Washington Journal of Law, Technology & Arts

Volume 4 | Issue 1 Article 5

6-6-2007

Employee Internet Misuse: How Failing to Investigate Pornography May Lead to Tort Liability

Jamila Johnson

Corporate & Commercial
Cite as: Jamila Johnson, *Employee Internet Misuse: How Failing to Investigate Pornography May Lead To Tort Liability*, 4 Shidler J. L. Com. & Tech. 1 (Jun. 6, 2007), *at* <http://www.lctjournal.washington.edu/Vol4/A01Johnson.html>

EMPLOYEE INTERNET MISUSE: HOW FAILING TO INVESTIGATE PORNOGRAPHY MAY LEAD TO TORT LIABILITY

Jamila Johnson[1]

Abstract

This Article addresses a New Jersey appellate court's holding which suggests that employers have a common law duty to investigate online misconduct by their employees. In *Doe v. XYC Corp.*, the Appellate Division of the Superior Court of New Jersey held that an employer has a duty to act when (1) it knows that an employee's use of the Internet would endanger a third person; and (2) it has reason to believe that it may discipline the employee for online activities in the workplace. The court stated that, under this duty to act, an employer must investigate, discipline, and inform authorities of the danger. This Article discusses the implications of the case for employers.

Table of Contents

INTRODUCTION

<1>In late 2005, a New Jersey appellate court held that an employer who has knowledge that its employee is viewing child pornography[2] on a company computer has a duty to investigate and act lest the employee's action lead to harm to a third party.[3] Individuals generally have no duty to act absent a special relationship with a victim or with an aggressor.[4] A New Jersey appellate court in *Doe v. XYC Corp* examined this legal doctrine and assessed whether employers have a duty to monitor employee Internet use to prevent employees from causing harm to third parties. The court used the analysis of vicarious liability in The Restatement (Second) of Torts in order to find that employers have a duty to police company computers when suspicion of wrongdoing arises. The court's holding thereby expanded the limited circumstances in which an affirmative duty to act arises. Despite its limited effect as precedent, this case illustrates how at least one appellate court has applied common law doctrine in a novel situation involving use of technology.

INVESTIGATING VIOLATIONS

<2>In late December 2005, a New Jersey appellate court ruled that a trial court had erred when it granted a summary judgment motion in favor of a company in a negligence suit. [5] The mother of a girl who had been sexually assaulted by

her stepfather filed the suit against the stepfather's employer.[6] The mother alleged that the company had an Internet use policy and had notice that the employee, the stepfather, had viewed pornography on workplace computers at the defendant company's 250-person headquarters.[7] The argument followed that: had the company further investigated its suspicions, the company would have discovered that its employee was uploading photos of his minor stepdaughter onto child pornography websites. Additionally, the plaintiff argued that these photos were taken without the daughter's knowledge, and, had the company investigated and acted in a timely manner, the abuse that soon followed would never have happened.[8]

<3>The defendant employer is alleged to have made several mistakes over the years, all of which could easily be repeated by other employers. The employer allegedly did not take the complaints of co-workers seriously and failed to use the information gathered by monitoring the employee's Internet use to start a timely investigation.[9] Specifically, the plaintiff's complaint states that XYC's suspicions of the employee's online habits had been evident for about four years.[10] During these four years, employees in the Information Technology department ("IT department") reviewed computer reports and noticed that the employee in question had been visiting pornographic sites, but they did not inform supervisors.[11] Further, the employee's immediate supervisor reported suspicions of Internet misuse to the IT department — suspicions that were again confirmed by this unit.[12] When tracking the employee's Internet activity, the IT department found more evidence that the employee accessed bestiality and necrophilia photos as well as pornographic websites with "teen" in the title[13] from his company computer.[14] The department, however, took no action because the head of the department stated that tracking website usage of individual employees was against company policy[15] and that nothing could be done with the information gathered.[16]

<4>On other occasions another co-worker reportedly complained to company supervisors that the employee acted suspiciously and constantly shielded his computer screen.[17] The co-worker also reported concerns about the employee viewing pornography.[18] At that time, management took no action.[19] A year later, a co-worker still concerned that he was looking at pornography, accessed the websites in the defendant's Internet search history. She brought the records to an immediate supervisor.[20] The supervisor subsequently went into the employee's cubicle, found the same evidence and brought it to management's attention.[21]

