NOTE

Employer Liability for Employee Online Criminal Acts

Jeffrey S. Nowak*

* B.A., Indiana University—Bloomington, 1995; candidate for J.D., Indiana University School of Law—Bloomington, 1999. The author would like to thank Professor Fred Cate and Dana Connell for their valuable assistance with this Note. The author is particularly indebted to the Honorable Wayne R. Andersen, U.S. District Court Judge, whose constant concern for children and human relationships helped inspire this Note.

I. INTRODUCTION

Typing away at his computer while at work, Jacob Jacks forged a new and unhealthy relationship with an unassuming woman through an online "sex chat room." A computer technical advisor for Prodigy Services Company, Jacks repeatedly entered the chat room during work time for one reason: to befriend Barbara Haybeck and to persuade her to engage in sexual intercourse.[1] Jacks, a known sexual predator who had AIDS, used the Internet access provided by his employer to spend extensive time online with Haybeck.[2] Ultimately, Jacks succeeded in luring her into a sexual relationship. Before and during the relationship, Jacks denied having AIDS.[3] Haybeck contracted the deadly virus as a result of the sexual relationship and attempted to hold Prodigy liable for Jacks's Internet activity on the job.[4]

In workplaces driven by the latest and most advanced technology, this scenario does not seem too unrealistic. Misuse of the company computer and Internet services provide other reprehensible fact patterns as well. Jacks's activity might not have been limited to e-mailing a woman to engage in consensual sex acts. Employer liability could also become an issue, for example, if he were selling child pornography over the Internet at work, entering other chat rooms to lure underage girls into his sex web, or even harassing a third party by use of the company's online service. While the computer and the Internet as effective communication devices have changed the face of business, they present new and unanswered problems for employers.

What are the legal consequences for Prodigy and other employers when an employee uses a computer and his or her company's Internet service to engage in criminal activity or activity that furthers a criminal act?[5] Can the victim hold the employer liable under a respondeat superior or negligence doctrine? There is little question that these employees should be civilly, as well as criminally, liable for their abhorrent acts. However, the issue of employer liability becomes more recondite when these predators are not the

1. *See* Haybeck v. Prodigy Servs. Co., 944 F. Supp. 326 (S.D.N.Y. 1996).

2. *Id.* at 328.

3. *Id.*

4. For purposes of this Note, it is important to emphasize that Ms. Haybeck filed suit against Prodigy in its capacity as Jacob Jacks's employer rather than as a commercial online service provider. In *Haybeck*, Prodigy was treated similarly to any other employer that maintains and operates its own Internet system.

5. Use of the company Internet service for activity unrelated to the business may not, in itself, constitute a criminal act. Rather, a plaintiff will allege that the employer supplied the means (computer) to further the eventual criminal act. Therefore, according to the plaintiff, the employer should be held liable under respondeat superior or for its negligence in allowing the employee access to the Internet.

parties involved in a suit resulting from their illegal conduct. Because the emergence of the information superhighway offers employees a new outlet to conceal improper activity from their employers, employer liability is only further complicated.

Only twenty-five years ago, a mere 50,000 computers existed worldwide.[6] In 1997, that number was estimated at 140 million.[7] Today, 120 million people are linked via the Internet,[8] the vast majority of whom have gone online since 1990.[9] That number is three times as many as were online even two years ago.[10] Experts estimate that, in 1997 alone, these users sent nearly 2.7 trillion e-mail messages through their computers.[11] According to experts, "traffic on the Internet is doubling every 100 days."[12]

6. Larry Irving, *"Using Electronic Networks for Commerce: Charting a New Course for Business and Government," Remarks by Larry Irving, Assistant Secretary for Communications and Information National Telecommunications and Information Administration, U.S. Department of Commerce at E://Comm '97 - USA Washington, D.C., June 25, 1997* (visited Feb. 26, 1998) <http://www.ntia.doc.gov/ntiahome/speeches/E-COMM.htm> [hereinafter *E-Comm*].

7. *Id.*

8. Larry Irving, *"The E-Commerce Revolution: The Respective Roles for Industry and Government," 1998 Harbinger Users Conference, Chicago, IL, Remarks by Larry Irving, Assistant Secretary for Communications and Information National Telecommunications and Information Administration, U.S. Department of Commerce, Aug. 24, 1998* (visited Sept. 10, 1998) <http://www.ntia.doc.gov/ntiahome/speeches/harbin.htm> [hereinafter *E-Commerce Revolution*].

9. Frank C. Morris, Jr., *E-Mail Communications: The Next Employment Law Nightmare*, 20 ALI-ABA COURSE MATERIALS J. 49 (1995).

10. Irving, *E-Commerce Revolution*, *supra* note 8.

11. Larry Irving, *"Refocusing Our Youth: From High Tops to High-Tech," National Urban League and the National Leadership Council on Civil Rights Urban Technology Summit, Remarks by Larry Irving, Assistant Secretary for Communications and Information National Telecommunications and Information Administration, U.S. Department of Commerce, June 26, 1998* (visited Sept. 10, 1998) <http://www.ntia.doc.gov/ntiahome/speeches/urban62698.htm> [hereinafter *Refocusing Our Youth*]. The number of online users within schools and libraries has also increased exponentially. Seventy-two percent of public libraries offer Internet access. Almost 80% of schools are connected by the Internet, more than twice as many as in 1994. Currently, 27% of classrooms are connected, compared to only 3% in 1994. Larry Irving, *American Library Association National Telecommunications and Information Administration, Town Hall Meeting on Universal Service and the E-Rate, Welcoming Remarks by Larry Irving, Assistant Secretary for Communications and Information National Telecommunications and Information Administration, U.S. Department of Commerce, June 26, 1998* (visited Sept. 10, 1998) <http://www.ntia.doc.gov/ntiahome/speeches/ala62698.htm>.

12. Irving, *Refocusing Our Youth*, *supra* note 11; *see also* William M. Daley, *Remarks by U.S. Secretary of Commerce William M. Daley, Latin American Telecommunications Summit, San Carlos de Bariloche, Argentina, April 21, 1998* [As Prepared for Delivery] (visited Sept. 10, 1998) <http://www.ntia.doc.gov/ntiahome/speeches/042198_wmd_LATS. htm>.

For obvious reasons, this explosion of communication has greatly impacted the workplace. "Today, 90 percent of all companies with more than 1,000 employees use E-mail."[13] In 1996, a mere "34% of the Fortune 500 companies had World Wide Web sites"; in 1997, 80 percent of these companies had Web sites.[14] Meetings that formerly involved a pen, paper, and a handshake now involve a fax machine, a teleconference, or a simple e-mail message. The advantages of the computer workplace are obvious. Not only does technological advancement aid the average business, it also impacts the consumer who now receives services more efficiently and rapidly.

