Jane DOE individually and as g/a/l for Jill Doe, a minor, Plaintiff-Appellant,
v.
XYC CORPORATION, Defendant-Respondent.

887 A.2d 1156 (N.J. Super. 2005)

Superior Court of New Jersey,
Appellate Division.

Argued Sept. 28, 2005.
Decided Dec. 27, 2005.

Before Judges CONLEY, WEISSBARD and SAPP-PETERSON.

The opinion of the court was delivered by WEISSBARD, J.A.D.

Even the workplace is not free from the scourge of child pornography, as the present case illustrates.

Plaintiff Jane Doe (Jane), on behalf of her minor daughter Jill Doe (Jill), appeals from a summary judgment dismissing her complaint against defendant XYC Corporation which sought to hold defendant responsible for the activities of one of its employees (Employee) who was Jane's husband and the stepfather of Jill. We reverse. We hold that 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 and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties. No privacy interest of the employee stands in the way of this duty on the part of the employer.

I

The case having been dismissed on summary judgment, we set out the facts, as well as the inferences from the facts, in the light most favorable to plaintiff. [FN1] *Brill v. Guardian Life Ins. Co. of Am.*, 142 *N.J.* 520, 540, 666 *A.*2d 146 (1995).

A. EMPLOYEE'S WORKPLACE HISTORY.

Defendant employed approximately 250 employees at its headquarters in Somerset County, where Employee was an accountant. His workspace consisted of a small cubicle located along a wall which also contained the cubicle of another accountant, as well as corner offices of defendant's Director of Finance and its Controller, Pamela Martin. The cubicles had no doors and opened into a hallway.

Sometime in 1998 or 1999, Corey Shelton, defendant's former Internet Services Manager, informed George Griesler, defendant's Senior Network Administrator, that he had noted, on reviewing computer log reports, that Employee had been visiting pornographic sites. Griesler and

Shelton told Employee to stop the activity but did not inform any of their supervisors. In early 2000, Employee's immediate supervisor, Keith Russinoff, also told Griesler that Employee was visiting inappropriate websites. Russinoff asked Griesler if he could track Employee's Internet usage and Griesler conducted a limited investigation by reviewing computer logs for a day or two and isolating those visited by Employee. Although Griesler had the ability to open those websites, he did not do so, nor did he print out a list of the sites in question. Based on the website titles, Griesler recognized the sites as pornographic, although he only recalled the name of one site, "Sextracker," that Employee had visited several times. Griesler advised Russinoff and Jessica Carroll, defendant's Director of Network and PC Services, about the results of his investigation, but was shortly thereafter admonished by Carroll not to access any employee's logs, including that of Employee, ever again.

Carroll recalled being told by Griesler that Employee's server logs revealed that he was visiting pornographic sites on his office computer, including "bestiality" and "necrophilia" sites. Carroll did not report the matter further or discuss it with Employee, because of a company policy communicated by e-mail to certain management personnel from Kevin O'Connor, Senior Director of Business Information Systems, that prohibited monitoring of or reporting the Internet activities of employees. Violation of the policy could result in a penalty ranging from reprimand to termination.

Around December 2000, another accounting department employee, Mary Ann Carlson, told her manager, Jill Ray, that Employee was acting strangely by shielding his computer screen and quickly minimizing it so that others could not see what he was doing. Carlson saw Employee act in this manner two or three times a day, and discussed his behavior with Ray, who had also seen it at least five times. They surmised that Employee was viewing pornography. Ray eventually discussed the matter with the Manager of Financial Reporting, Suzanne Colon, advising her that she and Carlson were uncomfortable with Employee's conduct. Nevertheless, no action resulted from their complaints.

In February 2001, Carroll herself looked at the sites Employee had been visiting and concluded that they were pornographic. She did not open the sites and did not discuss her findings with anyone or take any action.

