Lead Report

Employment Issues

Court: Employer Awareness of Employee's Child Porn Web Visits Created Duty to Act

In an important decision for employers that monitor employee computer use, a New Jersey appeals court ruled Dec. 27 that an employer that suspected an employee was accessing child pornography Web sites at work had a duty to take action (*Doe v. XYC Corp.*, N.J. Super. Ct. App. Div., No. A-2909-04T2, 12/27/05).

The ruling revives a negligence claim brought by the employee's wife on behalf of her daughter against the employer. The then-10-year-old daughter's nude and semi-nude pictures were uploaded from her stepfather's work computer at a company identified as XYC Corp. New Jersey Superior Court's Appellate division said an employer can be found liable when it is aware that employees are accessing pornography at work and does nothing.

''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 take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties,'' Judge Harvey Weissbard said for the three-judge panel.

The court said that the public policy against child pornography favors ''exposure of crime.'' Thus, the court explained, employers should report an employee's action to the proper authorities and take ''effective internal action to stop the activities,'' whether by terminating the employee or taking some less drastic action.

Disagreeing with XYC's contention that there was no duty because it had no obligation toward the child, the court said the employer had a duty to make sure its employee did not operate as a risk to others. The court also said it was not necessary to show that the employee could harm the child; it only required a showing that the employee could harm anyone.

''[T]he defendant had knowledge that Employee was engaging in activities that posed the threat of harm to others, although not necessarily to [the child],'' Weissbard said.

Employee Monitoring Concerns. The employee was an accountant at the company's headquarters in Somerset County, N.J. His work space involved a shared cubicle with no doors that opened to a hallway.

XYC, which monitors computer log reports, began noticing that the employee was accessing pornographic sites at work. Two information technology employees contacted the employee and told him to stop, but did not report the behavior to their supervisors.

The employee's supervisor also raised concerns about the impression that the employee was accessing pornography and asked IT employees to monitor the employee. The IT department monitored the employee for two days, but did not keep a log of the sites visited, or open the Web sites he accessed. None of the sites appeared to be directly related to child pornography. When the supervisor contacted a top IT official in the company, he was admonished for accessing computer logs and told never to do it again.

The decision ''poses challenges for employers because it does not specifically define the types of information'' that would trigger a duty.

PHILIP L. GORDON, LITTLER MENDELSON, DENVER

The IT official never contacted the employee about the sites because she allegedly believed that company policy prohibited monitoring or reporting employee Internet activities and that any employee who engaged in monitoring could be disciplined.

In addition, another co-worker also began complaining about the employee accessing pornography, noting the employee was trying to shield his computer screen and quickly minimizing the screen so others could not see what he was accessing. The co-worker complained to her supervisor—who also witnessed the behavior—and the supervisor complained to others in the company, but no action was taken.

Uploading Pictures from Work. Company officials continued to have concerns about the employee's computer usage and even went to his cubicle while he was on break to look at the sites visited listed on his Web browser. Despite evidence that he was accessing numerous pornography sites—including sites that appeared to contain child pornography—the company again only told the employee to stop his activities.

Five months before his eventual arrest, the employee began secretly videotaping and photographing his wife's daughter at their home in nude and semi-nude positions. The child had gone to the employee's ''Take Your Daughter to Work Day,'' and company officials knew he had a young child in his household, the court wrote.

In June 2001, the employee uploaded three pictures of his stepdaughter to child pornography Web sites using his company computer. He ultimately admitted having more than 100 pornographic images on his work computer. He was arrested in late June 2001 after a search of his work computer and work space, based on a police search warrant, revealed evidence of illegal activity.

A search of the workplace found e-mails sent to child pornography Web sites and to others interested in child pornography. In a company dumpster the police also found photographs of the child. The employee was terminated after the search.

The employee's wife filed a negligence lawsuit against XYC, seeking damages for care and treatment of the child and alleging that the harms were proximately caused by the company's breach of its duty. A trial court judge rejected the claim and granted summary judgment to the employer.