As new means of communication, however, the computer and Internet activity in the workplace yield disadvantages as well. Employees may spend a significant part of their workday surfing the Internet, which is merely a double-click away. But what awaits employees on the Internet are "hits"[15] unrelated to their employment roles and to the missions of their companies. Therefore, workplace Internet use creates a unique opportunity for employees to engage in activity contrary to the interests of the employer, including criminal activity or harassment. Wrongdoers like Jacob Jacks will continue to realize that the employer's Internet service can be used as a personal tool that can levy tremendous destruction upon the lives of private third parties. In response to perpetrators like Jacks, government and judicial systems have been slow to enact specific laws to confront this type of technological terror. Legislatures and courts now struggle to pass laws and resolve conflicts to keep up with this ever-changing technology.[16] In the meantime, employers must take precautions to protect themselves from unnecessary liability until legislatures can adequately address these questions of law.

This Note examines the application of the doctrines of respondeat superior and negligent retention as applied to the Internet in the workplace. It intends to aid employers that want to take proactive steps to minimize their liability for the actions of their employees on the Internet.[17] Part II analyzes

13. Morris, *supra* note 9, at 50.

14. Irving, *Refocusing Our Youth*, *supra* note 11.

15. "A 'hit' is a click of the mouse to request a file from a site." Sally Greenberg, *Threats, Harassment, and Hate On-Line: Recent Developments*, 6 B.U. PUB. INT. L.J. 673, 677 n.30 (1997).

16. Diana J.P. McKenzie, *Commerce on the Net: Surfing Through Cyberspace Without Getting Wet*, 14 J. MARSHALL J. COMPUTER & INFO. L. 247 (1996).

17. According to the court in *ACLU v. Reno*, 929 F. Supp. 824, 834 (E.D. Pa. 1996), the most common methods of communications on the Internet consist of:

(1) one-to-one messaging (such as "e-mail"),

(2) one-to-many messaging (such as "listserv"),

(3) distributed message databases (such as "USENET newsgroups"),

(4) real time communication (such as "Internet Relay Chat"),

(5) real time remote computer utilization (such as "telnet"), and

the doctrine of respondeat superior, which imputes liability to an employer for the actions of an employee that occur within the scope of employment. Part III focuses on negligent retention, the doctrine most likely to entrap employers as they continue to add more computers (and thus, more Internet users) to the workplace.[18] Part IV offers employers suggestions to limit their liability as a type of online provider and recommends an Internet policy to enforce proper employee use of the Internet while on the job.

II. THE DOCTRINE OF RESPONDEAT SUPERIOR

A. Traditional Definition of Respondeat Superior

The traditional basis for an employer's liability for its employees' acts is the doctrine of respondeat superior, under which the employer is liable for employee acts that are within the scope of employment or in furtherance of the employer's interest.[19] "Under respondeat superior, the employer 'stands in the shoes' of its employees,"[20] as long as the act in question is within the scope of employment. Courts determine whether an employee's tortious conduct falls within the scope of employment by considering such factors as the time and place of the act, the nature of the employee's duties, and the purpose for which the employee acted.[21] The Restatement (Second) of Agency, section 228, establishes the test adopted by most jurisdictions to determine what conduct falls within the scope of employment:

> (1) Conduct of a servant is within the scope of employment if, but only if:
>
> (a) it is of the kind he is employed to perform;
>
> (b) it occurs substantially within the authorized time and space limits;
>
> (c) it is actuated, at least in part, by a purpose to serve the master, and

(6) remote information retrieval (such as "ftp," "gopher," and the "World Wide Web").

Id. For purposes of this Note, these common uses of the Internet are the means most readily available to employees.

18. Also known as "negligent supervision." Diana Rousseau Belbruno, *Selected Negligence Problems in Employment Law*, *in* HANDLING CORPORATE EMPLOYMENT PROBLEMS 1991, at 341, 381-87 (Pract. L. Inst. 1991).

19. RESTATEMENT (SECOND) OF AGENCY §§ 228, 243 (1957) [hereinafter RESTATEMENT]; Wagstaff v. City of Maplewood, 615 S.W.2d 608 (Mo. Ct. App. 1981) (finding that the act of a policeman who fatally shot the plaintiff was outside the scope of his employment).

20. Rosanne Lienhard, *Negligent Retention of Employees: An Expanding Doctrine*, 63 DEF. COUNS. J. 389, 389 (1996).

21. *See* RESTATEMENT, *supra* note 19, §§ 219-237.

(d) if force is intentionally used by the servant against another, the use of force is not unexpectable by the master.

(2) Conduct of a servant is *not within the scope of employment* if it is different in kind from that authorized, far beyond the authorized time or space limits, or too little actuated by a purpose to serve the master.[22]

Courts have held that acts that are so personally driven or outrageous are clearly outside the scope of employment.[23] For example, in *Heindel v. Bowery Savings Bank*, Robert Turner, a security guard at a New York shopping mall, forced a fifteen-year-old girl to accompany him to the mall's security office where he assaulted, raped, and sodomized her.[24] The victim's father filed suit against Turner's employer, arguing that the security company was "vicariously liable" for his acts.[25] While the court acknowledged that an employer can be held liable for torts committed by the employee during the course of employment, the employer cannot be held liable when the personal motives of the employee are unrelated to the employer's business.[26] Finding that Turner's acts were committed for personal motives and were a complete departure from the normal duties of a security guard, the court held, as a matter of law, that his conduct did not further the employer's interest.[27] The court granted summary judgment for the employer. While not explicitly mentioning the Restatement, the *Heindel* court could have easily been guided by common sense exceptions to the scope of employment rule contained in the Restatement. For example, section 235 of the Restatement specifically protects employers when employees commit intentional torts for purely personal reasons unrelated to the business.[28]

22. RESTATEMENT, *supra* note 19, § 228 (emphasis added). *See also* WARREN A. SEAVEY, HANDBOOK OF THE LAW OF AGENCY § 87, at 148-52 (1964) (describing the "scope of employment").

23. *See, e.g.*, Rabon v. Guardsmark, Inc., 571 F.2d 1277, 1277 (4th Cir. 1978) (holding that security guard's sexual assault upon plaintiff "was neither in furtherance of agency's business nor within scope of employment"); Wellman v. Pacer Oil Co., 504 S.W.2d 55, 55 (Mo. 1974) (finding that gas station attendant's actions in fatally shooting a patron were "so outrageous and criminal and so excessively violent that, as a matter of law, they were not within the scope of employment"); *Wagstaff*, 615 S.W.2d at 608; Joshua S. v. Casey, 615 N.Y.S.2d 200 (N.Y. App. Div. 1994) (holding that a priest's sexual abuse of a child was, as a matter of law, not within the scope of employment); Forester v. State, 645 N.Y.S.2d 971, 974 (N.Y. Ct. Cl. 1996) (finding that acts were outside the scope of employment where an instructor assaulted a student, even when the "acts occurred on school property during school hours").