In late March 2001, Carlson discussed Employee's computer activities with Russinoff, telling him that while walking past Employee's cubicle she had seen a picture of a woman in a bikini with "very large breasts" in a "sultry pose" on Employee's computer screen. Russinoff acknowledged to Carlson that he had also seen Employee blocking his computer screen. That same month, Russinoff went into Employee's cubicle during lunch when Employee was out, and clicked on the "websites visited" on Employee's computer. Russinoff discovered that Employee had visited "various porn sites" and printed out what was displayed on the screen. The printout identified obvious porn sites ("Big Fat Monkey Blowjobs," "Yahoo Groups--Panties R Us Messages" and "Sleazy Dream Main Page") as well as one that specifically spoke about children: "Teenflirts.org: The Original Non Nude Teen Index." Russinoff, however, did not scroll down the "websites visited" to see what other sites Employee had visited. Russinoff was not sure what the various "Yahoo Groups" sites were and did not open any of the sites to further investigate their contents.

Russinoff showed the printout to his boss, Colon, who showed signs of disgust. Later that day, Russinoff met with Colon and her boss, Pamela Martin, "to discuss what to do." They decided that Russinoff should talk to Employee. Russinoff met with Employee on March 6, 2001 and told him that there had been reports of inappropriate computer usage. He told Employee to stop these activities and Employee said he would. Russinoff confirmed his conversation with Employee in an e-mail to Colon and Martin on March 7, 2001. Employee appeared to stop his activities, but in early June 2001, Russinoff saw that he had started again. Nevertheless, he told no one and left on a business trip, not returning until after Employee's arrest on child pornography charges on June 21, 2001.

B. EMPLOYEE'S CONDUCT WITH JILL.

Employee and plaintiff were married in October 2000. For about five months prior to his arrest, Employee had been secretly videotaping and photographing Jill at their home in nude and semi-nude positions. Jill was ten years old at the time. Jill had been at defendant's headquarters for Take Your Daughter To Work Day and had attended company outings. As a result, supervisory personnel were aware that defendant had married a woman with a young child.

On June 15, 2001, Employee transmitted three of the clandestinely-taken photos of Jill Doe over the Internet from his workplace computer to a child porn site in order to gain access to the site. Employee later acknowledged that he stored child pornography, including nude photos of Jill Doe, in his workplace computer. He admitted to downloading over 1000 pornographic images while working for defendant. Employee was arrested on June 21, 2001 following a June 19, 2001 search of his work space and work computer based on a search warrant. At that time, his computer showed e-mails being sent to pornographic websites and interactions with others regarding child pornography. Indeed, photographs of Jill found in a dumpster at defendant's headquarters apparently led to his arrest. According to Martin, her search of Employee's desk on June 20 as part of defendant's exit policy [FN2] turned up a folder with seventy downloaded pornographic photos, including ones of young females. In addition, the Prosecutor's Office, in searching Employee's computer, found numerous child pornography images. Specifically, Detective DeBella searched Employee's workplace computer as it was on the day of Employee's arrest and found that Employee had indeed been visiting "Incest Taboo" and "Young Girls Nude 13 to 17 years old."

C. DEFENDANT'S MONITORING CAPABILITIES.

Defendant possessed and could have implemented software that would have permitted it to monitor employees' activities on the Internet. Specifically, defendant's Director of Network Services testified that defendant tried Web Trends, the most common such software, which would allow it to monitor where anybody goes on the Internet, and for how long they visit a particular site. Moreover, Griesler, then defendant's Network Administrator, described how readily defendant could have discovered the child pornography sites Employee visited everyday on his work computer. Griesler testified that defendant's network maintained log files by date. Each daily file identified all websites accessed on each particular day. By entering a code, Griesler could have isolated all of Employee's websites visited for any given day for months and could have opened

them. Of course, another way to have monitored websites Employee visited, at least recently, would have been to simply open his computer and click on "websites visited," which is what Russinoff did in March 2001.

Defendant recognized its right to monitor employee website activity and e-mails by promulgating and distributing a policy to that effect during the relevant time period. Specifically, the policy made clear that e-mails were the property of defendant and were not confidential. According to that policy, anyone who became aware of the misuse of the Internet for other than business reasons was to report it to Personnel.

