ARTICLE

HOW EMPLOYERS CAN PROTECT THEMSELVES FROM LIABILITY FOR EMPLOYEES' MISUSE OF COMPUTER, INTERNET, AND E-MAIL SYSTEMS IN THE WORKPLACE

LOUIS J. PAPA AND STUART L. BASS*

* Louis Papa, J.D., Brooklyn Law School; M.B.A. Computer Information Systems, Baruch College; B.A., Spanish/Political Science, State University of New York at Buffalo. Mr. Papa is licensed to practice law in New York, New Jersey and Washington, D.C. Since April 1993, he has managed his own law practice. He currently specializes in Civil Litigation on behalf of Insurance Companies and engages in transactional work in the Entertainment field. Mr. Papa has approximately thirteen years of teaching experience. He has been teaching at Hofstra University since the fall of 1998 and is currently an Assistant Law Professor in the Zarb School of Business teaching undergraduate and M.B.A. law classes. He has published articles in numerous fields and was recently cited by the ninth circuit Court of Appeals. He also had a case that he successfully defended and was reported in the Appellate Division, 2nd Department and was denied leave by the New York State Court of Appeals. Another successful case was reported in the New York Law Journal. Professor Papa continues to lecture on behalf of Corporations and at various conferences throughout the continental United States.

Stuart L. Bass, J.D., M.P.A. Professor Bass is an Associate Professor of Legal Studies at the Frank G. Zarb School of Business at Hofstra University. Professor Bass teaches a full range of business law courses including labor and employment and dispute resolution. Professor Bass has authored articles in leading law reviews and journals on legal ethics, employment discrimination, arbitration and statutory discrimination claims and securities regulations. Professor Bass serves as a mediator and arbitrator on several regional and national panels including the NYS Public Employment Relations Board, the NYS Employment Relations Board, NASD Regulations, Inc., the Federal Mediation and Conciliation Service and numerous state and local law enforcement panels.

The authors wish to gratefully acknowledge Brad Smith, a third year law student and editor-in-chief of the Journal of International Business & Law at the Hofstra University School of Law, for his able and outstanding research, his time, dedication and assistance in the preparation and editing of this article. We also wish to express our thanks and appreciation to Brett Millman, M.B.A. candidate, May, 2004 for his research and support in the development of the article.

TABLE OF CONTENTS

I. INTRODUCTION

In the workplace today, the use of computers and computer-related technology, such as the Internet and e-mail, continues to grow at a tremendous rate. Numerous employees in America and throughout the world use computers and related technologies. Not only do these computers have Internet access and numerous programs, but their use is accompanied by a great deal of responsibility. The amount of illegal activities that employees can perform from their computers has dramatically increased over recent years. Using their computers, employees can send threatening or sexually harassing e-mails from their workplace, copy and distribute confidential information, gain unauthorized access to others' computers and download and distribute illegal pornography.[1] Therefore, employers must protect themselves from the threat of liability by creating and requiring their employees to sign electronic equipment policy statements. Employees will waive their right of privacy and allow employers to monitor the use of their computers.

This Article advocates that employers create electronic equipment policy statements in order to significantly limit their liability from employees' misuse of computer systems. Part II discusses how computers, the Internet, and e-mail are all utilized by employees at a growing rate to participate in wrongful or illegal acts within the workplace. Part III discusses the theories of respondeat superior and negligent retention, where employers could be held both civilly and criminally liable for their employee's actions. Part IV analyzes cases where the employee's right to privacy was at issue and where computer usage policy statements played a significant role in helping to limit liability. Part V provides an example of an effective and currently used electronic equipment policy statement that was created by an employer and given to his or her employees, along with other suggestions to limit the employer's liability. Part

[1] Jonathan Bick, Respondeat superior applies to online activity; Internet-use policies are critical to protect employers from employees' illegal Internet acts, 169 NEW JERSEY L.J. 28 (August 26, 2002).

VI concludes this Note by analyzing the importance of an electronic equipment policy statement for employers in their everyday business operations.