24. *Heindel*, 525 N.Y.S.2d 428 (N.Y. App. Div. 1988).

25. *Id.*

26. *Id.*

27. *Id.*

28. "An act of a servant is not within the scope of employment if it is done with no intention to perform it as a part of or incident to a service on account of which he is em-

In addition, if the employee's actions are outrageous, courts have traditionally held that the actions serve no rational business purpose and are therefore outside the scope of employment.[29] In *Bates v. United States*, the Eighth Circuit found that the government as "employer" could not be held liable for the actions of a military policeman when the policeman's conduct was "'outrageous and criminal.'"[30] In *Bates*, a military policeman stopped a car of four teenagers for an alleged robbery near a Missouri military base. The policeman handcuffed the passengers and fatally shot the two boys in the car.[31] Afterward, he assaulted and raped the two girls, ultimately shooting them as well.[32] The court found that an employee whose "actions . . . were so outrageous and criminal—so excessively violent as to be totally without reason or responsibility" could not be found to be acting within the scope of his employment.[33]

B. Employee Misconduct on the Internet

These exceptions, which negate the scope of employment when employee actions are so outrageous or personal in nature, should have specific application to Internet use in the workplace. The Restatement requires that the employee's acts "serve the master."[34] Therefore, to perform within the scope of employment, the employee must be motivated to serve the master, even in part, by his acts. Wrongful activity on the Internet in the workplace cannot fall within the scope of the employment relationship because sexual advances or other outrageous conduct over a company's online service could not reasonably further an employer's interest. Just as it is highly inconceivable that the sexual assault in *Heindel* or the sexual assaults and murders in *Bates* furthered the employers' interests, it is also unthinkable that luring a

ployed." RESTATEMENT, *supra* note 19, § 235.

29. "'The master can reasonably anticipate that servants may commit minor crimes in the prosecution of the business, but serious crimes are not only unexpectable but in general are in nature different from what servants in a lawful occupation are expected to do.'" Wellman v. Pacer Oil Co., 504 S.W.2d 55, 58 (Mo. 1974) (quoting RESTATEMENT, *supra* note 19, § 231 cmt. a). "If the employee's actions are 'outrageous,' the employer escapes liability without regard to whether the conduct should be considered to be within the scope of employment." Rochelle Rubin Weber, Note, *"Scope of Employment" Redefined: Holding Employers Vicariously Liable for Sexual Assaults Committed by Their Employees*, 76 MINN. L. REV. 1513, 1534 (1992) (arguing that sexual assault by an employee clearly cannot further any employer's interest). *See also* Haybeck v. Prodigy Servs. Co., 944 F. Supp. 326 (S.D.N.Y. 1996).

30. *Bates*, 701 F.2d 737, 741-42 (8th Cir. 1983).

31. *Id.* at 739-40.

32. *Id.* at 740.

33. *Id.* at 741.

34. RESTATEMENT, *supra* note 19, § 228(1)(c).

third party into a sexual relationship by way of the company computer furthers an employer's objective.[35]

In the *Haybeck* case, for example, Prodigy employee Jacob Jacks spent countless hours online with the plaintiff while he was at work at Prodigy.[36] Jacks offered Haybeck free time on Prodigy to induce her into a sexual relationship.[37] In dismissing the claim against the employer under the doctrine of respondeat superior, the court found that an employee's actions cannot fall within the scope of his employment when they are wholly personal in nature.[38] While the *Haybeck* court did not specifically declare Jacks's actions to be outrageous, one could conclude that the court found that his acts were so reprehensible that they could not have furthered his employer's interests.[39] Jacks's decision not to disclose a medical fact about himself could not have been said to further Prodigy's business. Rather, his decision to conceal his HIV status arose from a personal motivation too attenuated to "serve his master."[40] Likewise, using the Internet as a tool for Jacks's personal satisfaction did not serve the interests of Prodigy and, therefore, fell outside the scope of employment.

Extensive case law confirms that courts traditionally do not use respondeat superior as a basis for expanding an employer's liability when the employee commits wrongful acts so attenuated or outrageous that they fall outside the scope of employment.[41] Although an employee's improper use of the company Internet service falls outside the scope of his employment, employers are not immune from liability. Employers can still be held accountable under a basic negligence doctrine.

III. NEGLIGENT RETENTION AS A MEANS OF EMPLOYER LIABILITY

A. Negligent Retention as an Alternative to Respondeat Superior

In cases where an employee's tortious conduct cannot result in any violation under respondeat superior, courts recognize an alternative theory of employer liability—negligent retention or supervision—under which a plaintiff can bring an action against the employer. This theory holds employers liable under a completely different theory of negligence when the em-

35. *See* Weber, *supra* note 29, at 1523.
36. Haybeck v. Prodigy Servs. Co., 944 F. Supp. 326, 328 (S.D.N.Y. 1996).
37. *Id.*
38. *Id.* at 329. *See generally* Weber, *supra* note 29.
39. *Haybeck*, 944 F. Supp. at 331.
40. *See* RESTATEMENT, *supra* note 19, § 228.
41. *See supra* note 23.

ployer negligently retains or supervises the alleged employee tortfeasor. Rather than argue employer liability under respondeat superior, plaintiffs now assert claims under this new concept—negligent retention.[42] This negligence theory supplements the doctrine of respondeat superior because it offers plaintiffs a second bite at the employer liability apple.

The two claims differ in focus. "Under respondeat superior, an employer is vicariously liable for an employee's tortious acts committed within the scope of employment."[43] However, negligent retention holds an employer primarily liable if the employer negligently places "an unfit person in an employment situation involving an unreasonable risk of harm to others."[44] Negligent retention, therefore, allows "plaintiffs to recover in situations where respondeat superior's 'scope of employment' limitation [formerly] protected employers from liability."[45] Even if plaintiffs are unsuccessful in arguing that the tort was committed within the scope of employment, they may still plead alternatively that the employer allowed the tort to occur because the employer failed to take reasonable care in supervising or retaining the tortfeasor employee.[46]

Once an employee has been hired, the employer has a legal duty to supervise the employee and his conduct while at work.[47] This supervision is necessary not only to protect other employees but also to shelter third parties from the wrongful acts of employees.[48] The Restatement admonishes an employer to properly oversee its employees. Section 213 of the Restatement declares that an employer "is negligent if he fails to use care to provide such regulations as are reasonably necessary to prevent undue risk of harm to third persons or to other servants from the conduct of those working under him."[49]

Under a theory of negligent retention, an employer is held liable for retaining an employee whom it knows or should have known is not fit for the employment position.[50] Simply put, the doctrine holds an employer account-

42. *See* Lienhard, *supra* note 20.

43. *See* Cindy M. Haerle, *Employer Liability for the Criminal Acts of Employees Under Negligent Hiring Theory:* Ponticas v. K.M.S. Investments, 68 MINN. L. REV. 1303, 1306 (1984).