II

Plaintiff's complaint, filed February 6, 2004, was in two counts. The first count alleged, in part, that:

> 15. XYC Corp. knew or should have known that Employee was using its computer and internet at his workstation to view and download child pornography and to interact with child pornography web sites.
> 16. Given the nature of the offense, XYC Corp. had a duty to report Employee to the proper authorities for the crimes committed on its property during the course of the work day.
> 17. XYC Corp. negligently, carelessly, with reckless indifference and or intentionally breached its aforesaid duty.
> 18. As a direct and proximate cause of XYC Corp.'s breach of duty, Employee was able to continue clandestinely photographing and molesting Jill Doe resulting in Jill Doe suffering severe and permanent harm.

In the second count, Jane sought damages for money she had expended for Jill's care and treatment as a proximate result of defendant's breach of duty, as alleged in count one.

III

In granting summary judgment, the motion judge, in a detailed oral opinion covering thirty pages of transcript, correctly focused on the critical issue as being "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," citing *Restatement (Second) of Torts* § 328B (1965). The judge went on to note *Restatement*, *supra,* § 314 ("The fact that the 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") and § 317, which we consider most relevant to the issues under review:

> 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.

The judge concluded that Employee's "conduct at home" was not under defendant's control, specifically referencing "the molestation of [Jill]." He continued, again referring to § 317, finding that it did "not appear that [Employee's] conduct at work was dangerous to others and [defendant] did not have direct knowledge or indirect knowledge of this misconduct until a report was made by [his] co-employees." Restating the issue as "whether [defendant] used reasonable care," the judge determined that defendant,

> acted as a reasonably prudent corporation. The corporation exercised the foresight, prudence and control that a reasonably prudent company would have under the similar circumstances. Upon receipt of complaints from [its] employees, defendant instructed the [Employee] to stop [his] conduct.

> Because there is no evidence that they were aware that the employee was viewing child pornography, and under *Blakey [v. Cont'l Airlines, Inc.*, 164 *N.J.* 38, 751 *A.*2d 538 (2000)] there is [no] duty to monitor private communications of [its] employees, this court finds that there has been no breach of a duty and no negligence on the part of the defendant corporation as a matter of law.

Further, the judge found that defendant had no duty to investigate the private communications of its employees. Finally, he found an absence of proximate cause, in that using ordinary care defendant could not have foreseen the ultimate harm, "that result being molestation of the child at home.... Terminating the employee would not have resulted ... in protecting the [minor] plaintiff." He continued:

> The harm to the plaintiff did not occur at the defendant's premises. It did not involve a chattel belonging to the defendant. The harm caused by the employee was inflicted at the plaintiff's home outside of the defendant's control during non-working hours by the errant employee.
> ....
> The duty to monitor employee's internet activities does not exist. In this case the defendant reprimanded the plaintiff and pursuant to its own company policy could have fired the employee for using the internet for nonbusiness related purposes. That action in the employer's view would have been the most drastic penalty it could have imposed. The company saw fit not to terminate but rather to reprimand. Termination of the employee, the most drastic measure under the existing policy, would not have protected the plaintiff from the injury alleged in the plaintiff's complaint: the clandestine photographing and

molestation of the plaintiff at her residence.

> There is no way that this Court can conclude that this corporate defendant in any way could have controlled and/or in any way protected the plaintiff from that injury. Jane Doe married the employee on October 28, 2000. He was arrested June 21, 2001. On June 15th, 2001, he transmitted three photos that he had clandestinely taken of the minor stepchild on the internet on his workplace computer to a child porn site to gain access to the site. In March of 2001 the employee was advised to stop viewing inappropriate sites at work. It is unclear of the exact date that the employer--the employee began viewing pornography at work, although it appears to have been sometime in 2000. Even if this Court were to conclude that the defendant owed a duty to the plaintiff, the plaintiff has failed to demonstrate in any fashion in light of the dates presented, in light of the clandestine photography taking place in the employee's home, how any failure to take action by the company could demonstrate that that breach caused the injuries to plaintiffs' suffer. This Court finds that the employer has not breached a duty, was not negligent, did not act in an unforeseeable fashion and did not actually or proximately in any way, cause the injuries to which the plaintiffs complain.

IV

On appeal plaintiff argues that defendant had "the right and the ability to monitor Employee's Internet, knew or should have known of his interaction with child porn sites, had a duty to report him to the authorities and its failure to do so renders it liable to plaintiffs." We agree in large part with plaintiff's arguments but not with the final leap to defendant's liability.

