ASAP™
A Littler Mendelson **Time Sensitive** Newsletter

in this issue:

FEBRUARY 2006

In a ground-breaking decision, the New Jersey Court of Appeals holds that an employer's failure to detect and stop an employee's unlawful activity using corporate e-mail and Internet resources can support a negligence claim against the employer by the victims of the employee's unlawful conduct.

Prohibiting Porn in Your Workplace Is Not Enough: New Jersey Court of Appeals Imposes New Duties on Employers Who Engage in Electronic Monitoring

By Philip L. Gordon, Esq. and John Julius, Esq.

In a precedent-setting decision, the New Jersey Court of Appeals held on the eve of 2006 that employers have a duty to uncover and stop an employee's use of corporate electronic resources for child-porn activities once the employer knows, or should know, that an employee is accessing *adult* pornography. If followed in other jurisdictions, this case, *Doe v. XYC Corp.*, No. A-2909-04T2 (N.J. Super. Ct. Dec. 27, 2005), could provide the basis for a whole new genre of employment litigation that seeks to hold employers responsible for the damages to victims of crimes committed by employees using corporate electronic resources. At a minimum, the case provides an important reminder that an employer who is put on notice that its employees are utilizing the company's electronic resources for nonbusiness purposes should take steps to ensure that the use does not include accessing pornography, or worse.

XYC Had Notice of Porn Surfing But Failed to Act

The plaintiff in the XYC case alleged that an XYC employee (the "Employee") who was her ex-husband and the stepfather of her ten-year old daughter had molested her daughter at home, taken pictures of the child partially clad and naked, and transmitted those photographs to child pornography websites using XYC's computer resources. Rather than suing her ex-husband, the alleged criminal, plaintiff claimed that XYC was negligent for failing to uncover and stop the Employee's activities and, therefore, XYC should be held liable for harm to the child resulting from Employee's unlawful conduct.

Between 1999 and Employee's arrest in June 2001, XYC was on notice that Employee was viewing adult pornography. IT personnel reviewing computer logs noted that Employee accessed URLs which suggested adult pornographic sites. A coworker complained to her supervisor that Employee, who worked in a cubicle that was open to public view, often blocked or minimized his computer screen when the co-worker approached. XYC's Director of Network and Personal Computing Services observed URLs, reflecting adult pornographic sites, stored in the browser on Employee's desktop. Employee's direct supervisor made the same observation and also noted that one of the sites was called "Teenflirts.org: The Original Non-nude Teen Index."

Despite these observations, no one at XYC visited any of the apparently pornographic websites to check their content. No one at XYC used the monitoring software that the company possessed to more closely examine Employee's web surfing activities. While XYC did reprimand the employee

on two occasions, the company took no further disciplinary action after the Employee appeared to stop his porn-viewing activities.

The Court of Appeals' Reasoning

The court of appeals found that XYC, "through its supervisory/management personnel, was on notice that Employee was viewing pornography on his computer and, indeed, that this included child pornography." Given that possession of child pornography is a felony under federal and New Jersey law, the court had little difficulty reaching the conclusion that XYC's management could not turn a blind eye to Employee's conduct. Instead, the court ruled, XYC had a duty to investigate further, to report Employee's activities to the appropriate law enforcement authorities, and to take effective internal action to stop those activities.

The court of appeals rejected XYC's assertion that its respect for Employee's privacy rights justified its failure to investigate further. In reaching this conclusion, the court relied heavily on XYC's electronic resources policy, which stated that all e-mail created using the company's computer system were XYC's property, that they were not private, and that XYC reserved the right to review, audit and access the e-mail. The court also noted that the policy restricted Internet access to business purposes only and required employees to report improper uses of the Internet to the personnel department. Putting aside the policy, the court also found that Employee had no privacy interest in his e-mail and Internet activity because his cubicle did not have a door and was openly visible from a hallway.

The court of appeals also rejected XYC's argument that the company could not be held responsible for the Employee's viewing of child pornography because that conduct was outside the scope of his employment. The court invoked the rule that an employer can be held responsible for damages caused by an employee's criminal conduct when the employee engages in the conduct on the employer's premises, using the employer's equipment, and the employer has the ability to control the conduct and knows or should know that there is a reason for exercising such control. The facts of the XYC case fell squarely within this four-part test.

Implications of the XYC Case for Employers

Read broadly, the court of appeals' decision, if followed in other jurisdictions, opens the door to a whole new genre of litigation holding employers responsible for damages arising from the criminal conduct of their employees. Only one element of the four-part test can even be disputed when an employee engages in criminal conduct using his employer's electronic resources, i.e., whether the employer knew, or should have known, of the need to stop the conduct. However, many employers will face difficulty defeating this element.