II. COMPUTER USE AS SEXUAL HARASSMENT

Among the most common and preventable difficulties created by employees misusing the Internet and currently facing employers is sexual harassment. Today, e-mail serves as a useful means for employees to harass other workers within the workplace, along with those outside of the workplace, during the course of their work day.[2] Ordinarily, employees engaging in sexual harassment utilize the employer's Internet service provider to download obscene material and the employer's e-mail system to distribute it, and as a result, the company risks facing sexual harassment charges.[3] These obscene or pornographic images could create liability for an employer if recipients, finding these images offensive, file sexual harassment charges.[4] Additionally, openly viewing sexually explicit online sites could be within the definition of "intimidation" that can create a "hostile work environment," which the Supreme Court has found is a form of sexual discrimination.[5] Similarly, "pervasive use of derogatory and insulting terms" aimed at male and female employees can also create a "hostile work environment."[6]

Several well-known corporations have already faced lawsuits that are based on Internet-related sexual harassment claims. For example, in 1990, a division of Calsonic International, Inc. in Shelbyville, Tennessee was sued by one of their female employees for $2.5 million.[7] In the lawsuit, she claimed that her supervisor subjected her to various forms of sexual harassment, including using the company's e-mail system to send her vulgar comments.[8] In another case, Microsoft Corporation was sued by a former female employee who was fired in 1990.[9] She claimed that she was not promoted by her manager due to

---

[2] *See id.*

[3] Trip Gabriel, *New Issue at Work: On-Line Sex Sites*, N.Y. TIMES, June 27, 1996, at C1; *see also* Erin M. Davis, *The Doctrine of Respondeat Superior: An Application to Employers' Liability for the Computer or Internet Crimes Committed by Their Employees*, 12 ALB. L.J. SCI. & TECH. 683, 697 (2002).

[4] *See* Gabriel, *supra* note 3; *see also* Davis, *supra* note 3.

[5] Meritor Savings Bank v. Vinson, 477 U.S. 57, 66 (1986) (holding that an employer may not need to have actual notice of improper conduct of an employee to be held liable for the employee's acts).

[6] *See* Davis, *supra* note 3; *see also* Andrews v. City of Philadelphia, 895 F.2d 1469, 1485 (3d Cir. 1990).

[7] Mitch Betts & Joseph Maglitta, *Is Policies Target E-Mail Harassment*, COMPUTER WORLD, Feb. 13, 1995, at 12.

[8] *Id.*

[9] *See* Stephanie Dahl, *Dangerous E-Mail: Companies are Finding that E-Mail Indiscretions Can Leave Them Legally Vulnerable*, INFORMATION WEEK, Sept. 12, 1994, at

her gender, and that the manager sent e-mail messages to her and other employees that were offensive to women.[10] According to the employee, these messages included innuendo about male genitalia and other sexual references.[11] Usually, the employers' failure to appropriately control e-mail usage results in a finding that is against the employer.

Recently, with the emergence and continued growth of electronic communications, harassment claims by employees based on the transmission or receipt of inappropriate e-mails have become quite common. Employees utilizing the e-mail system improperly often allows for the "instantaneous, and usually thoughtless, dissemination of inappropriate material to broad groups of people," while creating potential liability for the employer.[12] Because of this possibility, employers must be able to fully investigate an employee's use of his computer in the course of his employment.[13] This ability is beneficial to employers in two distinct ways: first, it allows employers to prevent harassment within the workplace, and second, it allows employers to properly defend themselves if they become part of a lawsuit on this matter.[14]

III. DOCTRINES OF RESPONDEAT SUPERIOR AND NEGLIGENT RETENTION

Under the doctrine of respondeat superior and the alternative theory of negligent retention or supervision, elements of foreseeability and negligence play an important role. If the employer "knew or should have known" that its employee was participating in a criminal activity and "it failed to act, or failed to inquire," then liability could be imposed.[15] The dominant theory is if an employer does not provide an adequate defense for liability under respondeat superior, and if an employee uses its employer's computer in committing a crime, the employer should be held criminally liable.[16] Increasingly, employees are committing serious acts with the use of their work computers and Internet connections.[17] Since the legislature and the penal codes are not keeping pace with the increase of computer crimes, there is a "general lack of

12.

[10] *See id.*

[11] *See id.*

[12] Michael J. Crowley & Christian A. Aviza, *Electronic investigations; Do an employer's interests prevail over employee privacy concerns?*, 9 CORPORATE COUNSEL A7 (August 2002).

[13] *See id.*

[14] *See id.*

[15] Doe v. United States, 912 F. Supp. 193, 194 (holding the employer partly liable because the employee's acts were foreseeable and the employer knew or should have known of the risk posed); *see also* Davis, *supra* note 3, at 709.

[16] *See* Davis, *supra* note 3, at 709.

