employer's acquiescence; and 3) employers are charged with a broad duty of protecting the employee from sexual harassment.[49]

The third variety, or general duty cases, described above provide the basis for an employer's duty to filter porn spam from employees. Weak arguments for the first and second variety of cases (as described in the passage above) can be made. For example, one could make a rather attenuated argument that an employer's lack of e-mail filtering or an adequate acceptable use policy ("AUP") is in some sense the employer acquiescing in the harassment of its employees. However, unlike the situation where an employer provides a revealing uniform, the lack of filtering or a company-wide AUP differs in that: 1) no distinction can be drawn between men and women with respect to an AUP or filtering

46. 29 C.F.R. § 1604.11(e).

47. *Id.*

48. *See Henson v. City of Dundee*, 682 F.2d 897 (11th Cir. 1982) (non-employee strangers may cause hostile work environment); *Folkerson v. Circus Circus Enterprises, Inc.*, 107 F.3d 754 (9th Cir. 1997); *Trent v. Valley Electric Association* (9th Cir. 1994) (comments made by non-employee trainer in the midst of mandatory training session could cause Company Title VII liability).

49. *Rosenbloom v. Senior Resource Inc.*, 974 F. Supp. 738, 743 (D. Minn. 1997) (using the sexual harassment jurisprudence as an analog for racial harassment), cited in the sexual harassment context in *Costilla v. Minnesota*, 571 N.W.2d 587, 592 (Minn. App. 1997).

scheme; and 2) the setting of a dress code is an active as opposed to a passive action on the part of the employer. Therefore it is most appropriate to examine the case of porn spam under the third category as one where the employer has a general duty to protect its employees against discrimination in the workplace.

Precedents are clear that employers risk liability if they fail to take reasonable measures to stop a harassment problem when they know about the problem. However, an employer can contend that it lacks adequate control over the Internet or its computer systems to prevent pornographic e-mails from invading their computer networks. If an employer successfully argues that it cannot control its information technology, it can free itself legally from any obligation to protect employees from spam. This is codified in the EEOC guidelines regarding sexual harassment and third parties,

> In reviewing [sexual harassment cases] the [Equal Employment Opportunity Commission] will consider the extent of the employer's control and any other legal responsibility which the employer may have with respect to the conduct of such non-employees.[50]

In an effort to free themselves from liability, companies will need to claim that their computer networks are a proverbial wild west where anything goes.

Although a company could have perhaps made this argument successfully a few years ago, certain trends have given employers more control over their computer networks and incoming e-mail. First, there has been filtering. The avalanche of spam for corporate networks and personal e-mail inboxes has provided the market impetus for the creation of technologies to allow e-mail filtering.[51] The list of companies or organizations providing filtering technologies or assisting with its implementation is quite impressive including Cloudmark, Brightmail, IronPort Systems, Mail Frontier, and Spam Assassin.[52] The existence and effectiveness of these filters would make a claim by an employer of inability to control (at least partially) its e-mail systems very difficult. Specifically, several filters are substantially effective in blocking pornographic messages.

The second trend that has given employers a presumption of control

---

50. 29 C.F.R. § 1604.11(e).

51. According to a study by the Radicati Group revenues for anti-spam vendors and outsourcers are expected to approach $653 million by 2003, growing to over $2.4 billion by 2007. *See Anti-Spam Filter Makret [sic] Market Analysis, Data & Figures* <http://www.gii.co.jp/press/rd14419_en.shtml> (accessed Feb. 18, 2004).

52. A list of many anti-spam tools can be found at *Master List of Anti-Spam Software*, <http://paulenglish.com/spam/software.html> (accessed Feb. 18, 2004).

over their own networks has been a legal one.[53] Employers have fought in court to maintain legal control over their networks in the context of monitoring employees e-mail and Internet use. Their legal success in permitting them to eavesdrop on employee computer and Internet activity may lead a court to conclude that companies presumptively have control over the incoming and outgoing data including pornographic e-mail.

B. Plaintiff Promotion

In addition to the backdrop of legal precedent and technological change described above, businesses face an increasing litigious environment with respect to sexual harassment claims. Why should businesses care about this pro-plaintiff environment? Simply because lawsuits are a costly distraction. They consume financial resources, tax executive time, and create morale problems within the company. Therefore, at best, a victory in a lawsuit can only be a pyrrhic one. With that in mind, the following shows how likely potential plaintiffs are to capitalize on any corporate misstep.