<5>The supervisor allegedly discussed the matter with the employee and thought the employee had stopped, but several months later saw evidence of misbehavior.[22] The supervisor told no one else of his continuing suspicions before going on vacation in June 2001.[23] When he returned later that month he found that the employee had been arrested on child pornography charges on June 21.[24]

APPLICATION OF RESTATEMENT (SECOND) OF TORTS § 317

<6>The court, in *Doe v. XYC Corp.*, applied a section of the Restatement (Second) of Torts related to vicarious liability to determine that there is a duty of care to third parties who may be injured by an employee's Internet use. [25] That duty of care requires an employer, at the very least, to investigate suspicions that arise regarding the possibility of misbehavior that is illegal or inherently dangerous to third parties.[26]

<7>Generally, a person has no duty to control the conduct of another person absent a special relationship.[27] Such a relationship exists in an employment situation, and an employer has a duty to control the actions of employees when those actions are within the scope of employment.[28] The law has often made an exception to this general principle so that, in certain circumstances, an employer has a duty to control actions outside the scope of employment.[29]

<8>The Restatement (Second) of Torts § 317 provides an exception to the "scope of employment" principle. This section

of the Restatement is most often cited in situations such as: "X" is an employer and allows employee "Y" to drive a company car for personal use. X knows that Y has a poor driving record and tends to cause many car accidents. Y then causes an accident injuring several people and causes property damage. Section 317 specifically states:

<9>Duty of Master To Control Conduct Of Servant

> A master is under a duty to exercise reasonable care so to control his servant while acting outside the scope of his employment as to prevent him from intentionally harming others or from so conducting himself as to create an unreasonable risk of bodily harm to them, if
>
> (a) the servant
>
> (i) is upon the premises in possession of the master or upon which the servant is privileged to enter only as his servant, or
>
> (ii) is using a chattel of the master, and
>
> (b) the master
>
> (i) knows or has reason to know that he has the ability to control his servant, and
>
> (ii) knows or should know of the necessity and opportunity for exercising such control.[30]

<10>Courts have interpreted this opening segment of Section 317 of the Restatement to impose a duty of reasonable care on employers to control their employees in situations where an employee may cause bodily harm to third parties. Many states read § 317 to apply only to physical injuries caused by an employee as suggested by the plain language of the Restatement.[31] Minnesota law, for example, finds the duty "unambiguously limited to preventing an employee from inflicting personal injury upon a third person" and does not extend an employer's duty to any other form of injury.[32] However, it should be noted that a multitude of cases involving the § 317 employer duty have emerged in discrimination and sexual harassment cases where the plaintiff presents a theory of negligent retention involving physical manifestations such as lack of sleep or mental distress as the required physical injury.[33]

<11>Section 317 is usually a helpful framework for cases based on a claim of negligent supervision.[34] Negligent supervision is described as "the failure of the employer to exercise ordinary care in supervising the employment relationship so as to prevent the foreseeable misconduct of an employee causing harm to others."[35] In *Mandy v. Minnesota Min. and Mfg.*, for example, a district court applying Minnesota law referred to Section 317 in a case dealing with sexual harassment.[36] The plaintiff, who had alleged violent touching (a physical harm) after having complained of sexual harassment, brought successful claims of negligent supervision and retention.[37]

<12>Section 317(a) requires that there must be a risk of bodily harm on the employer's property or that the employee must use the property of the employer to cause harm to third parties.[38] In many property cases, the property of the employer in such actions is a company vehicle.[39] Comment b accompanying § 317 has been a guide for these properties. The comment requires an employer to police its premises and use reasonable care to exercise its authority to prevent employees from doing harm to others and misusing "chattels which…[it] entrusts [to] them for use."[40]

<13>Section 317(b) causes the most controversy and uncertainty because it requires a plaintiff to show that the employer knew or should have known that the employee was engaged in dangerous misconduct that could harm a third party.[41] These cases usually rest on the question of fact: whether the employer "should have known, or even should have been suspicious" about what harm arose as a result of the employee's conduct.[42]