44. *Id.*

45. *Id.* at 1306-07.

46. *See, e.g.*, Bryant v. Livigni, 619 N.E.2d 550, 558-59 (Ill. App. Ct. 1993) (finding that employer had notice of supervisor's propensity toward violence where the supervisor had thrown a milk crate at a co-worker and had assaulted the co-worker's son).

47. *See* RESTATEMENT, *supra* note 19, § 213; Belbruno, *supra* note 18, at 348.

48. Belbruno, *supra* note 18, at 381.

49. RESTATEMENT, *supra* note 19, § 213 cmt. g.

50. *Negligent Hiring and Retention of an Employee*, 29 AM. JUR. TRIALS 272-77 (1982).

able when it "fails to properly direct or oversee the conduct of an employee subject to its control."[51] In cases regarding employee conduct, third-party plaintiffs often attempt to show that the employer failed to react to actual or constructive notice of facts, which should have suggested that the employee posed a "special" threat.[52] Actual notice is "such notice as is positively proved to have been given to a party directly and personally, or such as he is presumed to have received personally . . . ."[53] Constructive notice is "information or knowledge of a fact imputed by law to a person (although he may not actually have it), because he could have discovered the fact by proper diligence, and his situation was such as to cast upon him the duty of inquiring into it."[54] This theory requires the employer to proactively investigate issues that arise in the workplace.

Most negligent retention cases involve sexual harassment claims in the workplace. The typical claim is one in which an employee brings a Title VII action against the employer for the misconduct of a co-worker. In this scenario, the employer is not liable under state sexual harassment law or under federal law through Title VII if the employer had no notice of the co-worker's actions. But if the employer was placed on notice of the co-worker's alleged harassment, the employer could be liable under both Title VII and a theory of negligently retaining the co-worker.

A non-employee who is a victim of employee misconduct can state a similar claim under the theory of negligent retention. If an employer knows or should have known about allegations of improper conduct of an employee, then the employer has a duty to investigate the allegations and rem-

> The principal may be negligent because he has reason to know that the servant or other agent, because of his qualities, is likely to harm others in view of the work or instrumentalities entrusted to him. If the dangerous quality of the agent causes harm, the principal may be liable under the rule that one initiating conduct having an undue tendency to cause harm is liable therefor.

Destefano v. Grabrian, 763 P.2d 275, 287 (Colo. 1988) (quoting RESTATEMENT, *supra* note 19, § 317 cmt. d).

51. Janet K. Colaneri & Bobbi Reilly, *Non-Actor Liability for Sexual Assaults in Texas and the Effect of Insurance on Recovery*, 2 TEX. WESLEYAN L. REV. 279, 291 (1995) (attempting to strike a balance between perpetrators and property or business owners when sexual assault victims seek to hold the third party liable for the acts of the "agent").

52. J. Hoult Verkerke, *Notice Liability in Employment Discrimination Law*, 81 VA. L. REV. 273, 306 (1995).

53. BLACK'S LAW DICTIONARY 1061-62 (6th ed. 1990). *See generally* Meritor Sav. Bank v. Vinson, 477 U.S. 57 (1986) (holding that an employer need not have actual notice of ongoing improper conduct to be held liable).

54. BLACK'S LAW DICTIONARY, *supra* note 53, at 1062.

edy the situation according to its findings.[55] When a plaintiff offers evidence that the employer had notice of the employee's conduct but failed to take any remedial action, the plaintiff gains a strategic advantage in the litigation.[56] Therefore, courts specifically focus on whether the employer had notice concerning the employee's improper actions and whether the employer took appropriate measures to reprimand or dismiss the insubordinate employee.[57]

A Colorado court has suggested that a plaintiff can succeed under a claim of negligent retention only if the plaintiff shows prior knowledge or notice on the part of the employer as to the employee's alleged tortious conduct or propensity toward engaging in that conduct. In *Moses v. Diocese of Colorado*, a church parishioner brought a civil action against the Episcopal diocese and bishop for her injuries sustained through sexual relations with a priest from whom she sought counseling.[58] The plaintiff argued that because the diocese had notice of several other sexual relationships between priests and parishioners, the diocese as "employer" was negligent in retaining the priest in her case.[59] The court found that the diocese and bishop had been notified of ongoing problems within their church because sexual relationships between priests and parishioners had arisen seven times before.[60] The court noted that even the psychological reports notified the diocese that further supervision of their priests may be necessary.[61] While the court found that the priest's acts were clearly outside the scope of employment, the court held the diocese liable for negligent retention because the diocese "should have been alert to the possibility of problems with Father Robinson and taken adequate steps to insure [that he] was not in a position where he could abuse [his position] . . . ."[62]

---

55. *See* Jill Fedje, *Liability for Sexual Abuse: The Anomalous Immunity of Churches*, 9 LAW & INEQ. J. 133, 156 (1990) (Although this article deals with the liability of churches as "employers" for the sexual misconduct of the clergy, it has specific application to negligent retention principles here. 55.Larry Irving, *"Using Electronic Networks for Commerce: Charting a New Course for Business and Government," Remarks by Larry Irving, Assistant Secretary for Communications and Information National Telecommunications and Information Administration, U.S. Department of Commerce at E://Comm '97 - USA Washington, D.C., June 25, 1997* (visited Feb. 26, 1998) <http://www.ntia.doc.gov/ntiahome/speeches/E-COMM.htm> [hereinafter *E-Comm*].
).

56. *Id.*

57. *Id.*

58. *Moses*, 863 P.2d 310 (Colo. 1993).

59. *Id.* at 329.

60. *Id.*

61. *Id.*

62. *Id.*

Foreseeability is a key issue in deciding whether an employer is liable under the theory of negligent retention. The employer's liability will depend upon the scope of the original foreseeable risk that the employee created through his acts. According to basic tort analysis, "[i]f the intervening cause is one which in ordinary human experience is reasonably to be anticipated, or one which the defendant has reason to anticipate under the particular circumstances, the defendant may be negligent, among other reasons, because of failing to guard against it . . . ."[63] If an employer simply could not have foreseen the actions of its employee, it is more likely that a court would not hold the employer liable.[64] However, if it can be found that an employer had a duty to anticipate the intervening employee conduct and guard against it, a court is more likely to find the employer liable.[65]

A Connecticut court considered the issue of employer liability when the employer may not have foreseen the consequences of its employee's actions. In *Gutierrez v. Thorne*, a man was hired as a mental retardation aide by the state's mental retardation services agency.[66] As part of his duties, he visited with and assisted high-functioning retarded clients with budgeting and banking problems, shopping, and household needs.[67] He was given keys to the apartments so that he could gain access in the event of an emergency.[68] He later used the keys to enter an apartment and sexually assault a young female client.[69] The court was forced to decide whether a reasonably prudent employer would have more closely supervised an employee who had keys to enter the apartments.[70] If a reasonable employer would have seen the possibility of the general nature of the injury and would have taken extra precautions to supervise its employee in this situation, the employer here should also have foreseen the problems inflicted on the victim. The *Gutierrez* court held that the foreseeability of whether the defendant's conduct in permitting

63. W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 44, at 303 (5th ed. 1984) (citation omitted).

64. *See* Beshears v. Unified Sch. Dist., 930 P.2d 1376, 1384 (Kan. 1997) (finding that the school district could not have foreseen an "arranged" fight between two students after school hours); Bruchas v. Preventive Care, Inc., 553 N.W.2d 440 (Minn. 1996) (dismissing a negligent retention claim because the plaintiff failed to present any evidence that the employee had dangerous tendencies that were known, or should have been known, to the employer, such that it should have been foreseeable that the employee was unfit for his position and posed a threat to others); Belbruno, *supra* note 18.