The literature from the EEOC and plaintiff lawyers paint harassment with a particularly broad brush. The Women's Bureau of the EEOC produced a brochure covering sexual harassment claims under the *Civil Rights Act of 1964*, indicating that sexual harassment is "unwanted sexual attention at work."[54] Illegality is defined according to this brochure as harassment that "is making it hard for [the employee] to work."[55] This brochure presents prospective plaintiffs with a rather low bar to clear. Anything that impedes an employee's work and is of a sexual nature can be construed as harassment. The brochure continues with an entire section titled "You Can Win."[56] This brochure may not necessarily reflect reality given the legal standards set forth in court cases regarding harassment. However, its text may encourage many to seek legal redress in borderline situations.

For employers that may not review, update, or enforce their sexual harassment policies on a regular basis, these types of sentiments should

53. In the past, employers were unable to monitor employee e-mail communications over a network that was not their own for fear of running afoul of "wiretap" restrictions. *See* Jeffrey S. Nowak, *Employer Liability for Employee Online Criminal Acts*, 51 Fed. Comm. L.J. 467, 483 (1999). As e-mail has become more ubiquitous, employers have fought for and gained greater control over their networks with respect to these "wiretap" issues. *See* Eric P. Robinson, *Update on Employer E-mail Monitoring: The Ninth Circuit Joins the Mainstream*, 18 Lab. Law. 355 (2003). These gains in control come with the cost of the assumption that corporations control their systems.

54. Women's Bureau of the EEOC, *Sexual Harassment* <http://www.pinn.net/~sunshine/now-news/harass2.html> (accessed Feb. 19, 2004).

55. *Id.*

56. *Id.*

be alarming. However, they should also be motivating. As the EEOC observed in its sexual harassment guidelines:

> Prevention is the best tool to eliminate sexual harassment in the workplace. Employers are encouraged to take steps necessary to prevent sexual harassment from occurring. They should clearly communicate to employees that sexual harassment will not be tolerated. They can do so by establishing an effective complaint or grievance process and taking immediate and appropriate action when an employee complains.[57]

So, as an employer, the question becomes whether spam presents a problem legally, in the eyes of the potential plaintiff, such that an employer should take steps to forestall expensive legal action. The examination of this is in two parts. The first looks at the legal history and the precedents regarding sexual harassment examined in Section A above. The second examines employee attitudes, examined below.

C. Employee Attitudes

So how do employees feel about porn spam? Does it rise to the level of being offensive enough to create legal risk? As discussed above, the standard analysis for potential legal liability is whether the porn spam is severe or pervasive enough to make a reasonable woman believe that the conditions of employment are altered or the working environment is hostile or abusive.[58] Surveys or polls, although not dispositive in the context of a legal dispute, certainly can provide some indication as to the way juries or judges might view a particular issue.[59] Recent surveys prove instructive and alarming in the way employees view pornographic spam.[60]

These surveys clearly highlight that there is indeed significant risk that reasonable women will find pornographic spam in the workplace severe or pervasive. One survey asked those that are required to use e-

---

57. EEOC, *Sexual Harrassment*, <http://www.eeoc.gov/types/sexual_harassment.html> (accessed Feb. 19, 2004); *see also Sexual Harrassment: Know Your Rights!*, EEOC Guidelines, 186-188 (Martin Eskanazi & David Gallen, eds., 1992).

58. *See* Houghton, *supra* n. 32; *Burlington*, 524 U.S. at 756; *Faragher*, 524 U.S. at 808.

59. *See* Houghton, *supra* n. 32, at 835. "Third-party sexual harassment has been recognized by courts since at least 1981. While subsequent complaints of third-party sexual harassment may be voluminous, thus far, there have been few cases actually leading to litigation. However, there are indications that claims may be on the rise." The implication of this is that these third-party claims are generally being settled and/or dropped. Moreover, there likely will not be voluminous precedent before this becomes an issue for numerous businesses. Therefore, businesses must look beyond the courts for an assessment of the risk exposure in such cases.

60. *See* Unspam, *supra* n. 38; Fallows *supra* n. 8. The discussion of the Fallows survey is above. The statistics set forth in that study bear on the impact that pornography has on women. The Unspam statistics point more to legal risk than disparate impact. Thus, they are the focus of this section.

mail at work whether the offending behavior is "severe," "pervasive," or both.[61] The survey asked respondents that were work e-mail users, "Do you consider pornographic spam at work severe, pervasive, both, or neither?"[62] Forty-three percent of respondents who use e-mail at work said that porn spam at work already met the standard for sexual harassment in that it was "severe," "pervasive," or both.[63]

More troubling in terms of jury pool viewpoints were the responses that elucidated legal conclusions from respondents.[64] The survey asked respondents to rank their level of agreement with particular statements as "strongly agree," "agree," "neither agree nor disagree," "disagree," or "strongly disagree."[65] One of the statements was, "I believe unsolicited pornographic e-mails can contribute to a hostile work environment."[66] Seventy-percent of those using e-mail at work indicated that they either "agreed" or "strongly agreed."[67] Furthermore, sixty-four percent "agreed" or "strongly agreed" that "[e]mployers have a duty to protect employees from unsolicited pornographic email."[68] A majority of workers using e-mail believe employers have a duty to filter.[69] Therefore, the likelihood is that potential jurors would come into any sexual harassment trial with a preconception that employers have a duty to protect employees. Even with the burden of proof falling on the plaintiff, company defendants will face an uphill battle in convincing juries to support inaction.