<14>The *XYC* trial court granted the employer's motion for summary judgment.[43] The trial court focused on "whether or not the employer had a duty, as argued by the plaintiffs, to do more than it did with respect to this defendant employee and whether there was a standard of conduct to which the duty required this corporate defendant to conform."[44] The court found that there was no such duty under Restatement (Second) of Torts § 314, the section that the trial court found most relevant.[45] Under § 314 the court considered the fact that an actor realizes, or should realize, that action on his part is necessary for another's aid or protection does not of itself impose upon him a duty to take such action.[46] The trial court only referred to § 317 in passing.[47]

<15>In contrast, the appellate court in *XYC* found that § 317 was highly relevant and that an employer has a duty under § 317 to monitor employee computers. Specifically the appellate court found three duties applicable. First, an employer has a duty to investigate the employee's activities that arises when an employer has notice of an employee's improper computer use.[48] Second, an employer has a duty to take prompt and effective action to stop unauthorized activity by an employee, lest it result in harm to third parties.[49] Third, an employer has a duty to report an employee's illegal behavior to the authorities in certain circumstances, including child pornography.[50] However, the appellate court determined that the issue of proximate cause could not be settled based on the record before it, and therefore remanded the case back to the trial court for further fact finding.[51]

<16>As required under § 317, the plaintiff alleged physical harm due to sexual abuse. However, the plaintiff limited her claim to the conduct that took place at the employee's workplace — the uploading and transmitting of photos of a minor to child pornography websites.[52] While not mentioned by the court, it is important to consider the differences between pornography and child pornography. As a basic starting point, possession of child pornography is illegal,[53] whereas possession of adult pornography is not.[54] The appellate court stated that child pornography has "by its very nature… been deemed by the state and federal lawmakers to constitute a threat to 'others;' those 'others' being the children who are forced to engage in or are unwittingly made the subject of pornographic activities."[55]

<17>In *New York v. Ferber*, the U.S. Supreme Court accepted the judgment of the New York legislature that the "use of children as subjects of pornographic materials is harmful to the physiological, emotional, and mental health of the child."[56] Further, the Supreme Court found that the distribution of child pornography is intrinsically related to sexual abuse.[57] The Court found that the materials serve as a permanent record of the child's participation, and the harm is tangible and much larger than the pornography alone.[58]

<18>Commentators have stated that the holding in *XYC* is narrowed by its facts.[59] The case addressed child, rather than adult, pornography.[60] The viewing of most pornography is legal and therefore does not likely lead to legally cognizable harm to third parties that would fall under § 317.[61] An employer, therefore, would not have a duty to report an employee's observation of pornography on a company computer to authorities or reprimand the employee because the viewing of most pornography does not lead to a tangible harm to third parties and would not fall under § 317.[62] Yet, although the phrase "teen" in pornography websites may sometimes be indicative of child pornography, it is also common in pornography websites that do not have child pornography. Therefore, a company that chooses to monitor employee Internet use to prevent child pornography would also need to monitor whenever there is reason to know that an employee is viewing pornography.[63] There is certainly concern because few employers will want to search through the employer's computer records, and more have concerns about interactions with employees about such monitoring.[64] For some companies this level of monitoring would be impractical. But at the very least, some form of investigation into Internet use should begin if a company is put on notice as to employees accessing pornography at work.

<19>The second prong of § 317 requires that an employee actually injure a third party on the employer's premises or

while "using a chattel of the master."[65] The trial court in *XYC* held that the harm to the plaintiff did not occur at the defendant's premises and did not involve a chattel belonging to the defendant.[66] It held this because the harm caused by the employee — invading a 12-year-old girl's privacy, photographing her naked, and sexually abusing her — was inflicted at the home of the employee.[67] In contrast, the appellate court found that because all the photos were uploaded to the Internet with work computers, the "plaintiff must establish that [she] suffered some harm to her person or psychological harm as a result of the Internet transmission of her photos."[68] If she is able to do so at trial, then the second prong of § 317 is satisfied. In further application, it is unclear whether laptops in the home of an employee would be another situation where the employer would have to monitor the use of its chattel, but under the court's § 317 analysis, there is nothing to suggest a different result.