65. *See* Cheryl S. Massingale & A. Faye Borthick, *Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services*, 12 W. NEW ENG. L. REV. 167, 180 (1990).

66. *Gutierrez*, 537 A.2d 527 (Conn. App. Ct. 1988).

67. *Id.* at 529.

68. *Id.*

69. *Id.*

70. *Id.* at 531-32.

the employee to have a key to the plaintiff's apartment would result in a sexual assault upon the plaintiff was a question for the fact finder.

The *Haybeck* court also addressed the issue of negligent retention as applied to the employer Prodigy.[71] Applying the traditional approach to the theory of negligent retention, the court demanded that the plaintiff show how Prodigy was put on notice of its employee's wrongful activity:

> Clearly Jacks' act, whether it was his sexual conduct or his failure to reveal his medical condition, cannot be considered "one commonly done by such an employee"—there is no allegation that technical advisors in positions such as Jacks' commonly have sex with customers or failed to reveal the fact that they carried communicable diseases.[72]

Because Ms. Haybeck could not show that Prodigy knew that Jacks was concealing his HIV status from his sex partners or was having unprotected sex with them—anything that would alert Prodigy to wrongful activity—she could not argue that Prodigy's retention of its employee was negligent.[73]

As the courts in *Moses*, *Gutierrez*, and *Bates* held, recent jurisprudence clearly establishes that liability will not be imputed to the employer under a negligent retention claim unless the employer knew or should have known of the employee's improper conduct, which made him "unfit" for the position.[74] Where the Internet is involved, an employer can fall into and out of liability based upon the e-mail and Internet system the company uses. For example, if a small business uses a commercial service such as America Online[75] to conduct Internet activity, an employer will have little opportunity to screen or become aware of any improper online conduct. However, if a larger business decides to establish a private network with its own server,[76]

71. Haybeck v. Prodigy Servs. Co., 944 F. Supp. 326, 332 (S.D.N.Y. 1996).

72. *Id.* at 331.

73. *Id.* at 332. *See also* Kirkman v. Astoria Gen. Hosp., 611 N.Y.S.2d 615, 616 (N.Y. App. Div. 1994) (holding employer not liable for negligent retention of mall security guard who raped a customer where there was no showing that the employer had any knowledge of employee's propensity or history of such misconduct).

74. *See* Bryant v. Better Bus. Bureau of Greater Maryland, Inc., 923 F. Supp. 720, 750 (D. Md. 1996) (finding that the employer had no reason to know of the employee's violent tendencies until the plaintiff filed an administrative action); Evans v. Morsell, 395 A.2d 480 (Md. 1978) (finding no evidence that the owner of a tavern knew or should have known that a bartender who shot a patron was potentially dangerous); J. v. Victory Tabernacle Baptist Church, 372 S.E.2d 391 (Va. 1988) (rejecting plaintiff's claims that the defendant employer knew or should have known that its pastor had recently been convicted of aggravated sexual assault before he allegedly raped and sexually assaulted a ten-year-old girl).

75. Employers are not limited to commercial services to provide e-mail in their workplaces. For purposes of this Note, these systems will be referred to as "non-network" systems.

76. "A server is a computer that provides shared resources to network users. A server typically has greater CPU power, number of CPUs, memory, cache, disk storage, and

the employer's potential notice of improper conduct becomes greater because it exercises more control over the exchange of information. Employer liability should turn on this very point. How businesses store their Internet activity and how often they check this activity must affect their susceptibility to third-party lawsuits. The business that controls its own Internet system has the ability to store e-mail communication, to effectively monitor the Internet activity of its employees, and should not be allowed to assert that it has no knowledge of information it physically possesses.

B. Typical Company E-Mail Systems

Before assessing the potential liability of an employer that uses a non-network service versus an employer that operates an Internet system at its workplace, it is important to note the differences between the two possible e-mail systems. The first category, and probably the more prevalent, is an e-mail system where the employee uses e-mail through a commercial service, such as America Online, Prodigy, or CompuServe.[77] Through this system, users transmit messages to each other through terminal lines and routing mechanisms housed in a computer.[78] The only equipment necessary to transmit the e-mail message is a modem, computer, and appropriate software.[79] The employee sends the e-mail messages to a recipient via telephone lines usually owned and operated by a third-party server.[80] The employer merely acts as a liaison between the employee and the commercial entity by paying for the online service.[81] E-mail messages on this system usually remain confidential vis-à-vis the employer.[82] To gain access to any files on this basic e-mail system, the employer will literally have to search the individual computer for the files because the only information trail that exists is between the non-network service and the computer sitting on the employee's desk.

The second situation is an e-mail system owned and maintained by the employer. Here, the employer will most likely operate a server where e-mail

power supplies than a computer used as a single-user workstation." DONALD E. LIVELY ET AL., COMMUNICATIONS LAW: MEDIA, ENTERTAINMENT, AND REGULATION 820 (1997).

77. John Araneo, Note, *Pandora's (E-Mail) Box: E-Mail Monitoring in the Workplace*, 14 HOFSTRA LAB. L.J. 339, 341 (1996).

78. Lois R. Witt, Comment, *Terminally Nosy: Are Employers Free to Access Our Electronic Mail?*, 96 DICK. L. REV. 545, 546 (1992).

79. *Id.*

80. *Id.* at 547.

81. Araneo, *supra* note 77, at 342.

82. Michael W. Droke, Comment, *Private, Legislative and Judicial Options for Clarification of Employee Rights to the Contents of Their Electronic Mail Systems*, 32 SANTA CLARA L. REV. 167, 169 (1992).

and other Internet activity are often stored after this information is retrieved by employees.[83] Even when an employee deletes a message from his or her own computer, there will almost always be a record of e-mail messages and Internet hits stored on a system maintained by the employer.[84] These communications are also routinely stored through a backup system, leaving a trail of evidence, which can confirm the existence of improper conduct by the employee.[85] Employees and employers alike may believe that once an e-mail message is sent or deleted it will be removed permanently from the system.[86] While a paper file can often be discarded when it is no longer needed, electronic data that is deleted or overwritten can easily be retrieved. Most electronic information is stored on backup tapes for six months to a year.[87] The misconception that electronic messages are forever deleted can only further entice employees to recklessly send e-mail messages that could levy harsh legal consequences on their employers.