At the outset, we note our consternation over a significant procedural defect in plaintiff's case. Plaintiff takes the motion judge to task for having "mistakenly focused on the conduct of Employee at home in taking the nude photos, over which the Court concluded [defendant] had no duty to control. The focus, however, should have been on Employee's use of [defendant's] chattel, i.e., its computer network, to transmit [Jill's] photos on the Internet, over which it did have control."

It is true that the motion judge did focus on the Employee's conduct at home in taking the photographs of his stepdaughter. However, the reason for that focus, now claimed to be mistaken, rests at plaintiff's own doorstep. While the complaint did allege that defendant breached "a duty to report Employee to the proper authorities for the crimes committed on its property during the course of the work day," it continued by alleging that the proximate cause of defendant's breach of duty was that Employee "was able to continue clandestinely photographing and molesting Jill Doe...." Thus, the judge's focus was precisely that of plaintiff herself.

When the summary judgment motion was argued plaintiff's counsel asserted that "part of" his damage claim was for the transmission of Jill's photos over the Internet. As we have seen, that was clearly not the case. Defense counsel, however, did not challenge that assertion but simply argued the absence of proximate cause between any breach of duty on the part of defendant and

Employee's conduct at home. On appeal defendant still does not contend that plaintiff's present theory, the Internet transmission of the photos, constitutes a marked deviation from the complaint. Defendant argues only that plaintiff has waived any argument that defendant is liable for Employee's conduct in photographing and molesting Jill at home, by virtue of having failed to advance that claim in her appellate brief. In her reply brief plaintiff does argue that a "factual issue existed as to whether it was foreseeable, given Employee's conduct, that he would attempt to obtain photos of his stepdaughter, or other children, to transmit on the internet." Despite this ambiguous assertion, we conclude that plaintiff has limited her claim to Employee's conduct in transmitting the photos, the only conduct which took place at work.

Since defendant has not argued, before the motion judge or on appeal, that plaintiff's claim based on that workplace activity was not pled in the complaint, and since the issues raised are of considerable importance, we will address the merits. Nevertheless, as we have noted, plaintiff's criticism of the motion judge for analyzing the case based on the allegations in her complaint, is manifestly unfair and unfounded.

V

In analyzing plaintiff's claim, the following issues must be addressed: (1) whether defendant had the ability to monitor Employee's use of the Internet on his office computer; (2) assuming defendant had the ability to do so, whether it had the right to monitor Employee's activities; (3) whether defendant knew, or should have known, that Employee was using the office computer to access child pornography; (4) whether defendant had a duty to act to prevent Employee from continuing his activities; and (5) whether any failure to act on the part of defendant proximately caused harm to Jill. We discuss each question in turn.

A. DEFENDANT'S ABILITY TO MONITOR EMPLOYEE'S INTERNET ACCESS ON HIS WORK COMPUTER.

The first question is readily answered in the affirmative. 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. Griesler, defendant's Network Administrator, testified that he was able to use the network's daily log system to isolate and identify pornographic websites visited by Employee. However, he did not open any specific sites and, after reporting his findings to his supervisor, was instructed not to investigate Employee's Internet usage again. Further, Russinoff, Employee's immediate supervisor, opened Employee's computer while he was at lunch and clicked on "websites visited." Here again, none of the sites identified were actually explored and no further action was taken to determine the nature of Employee's pornographic related computer activities. Instead, Russinoff was simply instructed to tell Employee to stop whatever he was doing.

Thus, defendant's capability to monitor Employee's activities on his work computer was clearly

established.

B. DEFENDANT'S RIGHT TO MONITOR EMPLOYEE'S ACTIVITIES ON HIS OFFICE COMPUTER.

Defendant argued, and the motion judge agreed, that Employee's privacy interest trumped defendant's right to monitor his computer use at work. We disagree.