[17] *See id.*

adequate penal and statutory laws" to deal with these new "tech" types of crimes committed by employees.[18] Many recommend that courts should turn to alternative theories, such as respondeat superior, to find employers criminally liable.[19] This will partially ensure that society will find "appropriate retribution" and that employers will be "encouraged to take adequate precautions and measures in monitoring and investigating possible criminal activity that is occurring in their workplaces."[20]

Under the doctrine of respondeat superior, the actions of an employee acting within the scope of employment are the means of imputing intent and guilty acts to the employer.[21] For an employee's conduct to fall within the scope of employment, the conduct must be of the type that "the employee is employed to perform and that generally occurs during the time of employment."[22] The Restatement of Agency depicts the traditional test adopted by most jurisdictions to determine whether an employee's conduct falls within the limits of the "scope of employment" providing that:

The conduct of the employee is within the scope of employment if:

1. It is of the kind the employee is employed to perform;
2. It occurs within authorized space and time limits;
3. Some or all of it is done to serve the employer, and;
4. If the employees use force against another.[23]

The conduct of the employee is said to not be within the scope of employment if it is "different in kind from that authorized," beyond the authorized space or time limits, or "too little activated by a purpose to serve the master."[24] Additionally, it is beneficial for the employee if the activity in question meets at least some of the employer's objectives.

History shows that courts limit the situations when an employer may be liable for employees' wrongful acts. They generally hold that acts which are purely motivated by personal interests or are outrageous in nature are to be deemed as outside the scope of employment.[25] However, courts are willing to expand employer liability in instances where the employee's acts only benefit the employee.[26] Therefore, courts have found that an injury may be considered

[18] *See id.*

[19] *See id.* at 709-10.

[20] *See id.*

[21] *See* Bick, *supra* note 1.

[22] *See id.*

[23] *See* Davis, *supra* note 3, at 690.

[24] RESTATEMENT (SECOND) OF AGENCY § 228 (1957).

[25] *See* Bick, *supra* note 1.

[26] *See id.*

to occur outside the scope of employment if its origin is somehow connected with the employment so that there is "a connection between the employment and the injury."[27] As a result, employers may be held vicariously liable when one of their employees harms another because of the opportunity that the job offers.[28]

On the other hand, in cases where the employee's tortious conduct cannot result in any violation under respondeat superior, courts have displayed a willingness to recognize the negligent-retention theory.[29] This doctrine holds employers liable for negligence when the employer either negligently retains or manages the employee tortfeasor.[30] Significantly, even when an employee is not acting within the scope of employment, an employer could be liable under the negligent-retention doctrine.[31] This doctrine holds an employer responsible when he places an "unfit person in an employment situation involving an unreasonable risk of harm to others."[32] The negligent-retention theory is also utilized when the employer "fails to properly oversee the conduct subject to his/her control."[33]

Besides being held civilly liable, an employee's Internet activities could also create criminal liability for his employer. It is becoming more common for companies to be held criminally responsible for the improprieties of their directors, managers, supervisors and employees, especially when a company fails to establish and enforce corporate policy.[34] Importantly, courts do not impose strict liability for the actions of mischievous employees.[35] Under the doctrine of respondeat superior and negligent retention, there are elements of both foreseeability and negligence encompassed within them and these are necessary to help in analyzing liability.[36]

IV. CASES INVOLVING EMPLOYER LIABILITY, INTERNET USE AND RIGHT TO PRIVACY

Although many employees engaging in wrongful or illegal activities are acting alone, some employers may be held liable for their employees' actions. In 1909, in *New York Central v. United States*, the Supreme Court found that "a corporation could be held criminally liable for the acts, omissions or failures

[27] *Id.*
[28] *See id.*
[29] *See id.*
[30] *See id.*
[31] *See* Bick, *supra* note 1.
[32] *Id.*
[33] *Iid.*
[34] *See id.*
[35] *See id.*
[36] *See id.*

of an agent acting within the scope of his or her employment."[37] This is because the corporation acts through its agents and employees "whose knowledge and purpose may be attributed to the corporation."[38] Corporations are "legal entities," while their employees, since they act on behalf of the corporation, can serve as a "means of imputing intent and guilty acts to the corporation."[39] This is known as respondeat superior, where an employer can be held liable for the acts of their employees.