Additionally, this second system is usually overseen by a system administrator or computer technician who ensures the security and overall maintenance of the system. The system administrator usually controls the flow of stored information and is most capable of monitoring the Internet activity of employees. Unlike the employer that uses a commercial e-mail system, an employer that hires a system administrator to monitor its Internet system provides a less confidential communication environment for its employees.

C. Potential Liability for an Employer that Uses a Non-Network E-Mail Service

An employer that supplies its employees with a basic, non-network e-mail service to communicate at the workplace may have little opportunity to discover whether improper activity may be occurring between an employee and a third party via e-mail. When e-mail communication does not exist at the workplace, a supervisor may at least pick up on conversations or other outward displays of conduct between an employee and another party that may give rise to a suspicion of improper activity. However, with unlimited access to the Internet, employees may send improper e-mail messages without their employer's knowledge and innocently continue their workdays.

83. *See* Tim Cahoon, *Playing Peek-a-Boo with E-Mail*, HP PROF., Mar. 1, 1994, at 56.

84. Araneo, *supra* note 77, at 342.

85. Donald H. Seifman & Craig W. Trepanier, *Evolution of the Paperless Office: Legal Issues Arising Out of Technology in the Workplace*, 21 EMPLOYEE RELATIONS L.J. 5, 20 (1996).

86. *Id.* at 26.

87. Vera Titunik, *Collecting Evidence in the Age of E-Mail*, AM. LAW., July-Aug. 1994, at 119.

Because the opportunity to efficiently supervise employees in this environment is unrealistic, employers that maintain a non-network e-mail service should be most protected under the doctrine of negligent retention when the doctrine is applied to the Internet. Not only are these employers cut out of the communication loop (remnants of the e-mail communication only remain between the individual employee and the commercial service), they are forced to inspect each computer's hard drive or memory if they wish to explore their employee's activity on his computer. Even if backup files are created at some location within the company's limited computer system, it is still unlikely that the employer will have reasonably easy access to the activity.[88]

At these types of businesses, improper Internet activity and its liability is even more difficult to impute to the employer than with other types of communication within the workplace, such as a conversation between an employee and a third party over the company telephone. As long as the employer acts consistently with state and federal wiretapping statutes,[89] it can screen the phone call not only to determine whether the conversation falls within the scope of employment, but also to determine whether it is activity that the employer must prevent and remedy to avoid liability. Therefore, a simple telephone call may place the employer on notice of employee misconduct. An employer also receives notice through company voice mail or even a fax machine. These technological advancements give the employer voice or digital feedback concerning the actions of its employees. The same cannot be said, however, for an Internet system completely outside the control of the employer. When the employer relies on a third party to provide the Internet service, the employer can no longer "wiretap" the e-mail transmission. The employer is left to rely on a co-worker of the employee or constructive notice, which alerts a supervisor to the misconduct.

Yet the most outrageous acts may still be foreseeable and entrap even the smallest businesses. *Moses v. Diocese of Colorado* suggests that any information that notifies an employer of potential misconduct can implicate the employer in a negligent retention claim.[90] In *Moses*, the court reasoned that the employer should have further supervised its priests when reports indicated that relationships between priests and parishioners were becoming more common.[91] Similar "reports" can alert an employer to improper Internet activity. For example, if an employer knows that its employees frequent

88. *See* Araneo, *supra* note 77, at 342; Seifman & Trepanier, *supra* note 85, at 20.

89. State and federal wiretapping statutes fall outside the scope of this Note. This analysis assumes that the employer has met all the legal requirements under such Acts.

90. *Moses*, 863 P.2d 310 (Colo. 1993).

91. *Id.* at 329.

sexually explicit Internet sites or use their e-mail for non-business purposes, it becomes more foreseeable—regardless of the employer's Internet screening capabilities—that an employee will engage in conduct that harms a third party. While an employer can receive notice through other channels, these few tangible examples provide a clear warning that an employer must develop heightened supervision when the Internet is involved.

Although *Moses* involved the Diocese of Colorado, a large employer whose capabilities to monitor priests' activities were enhanced by its tremendous resources and manpower, its message to small businesses with a basic Internet setup is clear: Improper employee actions that are both foreseeable and that actually or constructively place the employer on notice will subject the employer to liability under state negligent supervision laws. Thus, employers with limited Internet supervision capabilities still must heed the basic duty echoed in the Restatement, which implores an employer to "provide such regulations as are reasonably necessary to prevent undue risk of harm to third persons . . . from the conduct of those working under him."[92]

D. Potential Liability for Employers that Maintain Their Own Internet Systems

Employer liability for the online criminal acts of its employees may cut a different way for employers that maintain and control their own servers through which e-mail is transmitted and on which it is stored. Because these employers control their own systems, electronic information is stored and saved for any supervisor to uncover.[93] It is difficult for these employers to argue that they do not fully know what activity their employees are engaging in since the evidence is available on their networks. On the contrary, since the employer is equipped with the ability to create backup files on the network, it has an increased opportunity to find the files.[94] The employer can view files on the hard drive and every e-mail message passing through its system that is placed in storage. Whereas a smaller business lacks the opportunity to check electronic information because it lacks its own computer network, employers possessing network capabilities cannot avoid the potentially scandalous activity of its employees. Thus, these employers find themselves in the same category as an employer that monitors its own telephone lines. Comments formerly made within the company halls, bathrooms, or even in private meetings may now be sent through the network system by an

92. RESTATEMENT, *supra* note 19, § 213 cmt. g.
93. *See* Seifman & Trepanier, *supra* note 85, at 20, 26.
94. *See id.* at 20.

employee.[95] Since these electronic messages can be stored on hard copy or on disks, the employer receives similar notice as it does with a telephone conversation, voice mail, or fax. The message makes its "noticeable" mark, albeit stealthily, on the employer.

In addition to maintaining their own networks, these employers traditionally retain a system administrator whose duties often include monitoring employee Internet activity on the system. While this administrator is invaluable to the novice computer user who is struggling to master Windows 95, his position in the company exponentially increases the employer's awareness of network and thus, Internet, activity. It is virtually impossible for a system administrator to contend that he is unaware of employee Internet activity when e-mail messages are stored on the very system he monitors.