These sentiments were even more pronounced when women respondents were isolated.[70] A full seventy percent of women believe unsolicited pornographic e-mails can contribute to a hostile work environment.[71] Sixty-six percent of women believe employers have a duty to protect employees from unsolicited pornographic e-mail.[72] Furthermore, forty-four percent of women believe unsolicited e-mail pornography in their workplace is already "severe," "pervasive," or both.[73] In addition to the implications of these statistics with respect to juror preconceptions, they also bolster the argument that pornography has a

61. *See* Unspam, *supra* n. 38.
62. *Id.*
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.*
67. *See* Unspam, *supra* n. 38.
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*
73. *See* Unspam, *supra* n. 38.

disparate impact on women as described above.[74]

III. METHODS FOR EMPLOYERS TO LIMIT LIABILITY

From the above discussion, it is relatively clear that there is risk for employers. Even if the sufficiency of pornography alone in creating a hostile work may be somewhat suspect, an employer's failure to control pornographic spam will, at best, assist claims against the employer if other aspects of a hostile work environment claim are present. Furthermore, at worst, a sexual harassment claim based solely on porn spam may turn out to be successful even in the absence of other factors. With the Minnesota library case,[75] as well as the relative increase in third party sexual harassment claims,[76] a lawsuit will eventually be filed against an employer for failure to control incoming pornographic spam. Therefore, employers need a how-to guide to protect themselves from apparent liability in advance of any such filings. Protection should be based on the affirmative defense afforded employers in *Burlington* and *Faragher*.[77]

Employers should focus on providing a reasonable measure of protection, particularly if there are employee complaints. Strategies to combat spam can be divided into five main categories: 1) stopping the spammers from sending spam to company e-mail addresses; 2) keeping spam sent to company e-mail addresses from getting into employee inboxes; 3) reducing the impact of any spam received; 4) setting policies and procedures that encourage employee participation in preserving a comfortable work environment; and 5) auditing and reviewing regularly and periodically the adequacy and effectiveness of policies.

A. KEEPING SPAMMERS FROM COMPANY E-MAIL ADDRESS: A DISGUISE FOR THE "SPIDER"

A reduction of the availability of company e-mail addresses to marketers will help companies reduce the amount of spam received and correspondingly reduce liability. Currently, one of the cheaper ways to prevent expropriation of e-mail addresses is the creation of spider-resistant formatting standards for a company's Internet sites, particularly

74. *See supra* Section II.A.1.

75. *See supra* nn. 2-6.

76. *See supra* n. 59.

77. As discussed above, the Supreme Court outlined an affirmative defense in *Burlington* and *Faragher*. *Burlington*, 524 U.S. at 756; *Faragher*, 524 U.S. at 808. The defense was proven through a two-pronged test: 1) did the employer exercise reasonable care to prevent and correct promptly and sexually harassing behavior?; and 2) did the employee unreasonably fail to take advantage of employer's preventive or corrective action. *Burlington*, 524 U.S. at 756; *Faragher*, 524 U.S. at 808.

with respect to the display of e-mail addresses.[78] Spammers use programs known as harvesters to gather e-mail addresses from available Internet pages.[79] These harvesting programs, also known as spiders, "crawl" through available pages and identify e-mail addresses by scanning for the e-mail address format.[80] So, if a Web site displays an e-mail address of "name@company.com" the harvester will recognize this as an e-mail format and will record it for inclusion in a marketing e-mail list.[81]

A company currently has some ability to prevent these harvesters from grabbing e-mails from the site through the formatting.[82] There are two formats for e-mail addresses that currently harvesters do not recognize: 1) an html encoded address; and 2) an address written in plain text.[83] The first option allows a company to have a "click here to email" type link for Web site viewers to use to contact you, but does not display the address in a spider-readable form. The second option is to write out the address in a way that is recognizable to human users, but unrecognizable to the spiders. For example, "name@company.com" can be rewritten as "name at company dot com."