What can employers do to save themselves from being held criminally liable for the actions of their employees? The following case illustrates what precautionary measures employers should take. In *TBG Insurance Services Corporation v. Superior Court of Los Angeles*, the employee who was also one of the company's senior executives, Robert Zieminski, was fired for misuse of his office computer by accessing pornographic websites.[40] The employer, TBG, provided two computers for his use, one for the office and one for home.[41] When the employee sued the employer for wrongful termination, the employer demanded that Zieminski produce the home computer and he refused by claiming he had a "right to privacy to the information stored on the computer."[42] However, TBG protected itself by having Zieminski sign his employer's "electronic and telephone equipment policy statement" when he received his computers and he agreed in writing that his employer could monitor his computers.[43] The California Court of Appeals concluded that because the employee consented to his employer's monitoring of both computers, that employee had no reasonable expectation of privacy when he used his home computer for his personal matters.[44]

By signing this policy statement, the employee "acknowledged and agreed" that the employer could access and review his computer files and that none of the information on the computer should be considered private.[45] Basically, the court found that when Zieminski signed the statement, he waived any right to privacy related to the home computer that TBG provided him.[46] In this statement, he agreed to use the computers for "business purposes only and not for personal benefit or non-Company uses, unless such was expressly

[37] New York Cent. v. United States, 212 U.S. 481 (1909); *see also* Bick *supra*, note 1.

[38] *See* Bick, *supra* note 1.

[39] *See id.*

[40] TBG Ins. Services Co. v. Superior Court of Los Angeles, 96 Cal. App. 4th 443 (Cal. Ct. App. 2002); *see also* Crowley & Aviza, *supra* note 12, at A8.

[41] TBG Ins. Services Co., 96 Cal App. 4th at 446.

[42] Crowley & Aviza, *supra* note 12, at A8.

[43] TBG Ins. Services Co., 96 Cal App. 4th at 446.

[44] *See* Crowley & Aviza, *supra* note 12, A8.

[45] *See id.*

[46] *See id.*

approved."[47] Zieminski also agreed with the statement's provision that the computer and/or system cannot be "used for improper, derogatory, defamatory, obscene or other inappropriate purposes."[48] Additionally, the employee understood that improperly using the computers could result in disciplinary action, such as discharge.[49]

This case's holding displayed the benefits and necessity of a "well-structured" computer and electronic media policy for employers.[50] Company policies designed to limit the employee's right of privacy can be extremely effective for companies involved in electronic investigations. Additionally, they are also quite useful in shielding the lawyer from liability.

In Utah, a similar circumstance arose in *Autoliv ASP v. Department of Workforce Services*.[51] Two employees, Thomas A. King and Christopher Guzman, were found to have sent sexually harassing and offensive e-mails to a former employee.[52] On numerous occasions, King and Guzman had violated the employer's policy against the transmission of sexually oriented and clearly offensive e-mail messages.[53] Eventually, the employees were fired for their behavior and "improper and unauthorized use of company e-mail."[54] The employees did not refute the fact that the messages had been sent, but they did say they were unaware that their actions were against the employer's policy and could result in immediate termination.[55] One appeals board found that while King and Guzman were responsible, the element of knowledge was missing, leaving no just cause for their discharge.[56] However, the Court of Appeals of Utah reversed, holding that the e-mail transmission of sexually explicit and offensive jokes, pictures, and videos, resulted in a "flagrant violation of a universal standard of behavior." As a result, the employees were discharged for just cause.[57]

In *Garrity v. John Hancock Mutual Life Insurance Co.*, two employees were terminated after the employer examined inappropriate sexual e-mails they sent within the office after doing an investigation based on a harassment complaint.[58] Both of these employees received these inappropriate e-mails

[47] TBG Ins. Services Co., 96 Cal App. 4th at 446.

[48] *Id.*

[49] *Id.*

[50] *See* Crowley & Aviza, *supra* note 12, at A8.

[51] Autoliv ASP, Inc. v. Dep't of Workforce Services, 29 P.3d 7 (Utah Ct. App. 2001).

[52] *Id.* at 9.

[53] *Id.*

[54] *Id.* at 10.

[55] *Id.*

[56] *See id.*

[57] *Autoliy ASP, Inc*., 29 P.3d at 10.

[58] Garrity v. John Hancock Mutual Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist.

"involving sexual content" on a regular basis and then transmitted them to fellow employees.[59] The two employees claimed that the employer had invaded their privacy by reviewing their e-mails, illegally intercepted wire communications, wrongfully discharged them, and defamed them.[60] Essentially, the issue at hand was whether the expectation of privacy was reasonable.