<20>The third prong of the § 317 analysis requires an employer to know of the reason to control the employee. In other words, the employer must know the possible harm that may occur and that there is a reason to suspect the harm could occur in this situation. Much of this decision relies on the question of whether XYC, after suspecting that an employee was viewing child pornography at work, should have investigated further. This is a question of whether XYC, which had the capability to monitor employee Internet usage, had a duty to do so.[69] The trial court relied on the New Jersey Supreme Court case *Blakey v. Cont'l Airlines, Inc.*[70] in finding that the employer had no duty to monitor the employee's "private communications."[71] It also found that absent this duty, there was no evidence that the company knew or should have known the employee was viewing *child* pornography.[72]

<21>The appellate court, however, found *Blakey* inapplicable because the communication of the employee was not a "private communication."[73] The messages were not private because XYC had an email policy that stated, "all messages composed, sent or received on the e-mail system are and remain the property of [XYC]. They are not the private property of any employee."[74] The employer's policy also stated that employees could "access sites, which are of a business nature only."[75] The company policy further stated that violations would be reported to human resources.[76]

<22>The appellate court determined that several facts showed that the employer knew or should have known about the actions of the employee. First, the court found that the company at least knew that the employee was looking at Internet sites that were not of a business nature.[77] Second, the court found that the employer's Internet policy requiring violations to be reported to human resources, "was not simply intended as an idle gesture but was intended to trigger an investigation…"[78] Therefore, the court concluded that the policy, viewed with the complaints, created a duty for the employer to investigate and discipline the employee.[79] Had the employer fulfilled this duty, the employer would have discovered the employee was accessing child pornography.[80] The court found the harm was reasonably within the company's apprehension.[81]

<23>Additionally, the court found that under § 317 and public policy, XYC had a duty to act to prevent the employee from harming others.[82] The court found that the illegal nature of the act also suggested strong public policy support for the holding.[83]

IMPLICATIONS FOR EMPLOYERS

<24>*XYC Corp*. is the first appellate case to apply § 317 to an employee's Internet use on a workplace computer as a distinct form of tangible property at the workplace. The New Jersey appellate court found that under the facts alleged, an employer had an affirmative duty to monitor and investigate further to prevent harm to third parties. Several implications may result. First, the scope of this situation can be read narrowly to apply only to child pornography.[84] However, this narrow reading provides little help to employers looking to shield themselves from such litigation. *XYC* suggests that once an employer has a policy or practice of monitoring email communications and suspects pornography, it has a

corresponding legal duty to investigate.[85] In the past year, half of Fortune 500 companies experienced at least one workplace Internet pornography incident, according to a Delta Consulting survey on inappropriate images in the workplace.[86] These incidents, under the *XYC* ruling, would have to be investigated and disciplined if the behavior could injure a third person.

<25>Second, the case could be read broadly to apply to any workplace Internet searches or communications that may cause physical harm to third parties. For instance e-mail communications that harass third parties and cause emotional trauma may meet the requisite harm requirement. Another possibility could be situations where an employee is blogging at work, providing incorrect medical advice or encouraging a minor to do something illegal.

<26>In situations where employers already monitor employee communications, does the mere fact of monitoring create an affirmative duty to investigate perceived employee misconduct or harmful uses of the Internet? [87] Employer monitoring of employee Internet usage is widespread and takes many forms according to the American Management Association (AMA). A 2005 AMA report states that 76 percent of employers monitor workers' Internet connectivity, keystrokes, and time spent on the keyboard.[88] The study also reports that 86 percent of employers who monitor email communications inform their employees.[89] Eighty-four percent of surveyed employers have written policies governing personal use of email and 81 percent have written policies governing personal use of the Internet.[90] After *XYC*, there is a possibility that other courts will view this employer policy of monitoring as a factor that removes privacy from employee communication—this would effectively invoke an employer's affirmative duty to act when suspicion of illicit activity arises.

<27>Based on *XYC*, an employer may need to actively investigate suspected violations of its computer usage policy if it has implemented a policy that states that an employee's communications are not private and that certain rules must be followed. One case in the Reporter's Notes to § 317 can provide helpful advice on this matter. The notes reference a case from the early 1900s, *Hogle v. H.H. Franklin Mfg. Co*. [91] The Restatement commentary notes that in the *Hogle* case the court went so far as to hold that the mere giving of strict orders was not sufficient to relieve the master from liability, although it does not appear that the orders given were actually enforced, or even that any effort was made to discover whether the orders had been sufficient to prevent the continuance of the improper practices."[92] This case might suggest that an employer's strict orders regarding Internet policies provide little protection against liability if the employer knows of its employee's illegal behavior.