The Center for Democracy and Technology did a six-month study of how marketers get e-mail addresses to send individuals spam.[84] The study used hundreds of randomly generated e-mail addresses and posted them in various ways, including publicly on a Web site, on a news group, or opted-in to the mailing list for particular marketers.[85] The Center

78. The Center for Democracy and Technology studied a variety of measures to make addresses difficult to "harvest" from Web sites. *See* CDT Study, *Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research Six Month Report* (Mar. 2003) <http://www.cdt.org/speech/spam/030319spamreport.shtml>.

79. *See* Timothy Muris, Chairman FTC, *FTC Spam Forum*, (FTC Conf. Cent., Washington, DC, Apr. 30, 2003) (explaining the techniques spammers use to gather e-mail addresses).

80. *See* WindowSecurity.com, *Email Harvesting Techniques FAQ* <http://secinf.net/anti_spam/Email_Harvesting_Techniques_FAQ.html> (accessed Feb. 18, 2004) (explaining how spiders search chatrooms, Web sites, and even watch Internet traffic as it travels through the network).

81. *Id.*

82. *See* CDT Study, *supra* n. 78.

83. Techniques exist to automate this process of obscuring addresses. While some of these techniques are too technical to discuss here, they can be effective and, once installed, make the process effortless. *See* Gaddo F. Benedetti, *Defeating Spam Spiders* (Aug. 19, 1999) <http://www.15seconds.Com/issue/990819.htm>; W3C Recommendations, *HTML 4.01 Specification, HTML Document Representation* (Dec. 24, 1999) <http://www.w3.org/TR/REC-html40/charset.html#doc-char-set> (specifying the HTML codes that can be used in Web sites); *see also* Dean Peters, *Mean Dean's Anti-spam Obfuscator* (Oct. 12, 2002) <http://www.Healyourchurchwebsite.com/archives/000154.shtml> (free resource to automatically generate encoded e-mail addresses).

84. *See* CDT Study, *supra* n. 78.

85. *Id.*

used both the html encoding and the plain text techniques to see if they could fool the spiders. The answer was a resounding yes:

> Obscuring an e-mail address is an effective way to avoid spam from harvesters on the Web or on USENET newsgroups. Even when posted in publicly accessible areas, none of the addresses we obscured—whether in English ('example at domain dot com') or in HTML—received a single piece of spam. Users who want to avoid spam should consider obscuring their addresses when possible.[86]

This obfuscation of e-mail addresses was their most concrete suggestion for stopping the tide of spam. Eventually harvesters may get smarter as these spam reduction techniques become adopted more broadly. However, these techniques have been found to be effective against the currently employed harvesting technologies. Although the CDT study did not cover it, employers may also be able to obfuscate e-mail addresses from spiders by representing the e-mail address as a graphic instead of text.

Even in the face of such potential technological challenges, a further technique for avoiding the publication of e-mail addresses on a company Web site will likely still be effective. Companies have the option of completely stripping company Web sites of e-mail addresses. Companies can avoid placing any e-mail addresses on Web sites whether encoded or not through the maintenance of a fill-in contact form which does not reveal any e-mail address.

If spammers are unable to secure e-mail addresses for recipients, porn spam has a more difficult time entering the workplace. Less porn spam means less risk for employers.

B. Stopping Spam Before the Inbox: Filtering

As indicated above in the discussion of employee attitudes, employees for the most part feel that employers have a duty to filter e-mail. And in terms of limiting liability for companies, e-mail filtration is a solid first step. Even though filtration companies oversell their ability in and of themselves to provide protection (as there are many other things that are still in the employer's control that can prevent spam from contributing to a hostile work environment), these companies in their marketing material rightly point to a reduction of potential liability for the

86. *See* Aron Roberts, *Protecting Your Website's Email Addresses from Being Used by Spammers* (Winter 2003) <http://istpub.berkeley.edu:4201/bcc/Winter2003/feat.spamharvest.html> (discusses using images and other techniques to thwart harvesting spiders). Some Web site designers also use scripting languages, such as Javascript, in order to further obscure e-mail addresses. *See* Dan Thies, *Spam-Proofing Your Website* (Oct. 23, 2002) <http://evolt.org/article/Spam_Proofing_Your_Website/20/4189/>.

receipt of offensive e-mails.[87]

However, wise implementation of corporate information technology policy should take into account that all e-mail filtration techniques are not created equal. The frequency of "false positives" provides an instructive example of why these filtration methods are not created equal. A "false positive" refers to an e-mail that a user desires to receive but that has been filtered out and either deleted or placed into a rarely viewed suspect folder, oft titled "bulk mail."[88] Companies hawking filters claim great effectiveness with a minimum of "false positives."[89] The effective-