Even though the employer, Hancock, had an internal e-mail policy, which explained that all of the information on the system was the company's property and that they reserved the right to access all of the e-mail files, the U.S. District Court in Massachusetts found "that even in the absence of a company e-mail policy, plaintiffs [the former employees] would not have had a reasonable expectation of privacy in their work e-mail."[61] In reaching this holding, the court relied upon the idea that, because the e-mails were communicated to other parties (the coworkers) and because Hancock was entitled to "look at e-mail on the company's intranet system," the two terminated employees had "no reasonable expectation that the e-mails would remain private." Therefore, the employees had "no enforceable right of privacy based upon the e-mails."[62] The court also found that even if the former employees "had a reasonable expectation of privacy in their work e-mail, [Hancock's] legitimate business interest in protecting its employees from harassment in the work place would likely trump" the two former employees' privacy interests.[63] Both federal (Title VII of the Civil Rights Act of 1964) and state (Massachusetts General Laws c. 151B) anti-discrimination statutes require the employer to "take affirmative steps to maintain a workplace free of harassment and to investigate and take prompt and effective remedial action when potentially harassing conduct is discovered."[64] Therefore, the court believed that the employer's legal obligation to investigate sexual harassment

LEXIS 8343, at *1 (Mass. Dist. Ct. 2002); *see also* Crowley & Aviza, *supra* note 12.

[59] *See* Crowley & Aviza, *supra* note 12.

[60] *See Garrity*, No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *3.

[61] *Id.* at *5-6; Crowley & Aviza, *supra* note 12; Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding that even in the absence of a company e-mail policy, the plaintiffs would not have had a reasonable expectation of privacy in their work e-mail to a supervisor. This is because "once the plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.").

[62] *See Garrity*, No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *5-6; Crowley & Aviza, *supra* note 12.

[63] *See Garrity*, No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *6; Crowley & Aviza, *supra* note 12.

[64] *See Garrity*, No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *6; Crowley & Aviza, *supra* note 12; Faragher v. City of Boca Raton, 524 U.S. 775 (1998); Burlington Indus., Inc. v. Ellerth, 524 U.S. 742 (1998).

of which they are aware would likely "trump" any right of privacy in the terminated employee's e-mails.[65]

Another important case, *Haybeck v. Prodigy Services*, has been the focus of numerous debates in the area of Internet-related sexual harassment.[66] Jacob Jacks, a computer technical advisor for Prodigy Services Company, repeatedly entered an online "sex chat room" while at work.[67] Jacks' motive was to become friends with the plaintiff, Barbara Haybeck, in attempting to entice her to engage in sexual intercourse with him. Jacks, who had AIDS and a history of being a "sexual predator," continuously used the Internet access provided by the employer to spend excessive amounts of time chatting online with Haybeck.[68] Eventually, Jacks persuaded Haybeck to have sexual intercourse with him.[69] However, at all instances during their initial e-mail communications and throughout their relationship, Jacks always denied having AIDS.[70] As a result of her relationship with Jacks, Haybeck contracted AIDS.[71] She subsequently filed a lawsuit against Jacks' employer, Prodigy services, for its "negligence, carelessness, recklessness and gross negligence . . . in [Prodigy's] ownership, operation, management, repair and control of [its] online network."[72]

In this case, the court dismissed Haybeck's claim against the employer, Prodigy, under the doctrine of responsdeat superior.[73] In its findings, the court held that an employee's actions cannot fall within the scope of employment when such actions are entirely personal in nature.[74] Even though the court did not specifically declare Jacks' actions outrageous, that his actions were "so out of the ordinary and appalling that they could not have furthered any employer's interest" can easily be inferred.[75]

Moreover, there are several indications that the employer's interest was not being furthered in the *Prodigy* case. One indicator that Jacks' was not furthering Prodigy's business was his decision not to disclose the fact that he had AIDS.[76] Instead, concealing this information likely arose from a personal

---

[65] *See* Crowley & Aviza, *supra* note 12.

[66] Haybeck v. Prodigy Services, 944 F. Supp. 326 (S.D.N.Y. 1996); *see also* Davis, *supra* note 3, at 698.

[67] *See Haybeck*, 944 F. Supp. 326; *see also* Davis, *supra* note 3, at 698.

[68] *See Haybeck*, 944 F. Supp., at 328; *see also* Davis, *supra* note 3, at 698.

[69] *See Haybeck*, 944 F. Supp., at 328; *see also* Davis, *supra* note 3, at 698.

[70] *See Haybeck*, 944 F. Supp., at 328; *see also* Davis, *supra* note 3, at 698.