We begin by addressing whether, as defendant claims, *Blakey v. Cont'l Airlines, Inc.*, 164 *N.J.* 38, 751 *A.*2d 538 (2000), is dispositive of this issue. That case involved a sexual discrimination/hostile work environment claim by Blakey, a female pilot for Continental. In part, Blakey contended that "a number of Continental's male pilots posted derogatory and insulting remarks about Blakey on the pilots' on-line computer bulletin board called The Crew Members Forum (Forum). The Forum is accessible to all Continental pilots and new members through the Internet Provider, CompuServe." *Id.* at 48, 751 *A.*2d 538. In remanding the case, the Court instructed the trial court to "first determine whether Continental derived a substantial workplace benefit from the overall relationship among CompuServe, the Forum and Continental." *Id.* at 60, 751 *A.*2d 538. This was necessary for determining whether the Forum "should be considered sufficiently integrated with the workplace to require," *id.* at 61, 751 *A.*2d 538, the employer to respond to "the posting of offensive messages on company ... e-mail systems when the employer is made aware of those messages." *Ibid.* It was in that connection that the Court made the following observation, relied on by defendant: "Business counselors caution employers that they should have policies that deal with sexual harassment on the message centers of this changing world. *That does not mean that employees have a duty to monitor employees' mail.* Grave privacy concerns are implicated." *Ibid.* (citations omitted) (emphasis supplied). The Court wrote:

> To repeat, employers do not have a duty to monitor private communications of their employees; employers do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace and in settings that are related to the workplace.
> [*Id.* at 62, 751 *A.*2d 538.]

Clearly, *Blakey* does not answer the question posed in this case, which does not involve "private communications" of Employee.

To begin, this is not a criminal case in which the State seeks to use evidence obtained through a search of his workplace computer against Employee. *See United States v. Angevine*, 281 *F.*3d 1130 (10th Cir.) (no Fourth Amendment right to suppress evidence of child pornography located on erased files of professor's workplace computer which was part of university network), *cert. denied*, 537 *U.S.* 845, 123 *S.Ct.* 182, 154 *L.Ed.*2d 71 (2002); *United States v. Simons*, 206 *F.*3d 392, 398 (4th Cir.2000) (employee had no legitimate expectation of privacy in contents of his workplace computer where employer had notified employees that their computer activities could be monitored), *cert. denied*, 534 *U.S.* 930, 122 *S.Ct.* 292, 151 *L. Ed.*2d 216 (2001); *United States v. Bailey*, 272 *F.Supp.*2d 822 (D.Neb.2003) (same). In the present case, we deal with whether

defendant employer could monitor Employee's use of his workplace computer in the context of civil litigation brought by a third-party claiming injury resulting from those computer activities. On this question, we have found no authorities directly on point. In *Biby v. Bd. of Regents of the Univ. of Nebraska,* 419 *F.*3d 845 (8th Cir.2005), Biby was terminated by the University based on information obtained in a search of his workplace computer files. *Id.* at 849. The University computer policy stated that computer files would be searched only if a legitimate reason existed, such as investigation of improper or illegal use of resources. *Id.* at 848. Biby sued the University, raising a number of theories, including a claim under 42 *U.S.C.* § 1983 based upon violation of his Fourth Amendment right to privacy. Specifically, he claimed that "he had a constitutionally protected privacy interest in his work computer, that the university's reasons for searching his computer were illegitimate, and that the scope of the search was unreasonable." *Id.* at 850. The district court granted summary judgment dismissing Biby's claim and the circuit court affirmed. Applying the standards set out in *O'Connor v. Ortega,* 480 *U.S.* 709, 107 *S.Ct.* 1492, 94 *L.Ed.*2d 714 (1987), also a § 1983 case, the court found no legitimate expectation of privacy by Biby in his computer files. In doing so, the court emphasized the existence of the university's workplace privacy policy, *id.* at 850-51, one of the facts which *O'Connor* deemed relevant in determining the reasonableness of an employee's expectation of privacy. *O'Connor, supra,* 480 *U.S.* at 723, 107 *S.Ct.* at 1498, 94 *L.Ed.*2d at 717. While those decisions do not apply directly to the question posed here, they do offer some guidance.