Applying traditional negligence law to this situation, a plaintiff can effectively argue that an employer's Internet system and its system administrator places the employer on notice that its employees conducted improper activity on the company's Internet system while at work. *Haybeck v. Prodigy Services Co.* exemplifies the situation these employers face.[96] In *Haybeck*, the plaintiff filed suit against Prodigy for its "negligence, carelessness, [and] recklessness . . . in [Prodigy's] ownership, operation, management, repair and control of . . . [its] on-line network."[97] While the court found Jacob Jacks's actions to be outside the scope of his employment, it did not adequately address Prodigy's liability as an employer that arguably was placed on notice of Jacks's activity on its elaborate Internet system. *Haybeck*'s conclusion forces large, intricate businesses to guess at the standards courts will apply to determine liability for their Internet systems. According to the court, the only wrong that occurred was Jacks's alleged unprotected sex with Haybeck while he was infected with AIDS—an act that took place off the employer's "premises"[98] and without the aid of Prodigy's "chattels."[99]

Yet, the question arises whether Jacks furthered his wrongful act, as any employee could, with Prodigy's chattels. Contrary to the court's finding, Jacks used his employer's chattel to further his criminal activity. But for the company computer, Jacks probably would not have met Haybeck in the chat room and therefore, would not have encouraged their relationship. The *Haybeck* court quickly glossed over this point, thereby sending the wrong impression to employers like Prodigy. Haybeck should have argued that Prodigy was aware of Jacks's questionable activity because Prodigy's electronic

95. *See* Araneo, *supra* note 77, at 355.
96. *Haybeck*, 944 F. Supp. 326 (S.D.N.Y. 1996).
97. *Id.* at 328.
98. *Id.* at 332.
99. *Id.*

files indicated that Jacks entered sex chat rooms and spent hours there[100] rather than engaging in work that "served"[101] the interest of his employer. Prodigy's suspicion should have heightened when its stored electronic files indicated that an employee entered a sex chat room for excessive periods of time.[102] While Prodigy might not have been privy to Jacks's particular motives in luring Haybeck into a sexual relationship, his actions were foreseeable because of the electronic trail Jacks left behind.

While employer liability seems to be elevated for employers that maintain their own servers, these employers have one strong defense—because their Internet systems are deluged with an infinite amount of electronic information, employers cannot adequately search for employee misconduct. Although a search for improper activity may be feasible for a company with 100 employees, it may be a much different task for a company with 5,000 employees. Such an argument, however, seems unlikely to rebut a plaintiff's claim. It implies that the larger employer is not taking the basic means to supervise its employees and is tacitly allowing employee misconduct to invade the workplace.

To make this defense succeed, employers must adopt methods that minimally assist the employer in weeding out employee misconduct on the Internet. Using software that blocks sexually explicit sites and that helps screen for certain words that appear in employee e-mail, employers utilize preventative devices that courts may favorably acknowledge in employer liability claims.[103] Although the employer should adhere to state and federal privacy laws in implementing these methods, they will prove effective in sheltering it from liability.

IV. SUGGESTIONS TO EMPLOYERS TO REDUCE THEIR LIABILITY FOR EMPLOYEES' WRONGFUL ACTS

A. Create a Company E-Mail Policy

For employers that carry either type of Internet system, company policies will significantly limit the risks associated with electronic communications in the workplace and reduce the employer's liability under negligent retention law.[104] Not only does a well-drafted Internet policy limit or eliminate potential liability for these lawsuits, it also proactively decreases e-mail

100. *See id.*

101. *See* RESTATEMENT, *supra* note 19, § 218(1)(c).

102. *Haybeck*, 944 F. Supp. at 327-28.

103. *See* Heather L. Gatley, *E-Mail, Cyberporn, and Employer Liability* (on file with the *Federal Communications Law Journal*).

104. Seifman & Trepanier, *supra* note 85, at 28.

abuse by informing employees that the employer is monitoring their e-mail activities. Such a policy also resolves any ambiguity under federal law about the employer's right to review employee e-mail.[105] Therefore, the employer's reason behind these office policies should be two-fold: (1) to make employees aware of proper Internet use at work, and (2) to adequately protect the employer from a negligence action.

An Internet policy should be implemented to put employees on notice that Internet use exists for work-related purposes only. Specifically, an effective policy on Internet use should:

(1) caution employees that the Internet is not a secure environment and may be accessed by others.[106] Further, the policy should inform the employees that backup files continually exist within the company's system and can be easily retrieved by a plaintiff who wishes to file suit against the employee or the company. The policy should warn employees that the employer has access to and may override individual passwords to maintain its business interests.[107] The policy should also "require employees to disclose all passwords . . . to the employer to facilitate such access."[108]

(2) explain the employer's monitoring procedures and how they may be lawfully used by management under state and federal privacy and wiretap laws.[109] The policy should provide that by using the company computer, the employee consents to monitoring (to achieve employer interests).[110] The employer should obtain a signed acknowledgment form from the employee consenting to such monitoring.[111]

(3) limit employee access to the Internet and establish authorization procedures for access.[112] For employers that use the Internet on a limited basis through a commercial service, it may be appropriate to set aside only

105. Araneo, *supra* note 77, at 358. *See also* Robert M. Barker et al., *E-Mail Issues*, INTERNAL AUDITOR, Aug. 1995, at 60 (arguing that simplistic e-mail regulations and policies will help limit potential for legal issues to arise); *see, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (finding that employee had no privacy rights in his e-mail communications under his employer's e-mail system).

106. *See* Seifman & Trepanier, *supra* note 85, at 28.

107. *Id.*

108. *Id.*

109. *See supra* note 105. Paul E. Hash & Christina M. Ibrahim, *E-Mail, Electronic Monitoring, and Employee Privacy*, 37 S. TEX. L. REV. 893, 910 (1996); *see also* Seifman & Trepanier, *supra* note 85, at 28.

110. *See* Seifman & Trepanier, *supra* note 85, at 28. "[T]he Justice Department recommends that system administrators add to every user's log-in a banner that gives 'clear and unequivocal notice that by signing on and using the system, they are expressly consenting to have their keystrokes monitored or recorded.'" Laura B. Smith, *Electronic Monitoring Raises Legal and Societal Questions*, PC WEEK, June 28, 1993, at 204.

111. *See* Seifman & Trepanier, *supra* note 85, at 28.

112. *Id.*

one computer with software and modem capability to access the Internet. Therefore, the employer can successfully monitor one computer used by employees on a revolving basis when business needs arise.

(4) clearly establish that the computer and other electronic communication devices are the exclusive property of the employer and should be used only to serve the interests of the employer.[113]

(5) proscribe the use of the employer's Internet service for personal messages, contacting third parties, or distribution that does not fall within the scope of employment.[114] The policy should particularly restrict simple "chain" e-mails and other messages that may appear innocuous.