[71] *See Haybeck*, 944 F. Supp., at 328; *see also* Davis, *supra* note 3, at 698.

[72] *See Haybeck*, 944 F. Supp., at 328; *see also* Davis, *supra* note 3, at 699.

[73] *See Haybeck*, 944 F. Supp., at 329; *see also* Davis, *supra* note 3, at 699.

[74] *See Haybeck*, 944 F. Supp., at 329; *see also* Davis, *supra* note 3, at 698.

[75] *See Haybeck*, 944 F. Supp., at 331; *see also* Davis, *supra* note 3, at 699.

[76] *See Haybeck*, 944 F. Supp., at 330; Davis, *supra* note 3, at 699; *see also*

motivation of Jacks that was "far removed from the purpose of serving his employer."[77] Additionally, Jacks use of the Internet as a tool for his personal satisfaction, did not serve the interest of Prodigy; consequently, it may be viewed as falling outside the "scope of employment" component of respondeat superior.[78] According to the traditional theory of respondeat superior liability, employer liability will not be "imposed if the employee commits wrongful acts that are so outrageous that they fall outside of the scope of employment" without furthering any of the employer's interests.[79] Therefore, under the traditional application of "scope of employment," the court in *Prodigy* correctly decided that the employer was not liable.[80]

RESTATEMENT, *supra* note 28, at §§ 228, 243.

[77] *See Haybeck*, 944 F. Supp., at 331; Davis, *supra* note 3, at 699; *see also* RESTATEMENT, *supra* note 28, at §§ 228, 243.

[78] *See* Davis, *supra* note 3, at 699.

[79] *See* RESTATEMENT, *supra* note 28, at § 228.

[80] *See Haybeck*, 944 F. Supp., at 331; *see also* Davis, *supra* note 3, at 699.

V. EXAMPLE OF INTERNET USE AGREEMENT AND OTHER SUGGESTIONS TO REDUCE EMPLOYER'S LIABILITY

To reduce the risk of liability under the doctrine of respondeat superior, employers should take three preventive actions. First, employers "should adopt appropriate Internet-use policies and procedures prohibiting illegal and wrongful Internet conduct."[81] Second, employers should use notices and training sessions to make their employees aware of the organization's Internet-use policy.[82] Third, employers should enforce this Internet-use policy "by taking prompt action in the event that they become aware of illegal or wrongful activity of their employees."[83]

The essential purpose of an Internet-use policy is to minimize the risks of Internet use without inordinately limiting its use. Essentially, a properly prepared and completely implemented Internet-use policy is one of the employer's best defenses against liability under respondeat superior.[84] An appropriate policy should be tailored to reflect and meet the specific needs of the employer.[85] Most of these Internet policies, though, will share some common elements.[86] For example, most policies should "emphasize that Internet use is for business purposes only and that sexual harassment is strictly prohibited."[87] Additionally, the employees should be informed that "adherence to the Internet policy is a condition of employment."[88]

This Internet policy "should be in writing and be easily accessible to employees," especially on the computer they use in accessing the Internet.[89] Furthermore, the employer should distribute a copy of the Internet policy to each employee, have the employee sign it, and put it in the employee's personnel file.[90] The employer should also state that is "openly monitoring its employee's Internet and e-mail activities."[91] Moreover, the policy should include a provision explaining that "the employee has read, understood, and comprehends the policy and agrees to follow the instructions of the employer"

---

[81] *See* Bick, *supra* note 1, at 29.

[82] *See id.*

[83] *See id.*

[84] *See id.*

[85] *See id.*

[86] *See id.*

[87] *See* Bick, *supra* note 1, at 29.

[88] *See id.*

[89] *See id.*

[90] *See id.*

[91] *See* Davis, *supra* note 3, at 711; *see also* Ruth Hill Bro, *E-Mail in the Workplace*, in ONLINE LAW: THE SPA'S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET, at 422 (Thomas J. Smedinghoff ed., 1996)

because without this statement the employer will likely not be protected from liability.[92] It is essential that this policy includes a provision stating that "the employee understands and agrees to follow the organization's Internet policy."[93] This policy must be "known by the employees and enforced by the employer," so that it will be more likely that the policy can shield the employer from liability.[94] As part of an employer's Internet access, it is important and highly recommended that employees be notified that their Internet use will be governed by the employer policy.[95] Moreover, employers wanting to avoid liability "should take prompt action in the event that they become aware of illegal or wrongful activities of their employees."[96]