<28>Since late 2005, when *XYC* was decided, at least one other case has cited to the opinion in a favorable manner.[93] However, the positive citation related to issues of proximate cause that should be left for the jury[94] — no other court has yet to adopt or reject a similar interpretation of § 317 made by the New Jersey Appellate Division.

CONCLUSION

<29>Only time will tell whether other courts will follow the lead of the *XYC* decision. However, the rationale in *XYC* is such that employers should think long and hard before turning a blind eye when complaints arise regarding suspected Internet misconduct, particularly if such misconduct is illegal. Employers need to distribute and implement computer use policies to prevent employees from causing harm to third parties. But without investigation into violations, the existence of these policies may open an employer to more liability if anyone is physically harmed by an employee's Internet behavior. Employers in New Jersey, and perhaps elsewhere, have a common law duty to act when they have knowledge of an employee viewing child pornography on a workplace computer.

<< Top

Footnotes

1. Jamila Johnson, University of Washington School of Law, Class of 2007. Thank you to University of Washington School of Law Professor Anita Ramasastry, Vincent Polley of Dickinson Wright PLLC and Evgenia Fkiaras for their guidance.

2. The case specifically addresses child pornography, or rather "the scourge of child pornography", in the workplace. Doe v. XYC Corp., 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005).

3. *Doe v. XYC Corp.*, 887 A.2d at 1158 (holding "an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities." Employer also has a duty to take "prompt and effective action" to stop the activity so that harm does not come to "innocent third-parties").

4. *See* Gelbman v. Second Nat'l Bank, 458 N.E.2d 1262 (Ohio 1984); Tarasoff v. Regents of University of California, 551 P.2d 334, 343 (Cal. 1976) (one person owed no duty to control the conduct of another); D'Amico v. Christie, 518 N.E.2d 896, 901 (N.Y. 1987) ("defendant generally has no duty to control the conduct of third persons so as to prevent them from harming others, even where as a practical matter defendant can exercise such control"). James v. Wilson, 95 S.W.3d 875, 890 (Ky. Ct. App. 2002) (quoting RESTATEMENT (SECOND) TORTS §314, Comment C, "the result of the rule has been a series of older decisions to the effect that one human being, seeing a fellow man in dire peril, is under no legal obligation to aid him, but may sit on the dock, smoke his cigar, and watch the other drown. Such decisions have been condemned by legal writers as revolting to any moral sense, but thus far they remain the law.").

5. *Doe v. XYC Corp.*, 887 A.2d at 1158.

6. *Id*.

7. *Id.* at 1158-61.

8. *Id.*

9. *Id*.

10. *Id.*

11. *Id.*

12. *Id.*

13. The word "teen" in the title of a pornographic website does not necessarily mean the actors are underage or that the website is illegal. The United Stated Supreme Court found in *New York v. Ferber* that a child pornography ban was permitted when the pornography was the product of sexual abuse—the production of the work, not its conduct, justified the state action. Where the images are themselves the product of child sexual abuse, *Ferber* recognized that the State had an interest in stamping it out without regard to any judgment about its content. New York v. Ferber, 458 U.S. 747 (1992). Further, the Supreme Court struck down a ban on images that merely depict child pornography without the use of actual minors as being distinguishable from *Ferber*. *See* Ashcroft v. Free Speech Coalition, 535 U.S. 234, 240 (2002).

14. *Doe v. XYC Corp.,* 887 A.2d at 1159.

15. The company's policy was not to review Internet use when there was no complaint or suspicion. *Id*.

16. *Id.* at 1159.

17. *Id*.

18. *Id.*

19. *Id.*

20. *Id.* at 1159-60.

21. *Id.*

22. *Id.* at 1160.

23. *Id.*

24. *Id.*

25. *Id*. at 1158.

26. *Id.*

27. *See* note 4. There is an exception in Minnesota, Vermont, and Rhode Island — states that have statutes providing for fines for failure to provide aid. Angela Hayden, Imposing Criminal and Civil Penalties For Failing To Help Another: Are "Good Samaritan" Laws Good Ideas? 6 New Eng. Int'l & Comp. L. Ann. 27 (2000).

28. *See* Strock v. Pressnell, 527 N.E.2d 1235, 1244 (Ohio 1988); Ventura v. Cincinnati Enquirer, 396 F.3d 784, 790 (6th Cir. 2005) (Under Ohio law, "the doctrine of respondeat superior applies only when the employee acts within the scope of his employment").

