

LEGISLATIVE UPDATE

David B. Lichtenberg, Esq.
Morris County SHRM Legislative Chair
Jackson Lewis LLP
(973) 538-6890 (phone)
lichtend@jacksonlewis.com

Doe v. XYZ Corp.
2005 NJ Super LEXIS 377 (App. Div. 2005)

Overview: NJ Appellate Court case decided December 27, 2005. Court addressed whether an employer has a duty to act when it knows or should have known that one of its employees was accessing child pornography.

Facts: Defendant Employee (“Employee”) worked in a shard cubicle with no doors. In or about 1999, Company’s IT Department, in reviewing computer log reports, noticed Employee was accessing pornographic web pages. Company policy limited Internet use to business purposes only. IT Dept. instructs Employee to stop, but did not notify Employee’s supervisors. In early 2000, Employee’s manager instructs IT Dept. to track Employee’s Internet usage. It was obvious Employee was visiting pornographic web sites but IT Dept. did not open the sites to determine the nature of the pages. In December 2000, co-employee complained Employee was shielding his computer screen. Employee’s manager witnesses the same conduct and assumed Employee was viewing pornography. Complaint was relayed by co-employee to Manager of Financial Reporting, but no action was taken. In March 2001, while Employee was at lunch, manager accessed Employee’s computer and confirmed Employee was visiting pornographic web pages. However, manager did not open pages. Employee was again instructed to stop visiting inappropriate web pages. Employee was arrested in June 2001 after it was discovered that Employee was uploading nude photos of his step-daughter to child porn web page using work computer. Police found numerous child porn images, e-mails regarding child porn, and web-sites that dealt with underage sexual activities.

Legal Holdings: Plaintiff’s lawsuit alleged that the Company knew or should have known of Employee’s conduct and had a duty to report Employee’s crimes. The trial court threw the case out – saying that the Company had no duty to monitor or investigate private communications of its employees, and that the Company acted reasonably under the circumstances. The Appellate Division reversed, holding that the Company had both the ability and the right to monitor Internet activity and knew or should have known Employee was accessing pornography at work. Therefore, if the Company had investigated, they would have learned that Employee was accessing child pornography. The Appellate Division held that the Company has a duty to prevent its employees from harming others, either while on the Company’s premises or using Company property, that Employee was using the Company’s property to potentially harm others and the Company had a duty to report Employee to the authorities and to take action to stop harmful activities. The matter was remanded to the trial court for a determination of whether the Company’s conduct caused the harm to the child.

Practical Tips: Review your company's electronic monitoring policies to insure that it minimizes employees' expectation of privacy. Insure that proper controls are put in place to report improper computer usage – the same way that proper controls are put in place to insure there is no harassment. Promptly investigate improper computer usage and consider whether formal disciplinary action is warranted. Consult legal counsel regarding duty to report to the authorities.