An employer can protect itself and minimize the risk of facing liability for the illegal online acts of their employees through "the formulation, distribution, and enforcement, of . . . [a company] policy that emphasizes that all e-mail and computer bulletin board communications are for business purposes [only] and that sexual harassment and other offensive communications are strictly prohibited."[97] Additionally, in this policy, the employer should warn employees that any violations of these standards could serve as a cause for disciplinary action, including termination of their employment.[98]

Creating such Internet and e-mail policies potentially achieves two favorable outcomes. First, these policies would provide employees with guidance about appropriate use of the Internet and e-mail systems at their workplace. Second, these policies would play a significant role in sufficiently protecting the employer from liability.[99]

---

[92] *See* Davis, *supra* note 3, at 711; Louise Ann Fernandez & Jennifer Rappoport, *Workplace Claims: Beyond Discrimination*, in 30th ANNUAL INSTITUTE ON EMPLOYMENT LAW, 1221, 1230 (Practicing Law Institute, Litig. & Admin. Prac. Course Handbook, Series No. H0-00AP, Oct. 2001), *available in* WL 662 PLI/Lit 1221 (discussing how under proposed legislation employees must be appropriately notified of any electronic communication monitoring policy); John Araneo, Note, *Pandora's (E-Mail) Box: E-Mail Monitoring in the Workplace*, 14 HOFSTRA LAB L.J. 339, 351 (1996) (stating that case law establishes a need for "actual proof of notice" of the policy).

[93] *See* Bick, *supra* note 1, at 29.

[94] *See id.*

[95] *See id.*

[96] *See id.*

[97] *See* Bro, *supra* note 91, at 419; *see also* Robert M. Barker et al., *E-Mail Issues,* INTERNAL AUDITOR, Aug. 1995, at 60 (describing how simple company e-mail policies will help in limiting potential legal issues from developing and providing general instructions for formulating a company e-mail policy).

[98] *See* Davis, *supra* note 3, at 711.

[99] Peter Brown, *Policies for Corporate Internet and E-Mail Use*, in THIRD ANNUAL INTERNET LAW INSTITUTE 637, 672 (Practising Law Institute 1999), *available in* WL 564

For a policy to protect the employer from liability, it is essential that it be strictly enforced. In addition providing the employee with a copy of the policy, it's advised that employers install a "pre-log-on screen" into the system, which will notify employees each time they start their computer that their use of it is "subject to and governed by employer policy."[100] Within this policy, employees should be cautioned that the Internet is "not a secure document" and can be "accessed by others."[101] Furthermore, the policy should inform employees that "backup files exist within the employer's database systems" and may be retrieved by a plaintiff choosing to file a lawsuit against the employee or the employer[102]. With employers implementing and monitoring these policies, their exposure to liability claims can be limited.

Importantly, courts will continue to demand that employers carefully supervise their employees, especially if the employer becomes aware of misconduct or illegal activity, but Internet policies can certainly serve as a defense against employer liability claims.[103]

The following is an example of an Internet use policy drafted by the authors and that can be utilized by an employer:

> I, _____, realize that electronic communications are to be used solely for company business, and that the (company name) (hereafter known as "the Company") reserves the right to monitor or access all employee Internet or e-mail usage. Furthermore, I am fully aware that the Company will keep copies of Internet or e-mail passwords, and that the existence of such passwords is not an assurance of the confidentiality of the communications.
>
> This Company also does not tolerate the following:
>
> > The transmission of any discriminatory, offensive or unprofessional messages.
> >
> > Access to any Internet sites that are discriminatory or offensive.
> >
> > Posting personal opinions on the Internet using the Company's access, particularly if the opinion is of a political or discriminatory nature.
>
> Lastly, I am fully aware that my use of computers in the employment

PLI/Pat 637 (discussing that an employer should provide notice to its employees that communications over the Internet, including e-mails, will not be confidential and could be monitored); *see also* Bro, *supra* note 91, at 421.

[100] Laura B. Smith, *Electronic Monitoring Raises Legal and Societal Questions*, PC WEEK, June 28, 1993, at 204.

[101] *See* Jim Galvin, *The Internet is Not Secure: So What?*, available *at* http://www.commerce.net/research/reports/1998/98 04b.html (last visited April 1, 2003).

[102] *See* Davis, *supra* note 3, at 712.