87. *See e.g.* Postini Corporation, *Why is Email Security So Critical?*, <http:www.postini.com/services/why_security_critical.html> (accessed Feb. 18, 2004) ("Spam containing offensive content, such as pornography, that comes in to a company through the e-mail system, can create a hostile work environment resulting in employee lawsuits — particularly if a company has not implemented an anti-spam solution"); Brightmail Corporation, *Business Benefits*, <http://www.brightmail.com/enterprise-benefits.html> (accessed Feb. 18, 2004) ("Filter out inappropriate and offensive content that may offend your employees. Employees have already begun to threaten to file lawsuits against their employers claiming that pornographic spam creates a hostile work environment"); Symantec Corporation, *Monitoring Email: Privacy Issues* (May 10, 2000), <http://enterprisesecurity.symantec.com/article.cfm?articleid=91&PID=na> ("Email content can be a potential mine field for sexual harassment and racial discrimination suits. Email is frequently used as evidence in these cases. Also, employers may face litigation for allowing this type of inappropriate email to traverse enterprise networks"); SurfControl Corporation, *Virtual Image Agent*, <http://www.surfcontrol.com/products/content/art_of_filtering/virtual_image_agent/default.aspx> (accessed Feb. 18, 2004) ("[i]f you are a corporate attorney, you know. Pornographic attachments are a major cause for legal liability. If you are a manager, you know. There is no excuse for the productivity losses and hostile work environment that result from online voyeurism"); MessageLabs Corporation, *Why Email Security: Face the Facts* <http://www.messagelabs.com/why/email/default.asp> (accessed Feb. 18, 2004) ("[i]t's not just about loss of productivity. Legal liabilities, IT resources, sexual harassment, HR issues, and company policies - they are all exposed to the real and ever increasing threats posed by email").

88. *See* SearchSecurity.com, *Glossary*, <http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci932649,00.html> (accessed Feb. 18, 2004) ("[i]n programs used to filter spam, a false positive is a legitimate message mistakenly marked as spam").

89. Postini Corporation, *Perimeter Manager Enterprise Edition* <http://www.postini.com/services/perimeter_manager.html> (accessed Feb. 18, 2004) (technology said to "maximize email filter accuracy and minimize false positives"); Brightmail Corporation, *Accuracy* <http://www.brightmail.com/accuracy.html> (accessed Feb. 18, 2004) ("fewer than 1 false positive in every 1 million messages identified as spam"); Symantec Corporation, Putting a Lid on Spam: an Update (Feb. 4 2004) <http://enterprisesecurity.symantec.com/article.cfm?articleid=3299&EID=0> (accessed Feb. 18, 2004) (best filters designed for minimum false positives); SurfControl Corporation, *SurfControl E-Mail Filter* <http://www.surfcontrol.com/products/email/spam_layers.aspx> (accessed Feb. 18, 2004) (filter designed to minimize false positives); MessageLabs Corporation, *Spam Protection — Features*, <http://www.messagelabs.com/services/spam/default.asp?section=241> (accessed Feb. 18, 2004) ("Minimizes false positives through ground breaking Skeptic technology").

ness of these systems as reported varies substantially.[90] The systems operate on different premises and with different biases. And although this space is not the appropriate forum for an in-depth review, executives setting communication policies should realize that the frequency of false positives in these filters varies. Some err on the side of eliminating spam, whereas others err on the side of delivering e-mail that may be spam. Whether these filters use a Bayesian filter,[91] spam-trap e-mail addresses,[92] a challenge-response system,[93] or review by actual human operators,[94] inevitably some filters will catch a greater percentage of

90. While it is easy to create a filter that catches all spam, or one that lets all good messages through, it is extremely difficult to create a filter that is able to do both. Individuals have claimed an accuracy rate of a spam filter as high as 99.98 percent, however this is typically due to tuning for the individual's preferences. *See* Bill Yerazunis, *Beyond 99.9% accuracy*, MIT Spam Conference (Jan. 16, 2004) <http://www.spamconference.com>. To create a spam filter that can achieve these results for a diverse population is a long way from being a reality. *Id.*

91. So called "Bayesian" filters rely on user-input and statistics to classify what messages constitute spam. *See* Paul Graham, *A Plan for Spam* (Aug. 2002) <http://www.paulgraham.com/spam.html>. While these filters are practical at the individual desktop level, they present problems when deployed at the server level. *See e.g.* Richard Jowsey, *Bayesian gateways*, MIT Spam Conference (Jan. 16, 2004) <http://www.spamconference.com>.