29. Pilgrim v. Fortune Drilling Co., Inc., 653 F.2d 982, 985 (5th Cir. 1981) ("Restatement (Second) of Torts § 317 sets forth circumstances under which an employer has a duty to control the conduct of an employee who is outside the scope of his employment.").

30. Restatement (Second) of Torts § 317 (1965).

31. *See* Semrad v. Edina Realty, Inc., 493 N.W.2d 528, 534 (Minn. 1992) ("The entire thrust of § 317 is directed at an employer's duty to control his or her employee's physical conduct while on the employer's premises or while using the employer's chattels, even when the employee is acting outside the scope of the employment, in order to prevent intentional or negligent infliction of personal injury."); Choroszy v. Wentworth Inst. of Tech., 915 F. Supp. 446, 451 (D.Mass. 1996) (explaining § 317 as extending only through "an 'unreasonable risk of bodily harm' to others). Note that the Iowa Supreme Court recently overturned a ruling that dismissed a claim for lack of physical injury. Kiesau v. Bantz, 686 N.W.2d 164, 180 (Iowa 2004).

32. Mandy v. Minnesota Min. and Mfg., 940 F. Supp. 1463, 1471 (D. Minn. 1996).

33. *E.g.* Schofield v. Trs. of Univ. of Penn., 894 F. Supp. 194 (E.D. Pa. 1995); Chontos v. Rhea, 29 F. Supp. 2d 931 (N.D. Ind. 1998); Davis v. USX Corp., 819 F.2d 1270, 1273-74 (4th Cir. 1987).

34. This is the case because inherently the Restatement (Second) of Torts deals with just that, torts. Many have been based on negligence, *e.g.* Corrigan v. U.S., 815 F.2d 954 (4th Cir. 1987) (Federal Tort Claim action brought by plaintiff struck by army vehicle driven by drunk army private). However, some cases citing Section 317 have been intentional torts. *See* Davis v. U.S. Steel Corp., 779 F.2d 209 (4th Cir. 1985) (plaintiff could sue company for assault and battery and intentional infliction of emotional distress claims under the doctrine of respondeat superior).

35. *Mandy*, 940 F. Supp. at 1471.

36. *Id.*

37. *Id*.

38. Restatement (Second) of Torts § 317(a) (1965).

39. *E.g*. Schele v. Porter Mem'l Hosp., 198 F. Supp. 2d 979, 995 (N.D. Ind. 2001); Killian v. Caza Drilling, Inc., 131 P.3d 975, 981 (Wyo. 2006); Brewster v. Rush-Presbyterian-St. Luke's Medical Center, 836 N.E.2d 635 (Ill. App. Ct. 2005).

40. Restatement (Second) of Torts § 317 cmt. B (1965).

41. *See* Campbell v. A.C. Equipment Servs. Corp., Inc., 610 N.E.2d 745, 750 (Ill. App. Ct. 1993) (duty only arises if employer knows of the danger); Thompson v. Green Mountain Power Corp., 144 A.2d 786, 789 (Vt. 1958) ("foresight of harm lies at the foundation of negligence"); Rue v. Wendland, 33 N.W.2d 593, 595 (Minn. 1948) (knowledge is "an essential element of negligence").

42. Doe v. Hartz, 52 F. Supp. 2d 1027, 1074 (N.D. Iowa 1999) (internal quotations omitted).

43. Doe v. XYC Corp., 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005)

44. Doe v. XYC Corp., 887 A.2d at 1161 (N.J. Super. Ct. App. Div. 2005) (citing the Restatement (Second) of Torts § 328B (1965)). "In an action for negligence the court determines (a) whether the evidence as to the facts makes an issue upon which the jury may reasonably find the existence or non-existence of such facts; (b) whether such facts give rise to any legal duty on the part of the defendant; (c) the standard of conduct required of the defendant by his legal duty; (d) whether the defendant has conformed to that standard, in any case in which the jury may not reasonably come to a different conclusion; (e) the applicability of any rules of law determining whether the defendant's conduct is a legal cause of harm to the plaintiff; and (f) whether the harm claimed to be suffered by the plaintiff is legally compensable." Restatement (Second) of Torts § 328B (1965).

45. Doe v. XYC Corp., 887 A.2d at 1161.

46. *Id.*

47. *Id.*

48. *Id.* at 1165-66.