Court: No Legitimate Privacy Expectation. In reversing, the appeals court pointed to XYC's e-mail and computer use policy that reinforced that e-mail was company property and that it had a right to review, audit, access, and disclose any e-mail. The court noted that the employee worked in an open area with no door and that his computer screen was visible from the hallway.

''Under these 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,'' Weissbard explained.

The issue left for the jury on remand, the appeals court said, was whether the XYC's duty breach was the proximate cause of the harm to the child.

Judges Ermine L. Conley and Paulette M. Sapp-Peterson joined in the decision.

Ruling Important For Employers. Philip L. Gordon, with the labor and employment law firm of Littler Mendelson, Denver, said the case ''is important for all employers whose employees use e-mail and the Internet, which in today's working world means virtually all employers.''

He noted that, ''consistent with other cases that have addressed the question,'' the court found that the employee could not claim his workplace computer activities were private from him employer, due to the existence of XYC's electronic resources policy.

''The Court of Appeals also addressed a question that has not been addressed in any prior case: when must an employer investigate the use of its computer resources to access or transmit child pornography,'' Gordon said. ''The court held that when supervisory/management personnel are on notice that an employee is viewing pornography, including child pornography, the employer is 'under a duty to investigate further.' ''

Moreover, the court wrote that ''when viewing or possessing child pornography is involved, the employer also has a duty to report the employee's activities to the appropriate authorities and to take effective internal action to stop those activities,'' Gordon said.

According to Gordon, the ruling ''poses challenges for employers because it does not specifically define the types of information that are sufficient to be considered notice that triggers the duties described above. In the XYC case, the employer knew in early 2000 that the employee was accessing pornographic sites at work, but the employer did not have evidence that the employee was accessing child pornography until March, 2001. The court's opinion, nonetheless, suggests that the employer's duty to investigate further was triggered in early 2000. In light of these facts, an employer who learns that an employee is accessing adult pornography at work arguably has a duty to determine whether the employee has accessed child pornography, and even if the employee has not accessed child pornography, to take some steps to ensure that the employee does not access child pornography in the future,'' Gordon said.

He noted that because possession of child pornography is a crime, law enforcement authorities should be contacted promptly, and employers should take possession of ''any computer or other electronic storage media potentially containing the child pornography. Before law enforcement arrives, all storage media potentially containing the child pornography should be isolated. No employee should be permitted to view this material, and IT professionals should not be asked to visit URLs associated with the employee. These steps are necessary because even the incidental viewing of child pornography could be a criminal offense.''

Attorney: Ruling Goes Further Than Other Courts. Management attorney Adam S. Forman of Miller, Canfield, Paddock & Stone, Detroit, told BNA that the ruling was unusual in both the reasoning it used to find liability and the messages it sent to employers.

While the decision seems to place employers in a tough dilemma that appears to increase liability if monitoring takes place, that responsibility is part of the reality of increased electronics in the workplace.

ADAM S. FORMAN, MILLER, CANFIELD, PADDOCK & STONE, DETROIT

''It seems this court has gone much further than any other court on finding liability for accessing pornography,'' Forman said. ''It will be interesting to see if other courts follow the ruling and how it is handled in an appeal.''

While the decision seems to place employers in a tough dilemma that appears to increase liability if monitoring takes place, that responsibility is part of the reality of increased electronics in the workplace, he said.

Forman said he was surprised by the connection made between accessing pornography and the assumption that the employee was accessing child pornography based on limited evidence. ''Employers should be on notice that porn activity on a company system should lead to some investigation and a response that is reasonably calculated to respond to the employee's actions,'' Forman said.

Attorneys for the parties did not respond to calls from BNA.

Kevin Kovacs of Purcell, Ries, Shannon, Mulcahy & O'Neill, Bedminster, N.J., represented the Does. Richard D. Catenacci of Connell Foley, Roseland, N.J., represented the employer.

BY MICHAEL R. TRIPLETT

Full text of the decision is available at http://op.bna.com/pl.nsf/r?Open=dapn-6kphxb.

  PVLR ISSN 1538-3423