PROSKAUER ROSE LLP®

Client Alert

A report for clients and friends of the firm

January 2006

Failure to Investigate Employee's Use of Computer to View Child Pornography and to Report Him to Authorities May Result in Liability to Third Parties

The New Jersey Appellate Division recently indicated that employers should become proactive in enforcing corporate policies that prohibit improper Internet access or computer usage. In *Doe v. XYC Corp.*, 2005 WL 3527015 (App. Div. Dec. 27, 2005), the court held that an employer on notice of an employee's use of a workplace computer for an illegal purpose — to access child pornography — has an affirmative 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 third parties." 2005 WL 3527015 at *1. The Court stated that merely telling the employee to stop such activity is insufficient because child pornography poses a threat to children. According to the Court, an employer who uncovers evidence that an employee is engaging in such activity has a duty to report it to the authorities and to take strong measures to stop it, including discipline or termination.

Like many companies, the defendant employer in *Doe* maintained a policy that restricted its employees' computer use to business purposes; reserved broad power to monitor and review e-mail and track Internet usage; made clear that e-mails were the property of the employer with no expectation of privacy; and authorized disciplinary measures if the policy was violated. Further, employees were required to report violations of the policy.

As early as 1998 or 1999, the employer's information technology ("IT") personnel had become aware that "Employee" was visiting pornographic websites. They told him to stop, but did not report it to their supervisors. In early 2000, the Employee's supervisor learned that Employee was viewing pornography at work, but only a limited review of computer logs was conducted at that time, apparently because of privacy concerns, and no action was taken against Employee. In December of 2000, two female employees complained that Employee was accessing pornography. Two months later, an IT Director saw evidence that Employee had been visiting such websites. She did not open the sites to investigate the precise nature of Employee's activities, however. Again, no action was taken.

Finally, in March 2001, one of the female employees who had previously complained raised it again with Employee's supervisor. The supervisor checked Employee's computer for websites recently visited, which, from the names of the sites, obviously were pornographic. The Court took particular note that the name of one of the websites "suggested" it might display child pornography. *Id.* at *12. The supervisor told Employee that there had been reports of his improper computer usage and that it must stop. No detailed investigation of the Employee's computer activities was conducted, however, and no formal disciplinary action was taken. Three months later, the supervisor saw that Employee once again was visiting pornographic websites, but did nothing.

Shortly thereafter, Employee was arrested after nude photos of his minor stepdaughter were found in a dumpster at the employer's headquarters. Searches of his work computer revealed he had used it to transmit the pictures that he had secretly taken of his stepdaughter, as well as for storing pornographic photos of other children, and to visit websites and interact with others trafficking in child pornography

activities. The minor child's mother filed suit on her daughter's behalf alleging, among other things, that the employer breached its "duty to report the employee to the proper authorities for the crimes committed on its property during the course of the work day" and sought to hold the company directly responsible for harm to the daughter. *Id.* at *4. Although the trial court dismissed the claims, the appellate court reversed.

The Four-Part Test For An Employer's Duty To Take Action

The Appellate Division established a four-part test which, if satisfied, will confer a duty of reasonable care upon an employer to stop the intentional criminal conduct of an employee. To satisfy this new standard, a plaintiff must prove that the employer: (1) has the ability to monitor its employees' Internet access; (2) has the right to monitor its employees' computer usage; (3) has actual or implied notice of its employee's criminal activity; and (4) has an affirmative duty to stop the employee's continuing criminal activity.

The first two elements are relatively simple to establish. Nearly every employer has the technological ability to monitor its employees' Internet access because, according to the court, "monitoring" can be as simple as a search of the employee's computer in the employee's absence to check the history of websites recently visited. The employer here also had a network log system that could identify websites visited and software is generally available for monitoring employee usage, as well. The second element is also readily met because an employee has no expectation of privacy in his e-mail or Internet usage as a matter of law when his employer maintains a written policy prohibiting computer misuse and reserves the right to monitor e-mail usage and Internet access. *Id.* at *8-9.

Information "Known Or Attributable" To The Employer

The third element focuses on whether the employer "knew, or should have known" that an employee is using an office computer for an illegal purpose, in this case to access child pornography. *Id.* at *6. The employer's "knowledge" will be broadly construed to include implied knowledge, based upon all of the "known facts that would inform a reasonably prudent person." *Id.* at *9. The Court concluded that upon receiving reports of improper computer usage, the employer had sufficient notice of possible illicit conduct, such that it was under a duty to investigate further. As the Court stated, "[w]e can reasonably assume that such reporting was not simply intended as an idle gesture but was intended to trigger an investigation" to determine whether an offending employee needed to be disciplined. The Court concluded that such an investigation would have revealed the "full scope" of Employee's child pornography activities. Thus, the Court imputed knowledge of those activities to the employer, even though it never conducted that investigation and did not have that information.

The Duty To Prevent An Employee's Continuing Illegal Conduct

Most significant, the fourth element of the test sets out the employer's duty to act affirmatively to prevent an employee from continuing his illegal activities. The Court noted the general duty of an employer to control and prevent its employee from harming others. Child pornography "by its very nature" constitutes a threat to "others" - the children who are the subject of such activities. *Id.* at *10. In these circumstances, the Court concluded, the potential risk of harm to others reasonably should have been foreseeable by the employer. Due to the unquestionably illegal nature of the possession or viewing of child pornography and the harm it inflicts on children, the Court concluded that the employer "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." *Id.* at *10. Although this kind of conduct is outside the scope of employment, the employer still has a duty to act where the activity occurs either on the employer's premises or by use of its property (in this case, a computer). *Id.* at *4. The case was remanded to the trial court for a determination of whether the employer's failure to act was the proximate cause of harm to the plaintiff.

EDITORS' COMMENT:

The *Doe* decision imposes a new, affirmative obligation on New Jersey employers with actual or implied knowledge that an employee has committed or is threatening to commit a crime in the workplace, especially where harm to others is a possibility. In the wake of *Doe*, employers should be particularly vigilant to insure that policies prohibiting improper computer usage and Internet access are implemented and that those policies are distributed, explained and diligently enforced. Reported instances of computer misuse or abuse should be thoroughly investigated to make sure that the extent of the inappropriate activity is uncovered, especially if there is any hint of unlawful activity. Where appropriate, legal authorities should be notified and effective internal measures employed to stop illegal computer activity in the workplace.

New Jersey employers should also recognize that a far wider range of offensive or improper, but not criminal, activity in the workplace may warrant the same diligence. An employer's implied knowledge that an employee is accessing or disseminating hate speech or harassing a member of a

protected class through his workplace computer could likewise trigger an affirmative obligation to investigate the activities of the employee and take prompt, reasonable action to stop the offensive conduct, whether or not there has been a complaint.

Lastly, it should be noted that despite policies informing employees that they have no expectation of privacy as to e-mails and Internet use, employers should be sensitive to the private nature of any personal information that may happen to be revealed in monitoring computer use, such as medical information, and take care to keep such information confidential.

Proskauer's Newark office has 40 attorneys with significant and diverse experience in labor, employment, employee benefits and immigration law. The following individuals serve as contact persons for this alert and would welcome any questions that you might have. For more information on this matter, please contact:

Edward Cerasia II
973.274.3224 – ecerasia@proskauer.com

Wanda L. Ellert
973.274.3285 – wellert@proskauer.com

Mark A. Saloman
973.274.6038 – msaloman@proskauer.com

We would like to thank Jason Schatz for his assistance in the preparation of this alert.