In this case, defendant had an e-mail policy which stated that "all messages composed, sent or received on the e-mail system are and remain the property of the [defendant]. They are not the private property of any employee." Further, defendant reserved the "right to review, audit, access and disclose all messages created, received or sent over the e-mail system as deemed necessary by and at the sole discretion of [defendant]." Concerning the internet, the policy stated that employees were permitted to "access sites, which are of a business nature only" and provided that:

> Any employees who discover a violation of this policy shall notify personnel. Any employee who violates this policy or uses the electronic mail or Internet system for improper purposes shall be subject to discipline, up to and including discharge.

The written e-mail policy contained an acknowledgement page to be signed by each employee. While the record does not contain a copy of such acknowledgement signed by Employee, there is no suggestion that he was not aware of the company policy. In addition, as we have noted, Employee's office, as with others in the same area, did not have a door and his computer screen was visible from the hallway, unless he took affirmative action to block it. Under those circumstances, we readily conclude that Employee had no legitimate expectation of privacy that would prevent his employer from accessing his computer to determine if he was using it to view adult or child pornography. As a result, we turn to whether defendant had reason to investigate Employee's use of his computer.

C. INFORMATION KNOWN OR ATTRIBUTABLE TO DEFENDANT CONCERNING EMPLOYEE'S PORNOGRAPHY ACTIVITIES.

We see no need to repeat the facts set out earlier in this opinion. Assessing those facts and the

reasonable inferences to be drawn from them, as we must in the summary judgment context, we conclude that defendant, through its supervisory/management personnel, was on notice that Employee was viewing pornography on his computer and, indeed, that this included child pornography. Knowledge includes "implied" knowledge, which "means knowledge based on other known facts that would inform a reasonably prudent person of the ultimate fact." *Black v. Pub. Serv. Elec. & Gas Co.*, 98 *N.J.Super.* 366, 375, 237 *A.*2d 495 (App.Div.1968). Such was the case here. Based on the company's policy, quoted above, such computer use was certainly not "of a business nature" but was, rather, "for improper purposes." That same policy required that violations be reported to personnel. We can reasonably assume that such reporting was not simply intended as an idle gesture but was intended to trigger an investigation so that it could be determined if, according to the policy, the offending employee needed to be disciplined. While defendant asserted that in 1999 a policy had been instituted and communicated to certain management personnel by O'Connor, that "no employee should monitor any other employee's computer use just for the sake of monitoring," and that an employee who did so could be terminated, the monitoring of Employee's computer could not, on the facts presented, have been considered "just for the sake of monitoring." Here, the reports of improper computer use by Employee were not merely gossip, but based on credible, first-hand information. Indeed, it is inexplicable why such a policy was deemed applicable to several reports, such as that of Griesler to Carroll in early 2000 based on his review of computer logs which showed visits to pornographic sites such as "Sextracker." Thus, defendant was on notice of Employee's activities and was under a duty to investigate further. Such an investigation would have readily uncovered the full scope of Employee's activities, as did the Prosecutor's Office when it searched his computer on June 19, 2001. We impute to defendant knowledge that Employee was using his work computer to access pornography.

D. DID DEFENDANT HAVE A DUTY TO PREVENT EMPLOYEE FROM CONTINUING HIS ACTIVITIES?

With 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." *Hopkins v. Fox & Lazo Realtors,* 132 *N.J.* 426, 439, 625 *A.*2d 1110 (1993) (citing *Kelly v. Gwinnell,* 96 *N.J.* 538, 552, 476 *A.*2d 1219 (1984)). The Court continued:

> Whether a person owes duty of reasonable care toward another turns on whether the imposition of such a duty satisfies an abiding sense of basic fairness under all of the circumstances in light of considerations of public policy. *Goldberg v. Housing Auth.*, 38 *N.J.* at 578, 583, 186 *A.*2d 291 (1962). That inquiry involves identifying, weighing, and balancing several factors--the relationship of the parties, the nature of the attendant risk, the opportunity and ability to exercise care, and the public interest in the proposed solution. *Ibid.* The analysis is both very fact-specific and principled; it must lead to solutions that properly and fairly resolve the specific case and generate intelligible and sensible rules to govern future conduct.
> [*Ibid.*]