According to a 2005 survey of the American Management Association, 80% of employers monitor their employees' e-mail and Internet use. As the XYC case itself reflects, even the most minimalist monitoring — checking URLs listed on computer logs or in the history folder of an employee's desktop browser — could generate sufficient information to be considered notice to the employer of the need to exercise control over the employee's use of its computer resources.

The court of appeals' opinion is particularly troubling for employers because the decision strongly suggests that *lawful* conduct can constitute sufficient notice of an employer's need to act. In concluding that XYC had sufficient notice of Employee's activities to impose a duty on XYC to act, the court of appeals relied almost exclusively on Employee's lawful (albeit inappropriate) viewing of *adult* pornography. Only one of the many pornographic websites visited by Employee possibly suggested child pornography and that website was ambiguous, referring to teens (possibly eighteen and nineteen year olds to avoid child pornography laws) and "non-nude" photographs. Viewed from this perspective, the XYC case arguably provides a foundation for a lawsuit against an employer by the victims of a terrorist attack if the employer's monitoring software reveals that an employee used corporate electronic resources to access a website containing bomb-making instructions. As another example, an employer could be held responsible when an employee uses its electronic resources to engage in online shopping using someone else's identity. The case might even provide legal precedent for imposing liability on employers whose employees download copyrighted songs or videos, if management is aware that the employee visited file-sharing sites or blogs, potentially extending to situations where such material is received via e-mail.

While the XYC case does not expressly impose on employers a duty to monitor their employees' e-mail and Internet traffic, the case strongly suggests that the large majority of employers who do monitor e-mail and Internet use must actively review, and when necessary act upon, information obtained through the monitoring program. In the XYC case, the appeals court determined that it was reasonable to impose on XYC duties to investigate further and stop the Employee's child pornographic activities based in part on the company's possession of monitoring software that was capable of tracking the Employee's e-mail and Internet use. The fact that the company had not implemented the software provided no defense. Similarly, the appeals court chastised XYC for not

checking websites visited when the URLs stored in computer logs and the browser's memory suggested pornographic activity. The court also reasoned that the employer gained notice of potentially harmful activities when co-workers complained of suspicious cubicle conduct that may have presaged nothing more than playing computer solitaire. In other words, employers cannot defend against a negligence claim similar to that asserted in the XYC case by arguing that they could not have uncovered unlawful activity because they do not actively use their monitoring capabilities.

The XYC case provides yet another reminder for employers of the importance of adopting and enforcing an effective electronic resources policy. Following a line of cases, the New Jersey Court of Appeals unambiguously held that XYC's electronic resources policy defeated the Employee's purported interests in the privacy of his e-mail and Internet activities. At the same time, the court emphasized that the failure by several managers to report Employee's improper conduct to the personnel department, as the policy required, supported a finding of negligence.

Even if the XYC case ultimately is read narrowly to impose duties only when employers are on notice that an employee is using corporate resources to view pornography, the case still will have significant ramifications for employers. A variety of statistics and anecdotal evidence suggest that viewing erotica at work is commonplace: 70% of porn is downloaded between 9 AM and 5 PM, according to the porn industry group SexTracker; Internet Filter Review reported that 20% of men and 13% of women surveyed had admitted to accessing pornography at work; and a major U.S. computer manufacturer discovered after installing monitoring software that several employees had visited more than 1,000 sexually oriented sites in less than one month.

Finally, employers must tread with caution when fulfilling a duty to investigate possible child pornographic activities. Employers should warn the employees involved in the investigation, as well as any involved in routine monitoring, to avoid accessing the child pornography themselves so that these employees do not expose themselves to possible criminal prosecution for viewing child pornography Because knowing possession of child pornography is a crime, employers who learn that an employee has accessed child pornography using corporate resources should immediately contact local law enforcement authorities and the FBI. In addition, the suspect computer should be isolated to avoid the possible destruction of material evidence and to prevent any other employees from viewing the child pornography.

Conclusion

Monitoring employee e-mail and Internet use can be a double-edged sword. While the surveillance permits employers to prevent abuse of corporate electronic resources, it also opens the door to claims against employers by those who are injured when an employee engages in criminal conduct using corporate electronic resources. To reduce the risk of such liability, employers should implement policies and procedures to ensure that the results of their electronic monitoring are routinely reviewed and that the review is followed by further investigation and disciplinary action, if necessary, when the monitoring reveals potentially unlawful conduct.

Philip L. Gordon is a Shareholder in Littler Mendelson's Denver office, and John M. Julius III is Of Counsel in Littler's San Diego office. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, Mr. Gordon at PGordon@littler.com or Mr. Julius at JJulius@littler.com.