49. *Id*. at 1165-1167.

50. *Id.* at 1167 (stating "[w]ith actual or imputed knowledge that Employee was viewing child pornography on his computer, was defendant under a duty to act, either by terminating Employee or reporting his activities to law enforcement authorities, or both? We conclude that such an obligation exists. The existence of a duty is a matter of law, 'deriv[ing] from considerations of public policy and fairness'") (internal citations omitted)). It should also be noted that all 50 states have some form of mandatory child abuse and neglect reporting law in order to qualify for funding under the Child Abuse Prevention and Treatment Act, as amended, 42 U.S.C. §§ 5101 et seq (2000). *See* Susan K. Smith, *Mandatory Reporting of Child Abuse and Neglect*, http://www.smith-lawfirm.com/mandatory_reporting.htm (last visited March 25, 2007).

51. *Doe v. XYC Corp*., 887 A.2d at 1169-1170.

52. *Id.* at 1163-64.

53. New York v. Ferber, 458 U.S. 747, 764 (1982).

54. Miller v. California, 413 U.S. 15, 22-23 (1973).

55. *Doe v. XYC Corp.*, 887 A.2d at 1168.

56. *Ferber*, 458 U.S. at 758.

57. *Id*. at 759.

58. *Id*. The Court also quoted David P. Shouvlin, *Preventing the Sexual Exploitation of Children: A Model Act*, 17 WAKE FOREST L. REV. 535, 545 (1981). "[P]ornography poses an even greater threat to the child victim than does sexual abuse or prostitution. Because the child's actions are reduced to a recording, the pornography may haunt him in future years, long after the original misdeed took place."

59. B.A. Howell & P.H. Luehr, *Child Porn Poses Risks to Companies that Discover it in the Workplace*, N.Y. L.J., Oct. 4, 2004, *available at* http://www.strozllc.com/docs/pdf/ChildPornPosesRisks.pdf.

60. First, *XYC* is not the first time the law has identified the liability employers might face from an employee's downloading or uploading of pornography. Three overlapping federal criminal statutes could put companies at risk for handling child pornography. 18 U.S.C. §§ 2251(a), 2252(a), 2252A(a); *See also* Howell & Luehr, *supra* note 50; Beryl A. Howell, *Digital Forensics: Sleuthing On Hard Drives*, 31-FALL VT. B.J. 39, 45 (2005). There is a limited affirmative defense available under the statute if an individual or employer has less than three images. The defendant must show that she did not retain any offending visual depiction, not allow anyone but law enforcement to access the image, and take prompt and reasonable steps to destroy each visual depiction or report the matter to law enforcement. A company that avoids the problem by not calling the authorities or deleting the material will still face problems for possibly obstructing an investigation. However, *XYC* is unique in that it suggests that there is a duty to investigate and to act in order to prevent cybercrime and connects issues of vicarious liability with crimes committed via the Internet.

61. As a general rule, pornography may not be banned (thereby making it illegal) unless it is obscene. Ashcroft v. Free Speech Coalition, 535 U.S. 234, 240 (2002). Obscenity is determined by the standard in Miller v. California, 413 U.S. 15 (1973). Child Pornography is illegal because of how it is made (or the harm) not what it depicts. *Ashcroft*, 535 U.S. at 249. Court cases have not addressed whether physical harm can arise from viewing of pornography.

62. *See* G.M. Filisko, *Employer Had Duty To Stop Porn Surfing*, 5 No. 1 A.B.A. J. E-REPORT 3, January 6, 2006.

63. "Employers are primarily concerned about inappropriate Web surfing, with 76% monitoring workers' Website connections. Fully 65% of companies use software to block connections to inappropriate Websites—a 27% increase since 2001 when AMA and ePolicy Institute last surveyed electronic monitoring and surveillance policies and procedures in the workplace." AMAnet.org, *2005 Electronic Monitoring & Surveillance Survey*, http://www.amanet.org/research/pdfs/EMS_summary05.pdf (last visited April 11, 2007).

