

Tech Trends

TECH TRENDS/LITIGATION

Monday, October 4, 2004

Child Porn Poses risks to Companies that Discover it in the Workplace

By Beryl A. Howell and
Paul H. Luehr

Companies and their lawyers who fail to keep up with child pornography law do so at their peril. The bipartisan resolve of state and federal legislators to combat child pornography has led to laws that put the fate of those who innocently possess child porn — such as counsel and their forensic experts — largely at the mercy of prosecutorial discretion.

Dealing administratively with employees who use company computers to view or download child pornography no longer suffices. In fact, company lawyers or managers risk serious criminal penalties if they merely terminate an offending employee and delete only visibly illicit images from his desktop computer.

The law generally treats child porn like heroin: mere knowing possession of it is a crime. Possession on behalf of a client to assist in an investigation or defense is no exception. As one court put it: “Child pornography is illegal contraband.”¹

Three overlapping federal criminal statutes make the handling of child pornography illegal. These statutes prohibit the knowing production, receipt, shipment, distribution, reproduction, sale, or possession of “any visual depiction involv[ing] the use of a minor engaging in sexually explicit conduct,” or of “any material that contains an image of child pornography.”²

Violations are punishable by a mandatory minimum term of imprisonment for five years and up to 20 years,³ except for mere possession, which is punishable for up to 10 years.⁴

The plain terms of these federal statutes should cause attorneys and forensic experts to be cautious. “Distribution” could cover counsel’s knowing transmittal of illegal images to an outside expert for analysis, despite the need to investigate the scope and origin of any pornography problem within corporate corridors.

Criminal liability may also be triggered by knowing possession of a single child porn image. A limited statutory affirmative defense is available when a defendant possesses fewer than three such images, but only if the defendant: (1) does not retain

any offending visual depiction; (2) does not allow any person other than a law enforcement agent to access the offending visual depiction; and (3) promptly takes reasonable steps to destroy each such visual depiction or reports the matter to a law enforcement agency and gives the agency access to each such visual depiction.⁵

Notably, this statutory affirmative defense is not available if three or more images are found — and usually where there is one such image, there are dozens or hundreds more. Thus, if a company finds multiple child porn images on an employee’s computer, the affirmative defense evaporates, and handling or even destroying the images may expose the company to criminal liability.

Some observers may find it absurd that discovery of child pornography in the workplace carries the risk of criminal liability. Yet, the scienter requirement for the possession crime is “knowingly” — no bad motive or evil intent is required. For this reason, courts have rejected the defense to possession charges that the defendant was doing research.⁶

Cautionary Tales

Courts also have rejected private investigations as an excuse to possess illegal images. In one case, a Virginia defendant contacted the FBI and the U.S. Customs Service periodically over two years, stating that “he had received child pornography over the Internet and wished to turn it over to the government to assist in the enforcement of child pornography laws.”⁷ Agents reminded the defendant that possessing child pornography was illegal, and later arrested and charged him with this crime. He was convicted in a bench trial.

After several years of appeals, his conviction was vacated in 2004 on the grounds that the prosecution did not prove that his images depicted actual children.⁸ Although the defendant was eventually exonerated, this case provides little comfort to in-house corporate counsel contemplating an internal investigation since defendant was not exonerated on a theory that his possession was “innocent.”

In another case, a Maryland couple set up a home surveillance camera to see if a neighborhood teenager was stealing from them. The camera inadvertently captured the teenager engaging in sexual acts with the couple’s dogs over several days. According to the couple, they discussed the situation with several friends and later voluntarily delivered the videotape to the police. Unbelievably,

the couple was arrested for possession of child porn, among other charges. They ultimately agreed to resolve the matter with probationary terms. Meanwhile, however, the couple lost its key business client over the scandal. The couple sued local authorities for violating their constitutional rights but lost on summary judgment.⁹

These examples are cautionary tales about handling child pornography, even when the purpose is to notify authorities. In other simple possession crimes involving narcotics or guns, some courts recognize a narrow “innocent possession defense,” where the person technically possesses contraband but attains it innocently with the intention of promptly turning it over to a lawful authority.¹⁰ One court explained, “[t]he ‘possession’ forbidden by the statute ‘should not be construed to mean a possession ... which might result temporarily and incidentally from the performance of some lawful act’... particularly when ... the act was designed to meet the social policy of the law.”¹¹ This reasoning could apply where a company discovers child porn on its network, yet there appear to be no cases applying the innocent possession defense to a child pornography case.

In short, current child pornography laws arguably create a duty to report child pornography to law enforcement. Strictly speaking, reporting does not even negate “knowing ‘possession,’” but prompt reporting should quell any prosecutor’s desire to indict, even in those jurisdictions that do not recognize the “innocent possession defense.”