[103] *See id.*

> context carries with it social norms that effectively diminish my reasonable expectation of privacy with regard to my use of the company's computers. Any violation of the above agreement may result in termination of my employment.
>
> Agreed by:
>
> _____
>
> Employee

However, it remains completely possible that an employer's Internet policy prohibiting the use of the computer and Internet for "non-business, offensive, and/or illegal conduct" might actually weaken an employer's defense in some instances.[104] If an employer has an existing policy but fails to enforce this policy, or if the employer is aware of an employee's wrongful or illegal actions but fails to take quick action, then the employer generally will not be shielded from liability.[105] Significantly, the key action in avoiding liability for any employer is implementation and enforcement of an appropriate Internet use policy.[106]

The courts can make it very difficult for the employers to protect themselves from being held liable for the acts of their employees. Along with having employees sign an agreement, there might be a need for more. Some employers might want to look into hiring an intra-office computer supervisor to monitor the employee's daily actions.

Any employer with a computer-friendly workforce bears great responsibilities. These employers will be sometimes forced to take unpleasant actions in order to protect themselves from the actions of their employees. Extra computer and Internet security should be hired. One possible solution is to have certain harassing words or documents "flagged" and make electronic correspondence containing those "flags" unable to be sent by employees. The employer must also remember to have their employee sign an electronic policy statement when hired. Unfortunately, data entry is not the only thing that employees use their computers for anymore. Many times, the employer ends up paying the price due to their employees' wrongful acts. The employer needs to face the harsh reality that is respondeat superior and therefore take every precaution necessary to guard their interests.

---

[104] *See* Davis, *supra* note 3, at 712; Terex Corp. v. UAW Local 1004, No. CIV.A. 2:97 CV243-D-B, 1998 WL 433948, at *7 (N.D. Miss. June 17, 1998) (stating that once an employer has knowledge of its employee's wrongful acts, the employer must take prompt action or face liability).

[105] *See* Davis, *supra* note 3, at 712.

[106] *See id.* at 712-13.

VI. CONCLUSION

With the growth of computers, the Internet, and e-mail, numerous legal issues develop for the employer. Since the Internet and e-mail enhance the opportunities for illegal online activity, employees offering computer and Internet use within the workplace are potentially liable to the victims who suffer from their employees' crimes. Without a doubt, employers need to be aware and monitor their employee's online activity, so they can limit their liability for their employee's illegal or wrongful conduct. Courts can hold employers liable under two different theories – respondeat superior and negligent retention. Under the theory of respondeat superior, a court may hold an employer liable if it is determined that the employee's acts were within the "scope of their employment."[107] Under the theory of negligent retention, the court can also hold an employer liable if the employer did not take any remedial measures to stop illegal or wrongful activity when the employer "knew or should have known" of these problems within the workplace.[108]

Most importantly, employers need to protect themselves by reducing their risk of liability for employees' misuse of computer, Internet, and e-mail systems in the workplace. To limit their liability, the employer should adopt strict and defensive Internet and computer use policies and procedures that prohibit illegal and wrongful computer and online conduct.[109] As the *Garrity* case in Massachusetts and the *TBG Insurance Services Company* case in California prove, it is of the utmost importance to develop and implement a "well-structured" company policy dealing with the use of computers and electronic communication systems by employees. This policy must establish that employees should have "no expectation of privacy in the use of company computers, e-mail systems or other electronic communication."[110] Creating a Internet and computer use agreement with the assistance of legal counsel that clearly outlines what employees are permitted to do and prohibited from doing on their work computers, along with appropriate adhesion and enforcement procedures, is essential. Moreover, by creating such an agreement the employer puts the employee on notice that he should not have any expectation of privacy in his computer use and that the employer may monitor its employees' electronic communication activities. By taking these significant steps, the employer will protect itself from liability while informing their employees of acceptable practices within the workplace, and this monitoring will quite likely allow the employees to increase their productivity while providing them with a framework for appropriate conduct in their electronic communications.

---

[107] *See id.* at 713.

[108] *See id.*

[109] *See id.*

[110] *See* Crowley & Aviza, *supra* note 12.

DISCLAIMER: This article has been strictly prepared and should be read for educational purposes only. The authors are not, under any circumstances, providing any type of professional advice but only raise issues in the workplace. If an individual or entity seeks assistance in this field they should consult with competent professionals or seek counsel specializing in this area of expertise. All situations require sound advice and should be addressed on a case by case basis and the individual state may play a pivotal role depending on the current state of the law at that juncture. The sample internet liability agreement cannot be utilized beyond the scope of this article and the authors make no representation as to its enforceability in any given state.