

# CLIENT ALERT

## Employment & Labor

January 2006

Volume VII No. 9

### Employer's Duty to Stop Workplace Surfing of Internet Porn

The Internet has quickly become an indispensable tool of modern commerce. Employers should be aware, however, that this new technology brings with it unexpected risks and potential liability. This point was highlighted recently by the New Jersey Appellate Division's *Doe v. XYZ Corporation* decision, in which the Court held that an employer has a duty, under certain circumstances, to investigate and stop an employee's unauthorized use of a work computer to access child pornography.

#### The Parties

The defendant, "XYZ Corporation," employed 250 employees at its headquarters, including an accountant identified in the decision only as "Employee." Employee worked at a cubicle that opened into a hallway. The plaintiffs were "Jane" and "Jill Doe," Employee's wife and stepdaughter, respectively.

#### Employee's Conduct At Work

In 1998 or 1999, XYZ's Information Technology ("IT") personnel discovered that Employee had visited pornographic Internet websites. They told Employee to stop, but did not inform his supervisors.

In early 2000, Keith Russinoff, Employee's supervisor, discovered that Employee was visiting inappropriate websites. IT reviewed computer logs and identified websites that Employee had visited, including bestiality and necrophilia sites. IT reported the findings to Russinoff and Jessica Carroll, XYZ's Director of Network and PC Services, but no further action was taken.

In December 2000, an employee and her manager suspected that Employee was viewing pornography, because he frequently shielded his computer monitor to prevent others from seeing what he was doing. The

manager reported the matter to Suzanne Colon, Manager of Financial Reporting, but no action was taken.

In February 2001, Carroll reviewed a list of websites that Employee had visited and concluded that they were pornographic, but did not take any action. Subsequently, after an employee saw a bikini-clad woman on Employee's monitor and Russinoff saw Employee blocking his screen, Russinoff entered Employee's cubicle when Employee was at lunch, and printed out a partial list of "websites visited," which included the names of porn sites and a site regarding children: "Teenflirts.org."

After consulting with his superiors, Russinoff told Employee, on March 6, 2001, that there had been reports of his inappropriate use of the computer. Employee agreed to stop but Russinoff later discovered that Employee had resumed his misconduct. Russinoff took no action. On June 21, 2001, Employee was arrested on child pornography charges.

#### Employee's Conduct Regarding Jill

For approximately five months before his arrest, Employee secretly took nude and semi-nude photographs and video of his ten-year-old stepdaughter, "Jill." On June 15, 2001, in order to gain access to a child porn website, Employee transmitted Jill's photos from his workplace computer to the site. After photographs of Jill were discovered in a dumpster at XYZ, police searched his work space and computer. Employee's e-mails to pornographic websites and interactions with other individuals regarding child pornography were discovered. Employee later acknowledged storing child pornography, including nude photos of Jill, on his work computer.

#### XYZ's E-Mail And Internet Policy

XYZ's e-mail and Internet policy stated that e-mails were the property of XYZ and were not confidential. The policy also stated that

Sills Cummis Epstein & Gross

A Professional Corporation

employees were permitted to access Internet websites “of a business nature only.” An employee who became aware of a violation of the policy was required to report it to the Personnel Department.

### The Lawsuit

Jill’s mother sued XYZ, on her daughter’s behalf, for breaching its duty to report the crimes that Employee was committing on its computer. She initially argued that XYZ was liable for harm Jill suffered as a result of Employee’s clandestinely photographing – and thereby molesting – her at home, but subsequently argued that XYZ was liable for harm Jill suffered as a result of Employee’s transmission of her nude and semi-nude photos via the Internet. The trial court granted XYZ’s Summary Judgment Motion.

### The Appellate Division

On appeal, the Appellate Division considered several issues. First, the Court considered whether XYZ had the ability to monitor Employee’s use of the Internet on his office computer. The Court concluded that Employer had the technical ability to do so.

Second, the Court considered whether XYZ had the right to monitor Employee’s Internet activities. In light of XYZ’s e-mail and Internet policy, and the fact that his computer screen was visible from the hallway,

the Court concluded 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.” Therefore, XYZ had the right to monitor Employee’s Internet activities.

Third, the Court considered whether XYZ knew or should have known that Employee was using its computer to access child pornography. The Court explained that, pursuant to XYZ’s policy, Employee’s misuse of the Internet was reported and should have triggered an investigation, which would have revealed the “full scope” of his activities. Accordingly, the Court imputed to XYZ knowledge that “Employee was viewing pornography on his computer and, indeed, that this included child pornography.”

Fourth, the Court considered whether XYZ had a duty to act, either by terminating his employment or notifying law enforcement, to prevent Employee from continuing his activities. The Court found that Employee was using XYZ’s property to engage in criminal conduct, XYZ knew that it had the ability to control Employee, and knew or should have known of the necessity of doing so. Therefore, XYZ had “a duty to exercise reasonable care to stop

Employee’s activities, specifically his viewing of child pornography.”

Fifth, the Court considered whether XYZ’s failure to act proximately caused harm to Jill. According to the Court, a jury could reasonably find that, had XYZ conducted a prompt investigation, it would have discovered and stopped Employee before his June 15, 2001 transmission of Jill’s photos. The Court explained, however, that there was insufficient evidence to establish that plaintiffs suffered damages as a result of the transmission. Therefore, the Court remanded the case to the trial court to address this issue.

### Conclusion

While some may view the *Doe v. XYZ Corporation* decision as a narrow ruling based upon unique facts, prudent employers recognize the crucial, broadly-applicable lesson that it teaches. Specifically, in addition to simply issuing policies on e-mail and Internet usage, *employers must consistently enforce those policies pursuant to carefully established, standard protocols and procedures.* This lesson applies equally to policies on harassment, Sarbanes-Oxley whistle blowing, and other areas. As XYZ learned, not enforcing a policy may be as risky as not having one at all.

*We send these Alerts to our clients and friends to provide information on recent developments in the law. The Alerts, however, should not be relied on for legal advice in any particular matter.*

### NEW JERSEY IDENTITY THEFT PREVENTION ACT

Effective January 1, 2006, New Jersey’s Identity Theft Prevention Act creates new safeguards against identity theft. It allows consumers to request a security freeze on their credit report; affirms the right to file and receive a copy of a police report concerning suspected identity theft; requires any company that collects and maintains computer records containing consumers’ personal information to notify affected consumers if the data is compromised; limits use of a consumer’s social security number and prohibits display and use of a number except as required by law; and requires businesses to destroy records containing personal information that is no longer needed. For companies that obtain employee background checks pursuant to the Fair Credit Reporting Act, an additional notice is now required entitled “New Jersey Consumers Have The Right To Obtain A Security Freeze.” Please contact us if you would like to receive a copy of this notice or have questions regarding the new law.

For further information,  
please contact:

David W. Garland, Co-Chair  
Employment & Labor  
973.643.6390  
[dgarland@sillscummis.com](mailto:dgarland@sillscummis.com)

Lester Aron, Co-Chair  
Employment & Labor  
973.643.5795  
[laron@sillscummis.com](mailto:laron@sillscummis.com)

### New Jersey

One Riverfront Plaza  
Newark, NJ 07102  
Tel: 973-643-7000  
Fax: 973-643-6500

[www.sillscummis.com](http://www.sillscummis.com)

### New York

30 Rockefeller Plaza  
New York, NY 10112  
Tel: 212-643-7000  
Fax: 212-643-6500