When child porn is found, company management should ask: Is this really illegal child porn? Was the employee actively sending child porn to other employees or individuals? Was the employee actively posting child porn to Internet sites from a company computer? Are the child porn images only on the employee’s workstation computer or are they also on PDAs, floppy drives or other removable media? During system back-ups, were the illegal child porn images saved to other parts of the corporate network? Do further stores of child pornography exist on company computers in encrypted, hidden, or renamed form? Must this be reported to law enforcement authorities and, if so, how much time is there to decide?

Finding answers to these questions will require careful probing and, unfortunately, can place in-house counsel between a rock and several hard places. Ignoring the problem could create a “hostile work environment” or impose liability on the company for harm caused by a known pedophile.

Beryl A. Howell, an attorney, is a Washington, D.C.-based managing director of Stroz Friedberg, a digital forensics consulting and technical services firm. **Paul H. Luehr**, also an attorney, is a vice president of the firm in Minneapolis.

Sticking one's head in the sand also could expose managers to "possession" charges or damage the company's reputation if unannounced searches and arrests of employees occur. If three or more child porn images exist, simply deleting them from the offending employee's computer could obstruct a known criminal investigation, and sending child porn to outside experts for analysis may implicate "distribution" issues.

Relying on internal technical employees to handle the problem also poses serious risks, including the possibility that they might inadvertently taint or destroy evidence, "leak" facts about the internal investigation, or "check out" Web sites visited by the suspect employee, thereby caching more illegal child porn onto the company network.

Once child porn has been discovered within a company, the safest options are to consult with a computer forensic expert about other possible locations of illegal images, promptly refer the discovery of any images to law enforcement, and cooperate in any further investigation. In fact, responsible computer forensic experts will make clear that discovery of child pornography during an examination should prompt a law enforcement referral. Companies may be reluctant to make such referrals since further investigation by law enforcement may be distracting and might result in bad publicity. Nonetheless, the alternatives of ignoring illegal images, transferring them, or destroying them carries significant risk of criminal liability for possession or distribution of child pornography, destruction of evidence, and obstruction of justice.

Given the risks at stake, whether certain images constitute child pornography is a critical issue. Federal statutes provide some guidance and define child pornography as an image that shows a minor engaging in "sexually explicit conduct."¹² Such conduct may take the form of actual or simulated "sexual intercourse," "masturbation," "sadistic or masochistic abuse," or a "lascivious exhibition of the genitals or pubic area."¹³

In many courts, "lascivious exhibition" is further defined based on six factors: (1) whether the genital or pubic area are the focal point of the image; (2) whether the setting of the image is sexually suggestive; (3) whether the child is depicted in an unnatural pose or inappropriate attire considering her age; (4) whether the child is fully or partially clothed, or nude; (5) whether the image suggests sexual coyness or willingness to engage in sexual activity; and (6) whether the image is intended or designed to elicit a sexual response in the viewer.¹⁴ Nudity is not required, if "a photographer unnaturally focuses on minor child's clothed genital area."¹⁵

The age of the person portrayed in the image may not be apparent and that raises questions about whether a pornographic image is illegal. Federal law prohibits possession of sexually explicit images of a "minor" and defines that term to mean a person under 18,¹⁶ even though many state child porn statutes turn on the "age of consent," which may be 16 or even younger.

Determining whether an image is illegal may require knowledge about whether the actual person depicted was under 18 at the time of the photo, or may require assistance from medical experts, who use the so-called "Tanner scale" to analyze body proportions, growth and development to ascertain a subject's age.¹⁷

Determining whether a picture is illegal also may turn on whether an image is "real," "virtual," "morphed," or "obscene." In 2002, the U.S. Supreme Court ruled that federal law may criminalize possession of images that depict real children engaging in sexually explicit conduct, but not possession of a cartoon or virtual image that only "appears to be" a minor or "conveys the impression" of a minor engag-

ing in such conduct.¹⁸

In response, Congress redefined "child pornography" to cover a computer-generated image "that is indistinguishable from that of a minor engaging in sexually explicit conduct,"¹⁹ only to generate another constitutional challenge in the courts.²⁰

Meanwhile, the distribution or receipt of "real" or "virtual" images may still be illegal if they are "obscene,"²¹ and the Supreme Court has hinted that it may be illegal to possess images of real children that have been "morphed" to look like child porn.²²

In light of these uncertain and shifting definitions, if there is any doubt about the illegality of an image, the safest option is to treat it as child pornography.

When child porn is found, there may be a natural tendency for managers and lawyers to handle the situation quietly, but that poses dangers in light of prosecutors' broad discretion.

Discovery of child porn on a specific company computer may be just the tip of the iceberg. A forensic examination of that computer will help determine whether the illegal images were sent via e-mail to other employees and may reveal whether the illegal images were printed or copied onto removable media, such as thumb-drives, floppy disks or CDs.

This examination also may reveal whether shared file servers or e-mail servers were used to archive illegal images and may reveal whether a peer-to-peer (P2P) file-sharing program has been improperly installed on the network and used to trade child porn.