92. So called "spam traps" are e-mail addresses distributed specifically intended to be included on spammers mailing lists, but not given to any legitimate mailers. *See* SearchDomino.com, *Glossary: spam trap*, <http://searchdomino.techtarget.com/gDefinition/0,294236,sid4_gci815802,00.html> (accessed Feb. 18, 2004). Messages that arrive at these addresses can be inherently classified as spam and blocked when they are sent to legitimate addresses. *Id.* Brightmail, for example has a "probe network" of spam trap e-mail addresses. *See* Brightmail Corporation, *Brightmail Filtering Technologies*, <www.brightmail.com/pdfs/Brightmail_Filtering_Technologies.pdf§pamtrap£rightmail&hl=en&ie=UTF-8> (accessed Feb. 18, 2004). Individuals are staffed watching what messages arrive at these addresses. *Id.* They then build filter definitions based on the messages the spam traps receive. *Id.* These definitions are distributed to Brightmail's customers. *Id.*

93. Challenge-response systems work by responding with a "challenge" message to any e-mail senders. *See* Heinz Tschabitscher, *What You Need to Know About Challenge - Response Spam Filters*, <http://email.about.com/cs/spamgeneral/a/challenge_resp.htm> (accessed Feb. 18, 2004). The challenges typically require the sender to perform a task, which is easy for a human being but difficult for a computer (identifying whether a picture is of kittens or puppies). *Id.* If the sender correctly responds to the challenge then the message is delivered. *Id.* If not, the message is assumed to be spam. *Id.* Spammers, because of the volume of messages they send out and the fact they rarely use legitimate return addresses, cannot respond to the challenges. *Id.* As a result, their messages do not get through. *Id.* Several companies make challenge-response systems. *See e.g.* Mailblocks, <http://www.mailblocks.com> (accessed Feb. 18, 2004); Spam Arrest, <http://www.spamarrest.com> (accessed Feb. 18, 2004); *see also* Earthlink SpamBlocker, <http://www.earthlink.net/spamblocker/> (accessed Feb. 18, 2004) (even major Internet service providers such as Earthlink have begun implementing challenge-response systems for their customers).

94. Some anti-spam systems work by a network of human beings identifying whether messages are spam. *See e.g.* Cloudmark SpamNet, <http://www.cloudmark.com/products/spamnet/learnmore/howitworks.php> (accessed Feb. 18, 2004). These identifications are

spam than others.

The methodology and effectiveness of a filtration scheme must also be matched with a company's goals. For example, some companies might want to take the risk of false positives to rid their inboxes of the vast amount of spam. Others might fear missing a legal notice disguised as spam. The example of a marketing firm working with Pfizer to create a campaign for its Viagra medicine illuminates the problem.[95] Almost all of these filters take into account the ubiquitous unsolicited e-mail touting the availability of a low-cost herbal version of Viagra. The marketing firm sculpting a campaign for the flagship Pfizer drug must carefully choose a filtering regime. The marketing firm in that case will likely need to choose a filtering regime that errs on the side of permitting some spam into its inboxes.

If employing an effective filtering mechanism creates too large of an imposition on a company's business, i.e. by creating an impossibly large obstacle, companies can claim that the exposure to porn spam is one of the risks associated with working in a particular industry or on a particular project. Employers may still face the risk of being sued, but will have a better chance of prevailing. However, the consideration of remedial action and the rejection for cause will provide an employer with a friendly set of evidence to present to a court.

C. Reducing the Offensive Effect of Spam: Image Loading

One of the most effective techniques in preventing porn spam from becoming a liability for employers is for those employers to disable image loading in their e-mail client programs. Many e-mail clients give employers the ability to stop html image loading for incoming e-mail.[96] The effect of disabling image loading is that imbedded images in e-mails come up as unreadable gibberish or empty boxes in place of pictures. Even if offensive text remains, the more objectionable pictures will no longer be present. Words or descriptions are hard to read from a distance and thus will not have the same impact on the workplace as a large

---

shared with other users of the network. *Id.* Known as collective spam filtering, together the network of users can help identify messages and block them as they are received by other users. *Id.*

95. *See* Tony Kontzer, *Anti-spam Software Tries to Avoid Throwing Out the Good E-mail with the Bad,* <http://www.informationweek.com/story/IWK20030216S0001> (accessed Feb. 19, 2004) (describes the false positive issues of the Boston Celtics dealing with one of its sponsors, Pfizer and how filters picking up "Viagra" e-mails also threw away legitimate correspondence).