(6) define and prohibit communications that may be considered harassment of fellow employees and third parties.[115]

(7) "[p]rohibit offensive, harassing, vulgar, obscene, or threatening communications, including disparagement of others based on race, national origin, marital status, sex, sexual orientation, age, disability, pregnancy, religious or political beliefs, or any other characteristic protected under federal, state, or local law."[116]

(8) proscribe the creation and dissemination of sexually oriented messages or sexually graphic images through the Internet, and prohibit unwelcome behavior, such as sexual advances and requests for sexual favors.[117]

(9) forbid employees from using the Internet system of another employee or transmitting e-mail messages from a co-worker's Internet hookup.[118]

(10) implement a document retention policy.[119] This system keeps the employee aware that backup is kept for only a limited amount of time. In Part III.C *supra*, this Note highlighted the common misconception that many employees believe that deleting an electronic message automatically removes it from the system.[120] While the backup is secure on an employer's server and network, it does not remain for an indefinite period of time.[121] This will benefit the employer because there will be less risk of liability with less backup available.[122] The limited period of backup storage also encourages employees to be more efficient in the sense that they need to be aware of

113. *Id.*
114. *Id.* at 29.
115. *Id.*
116. *Id.*
117. *Id.*
118. *Id.*
119. *See* Smith, *supra* note 110, at 204.
120. Seifman & Trepanier, *supra* note 85, at 20.
121. Araneo, *supra* note 77, at 363.
122. *Id.*

what files they actually have, instead of falling into the habit of relying on backup.[123] Once employers educate their employees on stored documents, they should also emphasize that the employees must not rely on this backup because the information is not permanently available.

(11) be submitted to all employees, particularly new hires. This policy, which should be signed by new hires, should also include a provision that the employee has read, understood, and will follow the instructions of the employer.[124] This may further limit employer liability given recent Supreme Court decisions that require employers to make their discrimination policies readily available to their employees. The policy should be periodically redistributed. Access to the system should be frozen until the form has been returned.[125] Providing each employee a copy of the policy on a single occasion may not be enough. Employers should install a pre-log-on screen into the system notifying employees that use of the Internet is governed by office policy.[126]

Although some of these policy elements may seem obvious to employers and employees alike, many employers are not implementing these preventive plans.[127] If these behaviors and activities are checked by Internet policies, employers can limit their exposure to liability claims. This policy assists all employers that are online. However, these steps particularly aid the employer that uses a commercial online (non-network) service. Because this employer cannot electronically monitor the computer, these guidelines represent proactive steps by this employer to weed out improper Internet activity in its workplace. While courts will continue to demand that this employer carefully supervise its employees, particularly when misconduct is reported, an Internet policy often serves as a solid defense to employer liability claims. In addition to an Internet policy, employers in this kind of Internet environment should also encourage employees to report improper activity to a supervisor or the employer's human resources department.

B. The Employer that Operates Its Own Internet System Should Take Additional Precautions

An Internet policy alone, however, does not limit the potential liability of the employer that operates its own Internet system because this employer is more readily put on notice of its employees' actions. What may go unnoticed in one workplace may be etched in a server's backup storage in another

123. *Id*.
124. *Id.*
125. *Id.*
126. *Id.* at 363-64. *See also* Smith, *supra* note 110, at 204.
127. Hash & Ibrahim, *supra* note 109, at 910.

workplace. Therefore, the employer that maintains its own server must take extra precautions to prevent liability under the doctrine of negligent retention.

This employer must first require its system administrator to monitor e-mail communications, consistent with state and federal wiretap laws, for improper employee conduct. Such a job requirement is not difficult to add to the list of the administrator's responsibilities. When the employer does not require this supervisor, as part of his duties, to monitor the system, the employer may have to explain to a court why it did not take the initiative to implement this relatively easy precaution. If an employer is willing to hire such an administrator, it is more likely that this person will be put on notice of inappropriate behavior or communication through the company computer. Plaintiffs injured by the acts of an employee may find it easier to impute notice to an employer when the employer hires and retains an employee whose sole job is to monitor the computer workplace and to assist co-workers to properly manage the latest technology. However, common sense must prevail. A court will unlikely hold an employer liable when it continues to take reasonable steps to protect its network from inappropriate employee activity. While these administrators must respect the privacy of the employee, they should work within the Internet policy created by the employer to protect the business from potential liability.

Additionally, the employer can use devices, such as firewalls, which block traffic that may be sexual in nature or improper in the workplace.[128] The firewall can be considered as a pair of mechanisms: one that blocks traffic, and the other that checks all incoming traffic.[129] In essence, the firewall can be formulated to block particular Internet sites or chat lines that an employer finds to be improper or outside the scope of employment. While this device curbs such improper access, it also serves as a potential defense to third-party claims. Because the employer secures this extra precaution within its Internet system, it can argue that it is reasonably taking proactive steps to properly supervise employees and "to prevent undue risk of harm to

128. A firewall is commonly used to block sex-related Internet sites.

> "A 'firewall' is a program or set of programs that enables a company to track, restrict or altogether block Internet access. Firewalls range from simple programs available at local computer stores for under $50 to complex matrices of programs designed to fit a network's specifications. . . . More complex programs can serve as the computer system's gatekeeper, monitoring what is brought into the computer environment as well as guarding against inappropriate transmissions."

Gatley, *supra* note 103.

129. Katherine Hutchison, *Firewall Technology Update: A Trusted Network Security Solution for Distributed Computing and Communications Environments* (visited Oct. 3, 1998) <http://www.cyberguardcorp.com/library/frames/industry_info/firewall_tech.html>.

third persons . . . from the conduct of those working under him."[130] The addition of the firewall not only ensures a safer workplace, it dissuades employees from engaging in Internet activity that may have a detrimental effect on third-party victims.

While the supervision of a system administrator and the addition of a firewall can aid the employer in limiting the number of negligent retention lawsuits, the employer that operates its own Internet system should also encourage employees to inform the company of any improper activity that might be present without the employer's knowledge. Although this employer has a heightened legal duty to supervise its employees, it should never underestimate the dedication of a majority of employees who wish to make their workplace safe for co-workers and consumers alike.

V. CONCLUSION

The widespread use of the Internet in the workplace raises a number of complicated and unanticipated legal issues for employers. Unfortunately, many of the existing statutory, regulatory, and common law rules and principles have not kept pace with advancements in electronic communications technology. The doctrine of respondeat superior cannot address these legal issues because much of the employees' improper Internet activity occurs outside the scope of the employment relationship. Currently, the doctrine of negligent retention forces employers to analyze their potential liability when they allow the Internet into their businesses. This doctrine requires employers to remedy improper activity when they know or should know of its existence within the workplace. This does not, however, foreclose all legal remedies for alleged victims in the future. Although remedial state and federal legislation, such as the Communications Decency Act, will surface, further regulation will undoubtedly raise even more legal issues for the employer. Given this state of uncertainty, adopting defensive policies and procedures and monitoring existing resources is the most effective way to reduce an employer's liability while taking advantage of today's technology.

130. RESTATEMENT, *supra* note 19, § 213 cmt. g.