Finally, a computer forensic examination may reveal whether some illegal images have been encrypted, hidden within other image files, or pasted into word processing documents.

Even if an employee did not intentionally "save" illegal images onto a company computer, the images may still be stored there. Images viewed on Web pages are automatically saved to a browser cache folder and stored on the user's hard drive until the contents are overwritten or deleted. Evidence from such browser caches have been used to convict individuals of possession of child pornography, particularly when the user has shown a sophisticated understanding of his computer, even in the absence of evidence that the defendant affirmatively saved images to his hard drive.²³

In short, finding illegal images stored in user-created folders on the offending employee's computer is merely the beginning of the search for all the illegal images and evidence that may exist on corporate computers. Moreover, finding illegal images on one employee's computer is just the beginning of the investigation into whether that person is responsible and whether he acted in concert with others to bring child porn into the company.

Special problems arise even when a company wants to preserve evidence of child pornography and turn that evidence over to law enforcement. Whenever child porn is found on a business network, the company understandably will want its business data segregated from the contraband, while law enforcement will often want to preserve as evidence the entire hard drive on which the contraband was found. Accommodating both legitimate interests often requires using a forensic expert

to provide detailed protocols about the examination process and the accuracy of any harvested data.

In many circumstances, negotiating a protocol with the investigating law enforcement agency or seeking direction from the court may be appropriate.²⁴ Stringent controls may be placed on your computer forensic expert regarding where the examination will take place (e.g. at the FBI lab), if images or sensitive business records can be copied or removed or redacted, and how the original hard drive and any forensic copies will be maintained (e.g. under a court seal or in the custody of law enforcement).

If a company is concerned about privileged documents or sensitive business records that exist on a hard drive held by law enforcement, a company may want to seek direction from the court or ask that the company's forensic expert be present during the initial examination of the hard drive.

The company also may want to seek a non-disclosure agreement covering its business records and a protective order requiring notice to the company prior to any subsequent examination of the hard drive by the government or third parties.

Current criminal laws governing the distribution and possession of child pornography pose substantial risks to companies that discover such contraband on their computers.

There may be a natural tendency for managers and lawyers to look the other way or handle the situation quietly and administratively. This approach poses many dangers, especially in light of the broad discretion exercisable by prosecutors. Pending a Solomonic fix by Congress, referral to and cooperation with law enforcement carries certain risks and procedural headaches, but it is the best course for the responsible corporate citizen.

1. *United States v. Kimbrough*, 69 F.3d 723, 731 (5th Cir. 1995).

2. 18 U.S.C. §§2251(a), 2252(a), 2252A(a).

3. 18 U.S.C. §§1466A(a)(2)(B), 2252(b)(1), 2252A(b)(1).

4. 18 U.S.C. §§1466A(b)(2)(B), 2252(b)(2), 2252A(b)(2).

5. 18 U.S.C. §§2252(c), 2252A(d).

6. *United States v. Mathews*, 209 F.3d 338 (4th Cir.), cert. denied, 531 U.S. 910 (2000); *United States v. Bunnell*, 2002 U.S. Dist. LEXIS 8319 (D. Maine).

7. *United States v. Hilton*, 257 F.3d 50, 52 (1st Cir. 2001).

8. *United States v. Hilton*, 363 F.3d 58, 65 (1st Cir. 2004).

9. *Bruette v. Montgomery County*, 2003 U.S. App. LEXIS 12754 (4th Cir.).

10. *United States v. Mason*, 2000 U.S. App. LEXIS 31868, at pp. 4-5 (D.C. Cir.), and cases cited therein.

11. *New York v. E.C.*, 761 N.Y.S.2d 443, 444-45 (Sup. Ct., Queens Cty 2003).

12. 18 U.S.C. §§2251(a), 2252(b)(4), 2256(8).

13. 18 U.S.C. §2256(2)(A).

14. *United States v. Dost*, 636 F. Supp. 828, 832 (S.D. Cal.), aff'd sub nom, *United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1986).

15. *United States v. Knox*, 32 F.3d 733, 750 (3d Cir. 1994).

16. 18 U.S.C. §2256(1) (2004).

17. *Hilton*, supra, 363 F.2d at 58, 60, 64 (1st Cir. 2004).

18. *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).

19. 18 U.S.C. §2256 (8)(B) & (C) (2004).

20. *Hilton*, supra, 363 F.3d at 65 (finding the new definition unconstitutional).

21. See e.g. 18 U.S.C. §§462, 1466(a).

22. *Free Speech Coalition*, supra, 535 U.S. at 240.

23. See e.g. *United States v. Tucker*, 305 F.3d 1193, 1198 (10th Cir. 2002), cert. denied, 537 U.S. 1123 (2003).

24. *United States v. Hill*, 2004 U.S. Dist. LEXIS 11116, at 10-11 (C.D. CA)