96. *See* Microsoft Corporation, *Introducing Outlook 2003* <http://office.microsoft.com/assistance/preview.aspx?AssetID=HA010714981033&CTT=98> (accessed Feb. 19, 2004). *See* Apple Computer, *Showing HTML Elements in Email* <http://docs.info.apple.com/article.html?artnum=151585> (accessed Feb. 19, 2004). *See* Qualcomm, *Computer Viruses and Email* <http://www.eudora.com/techsupport/kb/1612hq.html> (accessed Feb. 19, 2004).

offensive on-screen image. In addition, the removal of pictures has the effect of downgrading the offensive nature of the content. The less offensive or intrusive the content, the less pervasive or severe it is. Without the severity, sexual harassment claims become more difficult to substantiate.

Furthermore, the disabling of image loading will also prevent employees from receiving pornographic material from outside acquaintances. This prevents the viewing of such material in the workplace and/or disseminating it to fellow employees. Thus, such a technique not only weakens the effect inherent on pornographic spam, but also helps employers forestall other harassing behavior in the workplace that is ancillary to spam.

This technique may not be suitable for all companies. For example, an advertising firm might require liberal image loading in order for those companies to communicate efficiently internally and with their clients. Depending on the volume of material, companies could structure their e-mail clients to allow image loading from particular permitted addresses whether internal or external. However, for most companies there is no need for employees to receive HTML-based e-mail.

D. Encouraging Employees to Assist Employers in Creating a Positive Environment: Acceptable Use Policies Drafting and Enforcement

Generally, employers draft AUPs to proscribe certain employee behavior. There is certainly no one-size-fits-all AUP for employers to adopt. Employers' AUPs should be mindful of their industries and particular needs when drafting an AUP.[97] In addition to other restrictions that should be included in an AUP,[98] employers should include restrictions specifically targeted at reducing spam or limiting the impact of received messages on the work environment.

First, the policy should indicate that participation in USENET groups or other chat groups is not permitted. Because USENET groups are a place where spammers harvest e-mail addresses, employee participation in such groups risk disclosure to purveyors of pornography as well as other marketing messages. In addition to reducing the availability of

97. *See* Peter Brown, *Policies for Corporate Internet and E-mail Use*, 564 PLI/Pat 637, 672 (1999) ("[w]hile creating an Internet Use Policy may be critical, it is equally critical that such a policy is drafted in a way that fits the larger company culture. A company that permits limited telephone use, for example, should not try to draft an ironclad, 'no non-business use' Internet policy. Experience has shown that policies that run counter to the overall company culture often go unenforced. And from a litigation standpoint, an unenforced, or as is more likely the case, a selectively enforced, policy can sometimes be worse than no policy at all").

98. *Id.* at 670-673.

company e-mail addresses, thereby reducing potential liability, this policy has the advantage of keeping employees from the time wasting potential of newsgroups and chat rooms.[99]

Second, the policy should place limits on the use of public instant messaging programs like the AOL or the Yahoo programs. As a result of the increase of instant message spam, or spim, instant message programs have become another conduit for marketing messages.[100] As this "pipe" for marketing messages is used more prevalently, the risk that this conduit will be used by pornographers to the workplace is high.[101] The risk is particularly acute with respect to instant messaging programs because marketers that may be attempting to avoid legitimate businesses in their broadcasts have no way to distinguish between the public instant messaging IDs used for business purposes versus those used for personal purposes. Business people may protest that there are numerous benefits of instant messaging programs that they want to take advantage of and that proscribing these services is impracticable from a business standpoint.

This can be addressed in two ways. For companies that are large enough or have particular confidential information sensitivity, the establishment of an internal messaging program may be an attractive solution.[102] Not only does this alleviate the public access, which eliminates all spim, it prevents any eavesdropping risk inherent in public networks. The alternative for companies that want to utilize the public instant messaging programs is to outline in the AUP that all instant messaging programs will be: 1) used for business purposes only; and 2) configured to prevent access from any non-authorized individual.

Third, the AUP should proscribe employees from using their personal e-mail accounts in the workplace. Personal e-mail accounts can be

---

99. A more restrictive policy regarding posting any company e-mail address online might be even more effective. However, this may prove to be too difficult for companies or employees to abide by. The USENET and chat group limitations are good starts, but certainly can be supplemented by other restrictions regarding posting or e-mail address dissemination.

100. *See* Cara Garretson, *Coming Soon to Your IM Client: Spim* <http://www.pcworld.com/news/article/0,aid,114642,00.asp> (accessed Feb. 19, 2004). *See* also David McGuire, *Spammers Target Instant Message Users* <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contented=A36039-2003Nov13&notFound=true> (accessed Feb. 19, 2004).