We begin by noting that it is a crime, both state and federal, to possess or view child pornography, *N.J.S.A.* 2C:24-4b(5)(b); 18 *U.S.C.A.* § 2252, § 2256(8)(B). [FN3] Given the public policy against child pornography, as reflected in these statutes, and the fact that "public policy favors the exposure of crime," *Higgins v. Pascack Valley Hosp.*, 158 *N.J.* 404, 423, 730 *A.*2d 327 (1999) (citing *Palmateer v. Int'l Harvester Co.*, 85 *Ill.*2d 124, 52 *Ill.Dec.* 13, 421 *N.E.*2d 876, 880 (1981)), we agree with plaintiff that defendant had a duty to report Employee's activities to the proper authorities and to take effective internal action to stop those activities, whether by termination or some less drastic remedy.

At this point, we return to the *Restatement, supra,* § 317. That section places upon a master, in this case defendant, the duty to control his servant, here Employee, while the servant is acting outside the scope of his employment, as in the present case, to prevent the servant from "intentionally harming others or from so conducting himself as to create an unreasonable risk of bodily harm to them." That type of duty finds support in our case law, *DiCosala v. Kay,* 91 *N.J.* 159, 172, 450 *A.*2d 508 (1982), and we discern no sound reason not to apply it here. Defendant was under a duty to exercise reasonable care to stop Employee's activities, specifically his viewing of child pornography, which by its very nature has 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. We reject defendant's argument that a "special relation" must exist between the master (in this case the employer) and the person who is likely to be harmed. Defendant's reliance on *Restatement, supra,* § 315 as support for that proposition is misplaced, at least in the present context. Indeed, § 315(a) supports plaintiff's position, not that of defendant. The section provides that "there is no duty to control the conduct of a third person as to prevent him from causing physical harm to another unless (a) a special relation exists between the actor and the third person which imposes a duty upon the actor to control the third person's conduct...." In this case, there is a special relation between defendant (the actor) and the third person (Employee), that being the master-servant (employer-employee) relation. It is for that reason that § 317 follows § 315 since the former explains the circumstances in which the master comes under a duty to control the servant's conduct.

Returning to § 317, all of the requirements for liability in that section are present here. The servant was "using a chattel of the master" and the master both "knows or has reason to know that he has the ability to control his servant" and "knows or should know of the necessity and opportunity for exercising such control." Under these circumstances, a risk of harm to others was "reasonably within the [master's] range of apprehension." *Clohesy v. Food Circus Supermkts.,* 149 *N.J.* 496, 503, 694 *A.*2d 1017 (1997) (quoting *Hill v. Yaskin,* 75 *N.J.* 139, 144, 380 *A.*2d 1107 (1977)).

For these reasons we are unable to agree with the motion judge's conclusion that defendant had no knowledge that Employee had "engaged in any conduct that would cause a person to have reasonable cause to believe that [Jill] had been subjected to child abuse or acts of child abuse." On the contrary, as we have explained, the record and reasonable inferences therefrom support the conclusion that defendant had knowledge that Employee was engaging in activities that posed the threat of harm to others, although not necessarily Jill. We see no unfairness in the imposition of a

duty on defendant in these circumstances. *Kuzmicz v. Ivy Hill Park Apts., Inc.*, 147 *N.J.* 510, 515, 688 *A.*2d 1018 (1997). Whether Employee's activities, which defendant had the means and duty to stop, were likely to have caused injury to Jill goes to proximate cause, an issue to which we now turn our attention.

E. DID DEFENDANT'S BREACH OF DUTY PROXIMATELY CAUSE HARM TO PLAINTIFF

In *Reynolds v. Gonzalez,* 172 *N.J.* 266, 284, 798 *A.*2d 67 (2002), the Court most recently summarized the applicable principles:

> One of the underlying principles of tort law is that "an actor's conduct must not only be tortious in character but it must also be a legal cause of the invasion of another's interest." *Restatement (Second) of Torts* § 9 cmt. a (1965) (*Restatement*). It follows from that principle that the issue of a defendant's liability cannot be presented to the jury simply because there is some evidence of negligence. "There must be evidence or reasonable inferences therefrom showing a proximate causal relation between defendant's negligence, if found by the jury," and the resulting injury. *Germann v. Matriss,* 55 *N.J.* 193, 205, 260 *A.*2d 825 (1970).

