February 2006

CLIENT ALERTS

EPSTEIN BECKER & GREEN, P.C.

Resurgens Plaza
945 East Paces Ferry Road
Suite 2700
Atlanta, Georgia 30326-1380
404.923.9000

150 North Michigan Avenue
35th Floor
Chicago, Illinois 60601-7553
312.499.1400

Lincoln Plaza
500 N. Akard Street
Suite 2700
Dallas, Texas 75201-3306
214.397.4300

Wells Fargo Plaza
1000 Louisiana
Suite 5400
Houston, Texas 77002-5013
713.750.3100

1875 Century Park East
Suite 500
Los Angeles, California 90067-2506
310.556.8861

Wachovia Financial Center
200 South Biscayne Boulevard
Suite 2100
Miami, Florida 33131
305.982.1520

Two Gateway Center
12th Floor
Newark, New Jersey 07102-5003
973.642.1900

250 Park Avenue
New York, New York 10177-1211
212.351.4500

One California Street
26th Floor
San Francisco, California 94111-5427
415.398.3500

One Landmark Square
Suite 1800
Stamford, Connecticut 06901-2681
203.348.3737

1227 25th Street, N.W.
Suite 700
Washington, DC 20037-1175
202.861.0900

EBGLAW.COM

New Jersey Appellate Court Holds That an Employer That Suspects an Employee Is Accessing Child Pornography Web Sites Has a Duty to Take Action

The New Jersey Appellate Division in *Jane Doe individually and as g/a/l for Jill Dow, a minor, v. XYC Corporation* recently held that an employer who suspects an employee is accessing child pornography Web sites has a duty to investigate and prevent such conduct from continuing.[1] Failure to comply with this duty may render an employer liable to a third party that is affected by such conduct.

From 1998 through 2001, several employees informed XYC Corp. that Employee was using his computer to view pornographic Web sites. Although an investigation confirmed these complaints, no action was taken. Indeed, when XYC Corp.'s network administrator brought this conduct to the attention of the company, he was admonished for violating XYC Corp.'s policy against monitoring the Internet activity of its employees.

In March 2001, Employee's immediate supervisor was notified that a coworker had seen a picture of a bikini-clad woman with "very large breasts" in a "sultry pose" on Employee's computer screen. While Employee was out, the immediate supervisor checked the sites that Employee visited. The inspection revealed that Employee visited various pornographic sites, including "one that specifically spoke about children." Accordingly, Employee was told to stop using the computer to view inappropriate sites.

In early June 2001, Employee's supervisor discovered that Employee was again viewing pornographic materials at work. Again, no action was taken based on this discovery.

In October 2000, Employee married a woman with a 10-year-old daughter named Jill. In 2001, Employee began secretly videotaping and photographing Jill both nude and seminude. Jill had been at XYC Corp.'s

---

[1] Due to the sensitive nature of the subject matter before the court, both the plaintiffs' and the defendant's identities were kept anonymous and the employee who was accessing child pornography is referred to as "Employee."

headquarters for "Take Your Daughter to Work Day" and had attended company outings.

On June 15, 2001, Employee utilized his workplace computer to transmit three of the secret photos of Jill over the Internet to a child pornography site. This transmission was necessary for Employee to gain access to the site.

On June 21, 2001, Employee was arrested on child pornography charges.

After his arrest, Employee admitted that he had stored child pornography, including nude photos of Jill, on his workplace computer. He further admitted that while working for XYC Corp. he downloaded more than 1000 pornographic images onto his workplace computer.

Plaintiffs, Jane Doe, mother, and Jill Dow, daughter, brought suit against defendant, XYC Corp., alleging that XYC Corp. was responsible for harm caused to Jill when Employee utilized XYC Corp.'s computers to transmit and store pornographic photographs of her. The lawsuit alleged that XYC Corp. knew that Employee was viewing child pornography and knew that Employee had married a woman with a 10-year-old daughter. The suit alleged that XYC Corp. was therefore negligent in not reporting Employee's activities and that said negligence resulted ultimately in harm to Jill.

The Law Division ruled that XYC Corp. did not have a duty to report its employees' Internet browsing activities to authorities and thus could not be held liable for its failure to do so. Accordingly, the Law Division granted XYC Corp.'s motion for summary judgment.

On appeal, the Appellate Division stated that XYC Corp. could be held liable if (1) XYC Corp. had the ability to monitor Employee's use of the Internet on his office computer; (2) XYC Corp. had the right to monitor Employee's activities; (3) XYC Corp. knew, or should have known, that Employee was using the office computer to access child pornography; (4) XYC Corp. had a duty to act to prevent Employee from continuing his activities; and (5) XYC Corp.'s failure to act proximately caused harm to Jill.

The Appellate Division determined the first four factors were indeed present. First, the court found that XYC Corp. clearly had the ability to monitor Employee's activities on his computer. Second, based on XYC Corp.'s policy that employees were permitted to only "access sites which are of a business nature only" and that "any employees who discover a violation of this policy shall notify personnel," the court found that XYC Corp. had a right to monitor Employee's activities on his office computer. Third, the court found that XYC Corp. was on notice of Employee's activities. Fourth, the court found that XYC Corp. had a duty to exercise reasonable care to stop Employee from using the company's computer system to view child pornography.

Finally, the Appellate Division held that XYC Corp. could be held liable to Jill for any harm proximately caused by XYC Corp.'s failure to stop Employee from using his workplace computer to transmit and store pornographic images of her. The case was then remanded to the Law Division for a determination on this issue.

In the wake of the *Jane Doe* decision, employers should establish and distribute a policy that company computers and the Internet are to be used for business purposes *only*. The policy should also provide that the company will monitor the employees' computer and Internet activity. Additionally, employers should make all

efforts to enforce this policy. Further, once an employer is on notice that an employee is violating this policy, an employer has a duty to investigate the employee's activities and to take prompt and remedial action to stop the unauthorized activity. Based on the *Jane Doe* decision, an employer's failure to investigate and make all efforts to stop the unauthorized activity may result in an employer being held liable for harm suffered by third parties, based on the unauthorized activity.

* * *

Please feel free to contact **Joseph D. Guarino** in the firm's **Newark** office at 973/639-8267 if you have any questions or comments. Mr. Guarino's e-mail address is **jguarino@ebglaw.com**. **Dina C. Kerman**, an associate in the Labor and Employment Department, assisted in the preparation of this Alert.