101. Anita Hamilton, *You've Got Spim*, Time Mag. 77 (Feb. 2, 2004).

102. Numerous companies offer these types of software packages. *See* e.g. Dbabble, *Overview of DBabble Chat Server & Client* <http://netwinsite.com/dbabble/> (accessed Feb. 19, 2004); *ICRXpro Messenger* <http://www.ircxpro.com/products/default.asp?product=messenger> (accessed Feb. 19, 2004).

a conduit for pornography or offensive e-mail.[103] There is some indication that personal e-mail accounts receive a larger percentage of spam than work e-mail accounts.[104] Therefore, cutting this avenue off from spam receipt in the workplace can have a substantial impact.

Beyond the AUP techniques to reduce the amount of spam, other items in the AUP can be used to neutralize the impact of offensive spam. As well as potentially including some of the techniques discussed above in the AUP, these also include restrictions on: "clicking through" when pornographic spam is received; and forwarding messages with offensive content to those inside or outside the company.

Although drafting and adopting a strong AUP is a start, a company must make efforts to communicate and enforce the policy. Companies as a whole are not performing well in terms of distributing AUPs to their employees or monitoring the organizations compliance. Sixty-eight percent of companies that have AUPs are uncertain whether their employees have even seen their policy.[105] More troubling, seventy-nine percent of companies are unsure whether they are compliant with their policy.[106] One way to ensure that employees have seen the policy is e-mail distribution.[107] Because employers can keep audit records of an e-mail distribution (including potentially acknowledgment of receipt and acceptance) this provides a record keeping and distribution advantage over physical distribution or intranet posting.[108]

Enforcement of a policy is also a key to its effectiveness. By ignoring violators, corporate leaders send the message that violating the policy does not matter. A manual addressed to corporate chiefs considering AUPs highlighted:

> However well thought through the policy, any AUP will rapidly lose credibility and meaning if contraventions aren't penalised. If a policy clearly states that misuse such as a circulating pornography will incur disciplinary proceedings and threat of dismissal, these steps need to be seen to happen. Turning a blind eye devalues the policy, sends confusing messages to employees and encourages further misuse - if one 'offender' has been seen to be tolerated, how can others be fairly punished?[109]

The conclusion from the above observation is clear. No matter how carefully drafted, an unenforced policy will not serve a company well in ei-

103. *See* Caitlin Garvey, *Comment: The New Corporate Dilemma: Avoiding Liability in the Age of Internet Technoloy*, 25 Dayton L. Rev. 133, 158 (1999).

104. *See* Fallows *supra* n. 8. *See also* Unspam, *supra* n. 38.

105. Extend Technologies, *Why Most Acceptable Use Policies Fail?* <http://www.policymatter.com/press/whitepapers/items/44.asp> (accessed Feb. 19, 2004).

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.*

ther its risk reduction efforts or its promotion of a positive work environment.

E. KEEPING CURRENT: REGULAR AND PERIODIC REVIEW OF COMPANY POLICIES AND PROCEDURES

Technology continues to change very rapidly. As the technological or legal backdrop changes, companies must adopt new policies and practices to change with the times. For example, instant messenger spam is a relatively new phenomenon.[110] Employers that addressed the spam problem prior to the advent of spim will not have adequate technology, policies or procedures to address the issue. This is but an example of change that could render company anti-spam efforts out of date. As new legislation, anti-spam technologies and techniques, and methods by spammers are adopted, companies need to update their policies and procedures.

In order to prevent gaps in spam policies for long periods of time, companies should schedule periodic reviews of their anti-spam efforts. These reviews could involve only internal analysis. However, they can be bolstered by analysis from third-party technological and legal experts. These third parties may help companies perform such tasks as choosing the appropriate filter, adapting to new anti-spam laws, addressing risks that become apparent from lawsuit precedents, and auditing compliance with companies that schedule reviews of their efforts on a regular basis, e.g. once a quarter, will have a much better chance of adapting to changes or anticipating potential spam problems. In addition, any company that adopts solid policies and has periodic review will be able to use that as evidence that it has taken all prudent steps to guard against a hostile work environment.

IV. CONCLUSION

While the risk is not absolute or predictable, businesses face a potential large risk of liability if they ignore the problem of pornographic spam in the workplace. The expansion of the employer's liability for third party actions as well as the overall environment encouraging litigation in the sexual harassment context should give businesses pause from a legal standpoint. More practically, employers should be aware of the disruption that this material has in the workplace. With some reasonable steps, employers can minimize the legal risks and the practical disruptions. These steps include: 1) protecting company e-mail addresses from public disclosure through disguise of concealment; 2) filtering e-mail thereby preventing offensive spam from getting to employees' desktops;

110. *See supra* nn. 101, 102.

3) reducing porn spam's impact by disabling image loading; and 4) adopting an appropriate AUP. However, companies must be ever vigilant to the problem and adapt their policies and technologies over time. Such adaptation requires regular and periodic review not only of the policies and procedures, but also of the technological landscape.