64. *See* Monte Enbysk, *Should You Monitor Your Employees' Web Use?*, January 19, 2007, http://www.microsoft.com/smallbusiness/resources/management/employee_relations/should_you_monitor_your_employees_web_use.mspx (last visited April 11, 2007) ("This is a situation more and more businesses face today. Employee-monitoring devices — known to many as "spyware" — have become more attractive, affordable and easy to use. Companies see their value in helping to increase security, improve productivity, and to reduce employee misbehavior, competitive information leaks, and liability risks. Many employees, however, believe monitoring software infringes their privacy rights. If the implementation is communicated poorly, or the company simply goes too far in its zealousness, morale could be damaged and good people may quit." *See also* Stephanie Armor, *Employers Look Closely at What Workers Do On Job*, USA TODAY, Nov. 7, 2006.

65. RESTATEMENT (SECOND) OF TORTS § 317 (1965).

66. Doe v. XYC Corp., 887 A.2d 1156, 1162-63 (N.J. Super. Ct. App. Div. 2005).

67. *Id.*

68. *Id.* at 1170.

69. "In response to an interrogatory asking whether it had the 'capability ... to monitor and/or track employee use of the internet and/or e-mails at work on their work computer,' defendant responded that it 'could have implemented software that would have permitted it to monitor employees' activity on the Internet.' Indeed, as the facts recited earlier reveal, on at least two occasions defendant conducted a limited investigation of Employee's computer use, thereby demonstrating its capability to do so." *Doe v. XYC Corp.*, , 887 A.2d at 1164.

70. Blakey v. Cont'l Airlines, Inc., 751 A.2d 538 (2000).

71. *Doe v. XYC Corp*., 887 A.2d at 1162 (2005).

72. *Id.* at 1161.

73. *Id.* at 1162.

74. *Id.* at 1166.

75. *Id.*

76. *Id*.

77. *Id*.

78. *Id*.

79. *Id.* at 1166-1167.

80. *Id.*

81. *Id.* at 1168.

82. *Id.* at 1167-68.

83. Three overlapping federal criminal statutes could put companies at risk for handling child pornography. 18 U.S.C. §§2251(a), 2252(a), 2252A(a); *See also* B.A. Howell & P.H. Luehr, Child Porn Poses Risks to Companies that Discover it in the Workplace, N.Y. L.J., Oct. 4, 2004, available at http://www.strozllc.com/ChildPornPosesRisks.pdf; Beryl A. Howell, "Digital Forensics: Sleuthing On Hard Drives," 31-FALL Vt. B.J. 39, 45 (2005). There is a limited affirmative defense available under the statute if an individual or employer has less than three images. The defendant must show that she did not retain any offending visual depictions, not allow anyone but law enforcement to access the image, and take prompt and reasonable steps to destroy each visual description or report the matter to law enforcement. A company that avoids the problem by not calling the authorities or deleting the material will still face problems for possibly obstructing an investigation. However, *XYC* is unique in that it suggests that there is a duty to investigate and to act in order to prevent cyber crimes and connects issues of vicarious liability with Internet crimes.

84. *See* Helen Gunnarsson, *Must Employers Try To Stop Employees' "Unauthorized Activity"?*, 94 ILL. B.J. 172 (2006) (quoting Illinois attorney who finds it unlikely that the court would reach the same result with anything other than child pornography).

85. Since terms such as "teen" or "child" as a keyword search does not provide much guidance as to whether pornography is legal or illegal, employers may need to monitor more than just the names of websites.

86. Delta Consulting, "Survey: Inappropriate Images in the Workplace" (June, 2005). For fuller discussion of liability risks, *see* Howell & Luehr, *supra* note 50; *see also* Howell, *supra* note 51, at 45.

87. *See* Lisa J. Sotto & Elisabeth M. McCarthy, *Workplace Privacy In The U.S.: What Every Employer Should Know*, 866 P.L.I./Pat. 201, 227 (2006).

88. AMAnet.org, *2005 Electronic Monitoring & Surveillance Survey*, http://www.amanet.org/research/pdfs/EMS_summary05.pdf (last visited April 11, 2007).

89. *Id*.

90. *Id*.

91. Hogle v. H.H. Franklin Mfg. Co., 92 N.E. 794 (N.Y. 1910); *See also* RESTATEMENT (SECOND) OF TORTS § 317 reporter's notes.

92. RESTATEMENT (SECOND) OF TORTS § 317 (1965).

93. Lechmanick v. Kiss, 2006 WL 3328261, at *5 (N.J. Super. App. Div. Nov. 17, 2006)

94. *Id.*