Similarly, *Prosser and Keeton on the Law of Torts* states that

> [t]he plaintiff must introduce evidence which affords a reasonable basis for the conclusion that it is more likely than not that the conduct of the defendant was a cause in fact of the result. A mere possibility of such causation is not enough; and when the matter remains one of pure speculation or conjecture, or the probabilities are at best evenly balanced, it becomes the duty of the court to direct a verdict for the defendant.
> [W. Page Keeton et. al., *Prosser & Keeton on the Law of Torts,* § 41, at 269 (5th ed. 1984) (*Prosser & Keeton*).]

Thus, absent "proof of cause, there is no connection between the injury complained of and the fault of anyone." J.D. Lee & Barry A. Lindahl, *Modern Tort Law: Liability and Litigation,* § 4.01, 127 (rev. ed. 2000).

In the present context, there are two distinct proximate cause-of-injury issues. First, whether defendant's breach of duty could be said to have resulted in the specific action of Employee which is claimed to have caused harm to Jill, that action being identified as the transmission of three images via e-mail on June 15, 2001. Thus, the inquiry becomes whether there were sufficient facts in the record from which a reasonable fact-finder could conclude that had defendant not breached its duty, no harm would have resulted. In other words, had defendant acted to stop the activities of Employee when it had, or reasonably should have had, sufficient information on which to act, could the harm to Jill have been averted? If so, then proximate cause has been established.

Viewed in a light favorable to plaintiff, defendant was on notice of Employee's pornographic

related computer activity by early 2000. By late March 2001, defendant had knowledge, through its supervisory personnel, that Employee had visited a variety of "porn sites" including one that suggested child pornography. Yet, despite being reported to high level management, no action was taken. A reasonable fact-finder could conclude that an appropriate investigation at that time would have revealed the extent of Employee's activities and, presumably, would have led to action to shut down those activities. It is true, as defendant contends, that Employee could still have possibly utilized a computer elsewhere, such as at home or at a library, to transmit Jill's photos. But that possibility does not negate proximate cause as a matter of law; it simply presents a contested issue for a jury. [FN4] *Arvanitis v. Hios*, 307 *N.J.Super.* 577, 585, 705 *A.*2d 355 (App.Div.1998). As Judge Conley said there:

> [f]oreseeability that relates to proximate cause (as distinguished from that relating to a duty of care) involves " 'the question of whether the specific act or omission of the defendant was such that the ultimate injury to the plaintiff' reasonably flowed from the defendant's breach of duty." (quoting *Clohesy, supra*, 149 *N.J.* at 503, 694 *A.*2d 1017 (quoting *Hill, supra*, 75 *N.J.* at 143, 380 *A.*2d 1107)).

Proximate cause questions are generally for the trier of fact. *Ibid.*

The second proximate cause question, however, cannot be resolved on the present record. Plaintiff must establish that Jill suffered some harm to her person as a result of the Internet transmission of her photos. Of course, that harm could be psychological in nature, but there must be a showing of some harm proximately caused by defendant's breach of duty. Perhaps because the arguments before the motion court were focused on liability, little, if anything, was said about damages. As a result, we remand the matter to the Law Division at which time the issue of proximately caused harm may be addressed within the summary judgment context. Although we have rejected most of defendant's arguments concerning its potential liability, we do not foreclose the possibility that summary judgment may yet be granted.

Reversed and remanded. We do not retain jurisdiction.

FN1. The facts are drawn primarily from the depositions of the various witnesses.

FN2. We infer that Employee was terminated on June 19, 2001 after the search, although this fact is not found in the record.

FN3. The Protection of Children From Sexual Predators Act of 1998 (PCFSPA), requires electronic communication service providers to report suspected violations of 18 *U.S.C.A.* § 2252, and subjects the provider to sanctions for a knowing or willful failure to report. 42 *U.S.C.A.* § 13032(b)(3). We do not decide whether defendant was an electronic communications server. 42 *U.S.C.A.* § 13032(a)(1); 18 *U.S.C.A.* § 2510(15).

FN4. In his statement to the Prosecutor's Office, defendant stated that he only viewed pornography on his work computer.