

The American Bar Association
Criminal Justice Section
and the
Center for Continuing Legal Education
Present

An ABA-CLE Publication on

White Collar Crime 2008

**Digital Contraband:
Finding Child Porn in the Workplace**

By Beryl A. Howell¹
Stroz Friedberg
Commissioner, U.S. Sentencing Commission
Washington, DC

The search for records responsive to discovery demands or relevant to an internal inquiry may occasionally turn up the unexpected: digital contraband in the form of child pornography. Corporate computer usage policies usually ban the use of workplace computers to access, purchase or view pornography of any type. Nevertheless, in the course of electronic discovery, violations of this policy are regularly discovered, along with other usage policy violations, such as downloaded pirated music or the installation of unauthorized applications. Yet, finding child pornography on workplace computers is a different category of violation with potential consequences that are more serious than just an internal disciplinary headache. Pornographic images of children may be evidence of criminal activity and therefore require careful handling, further investigation and communications with law enforcement.

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 since “[e]ven an arguably laudable intent is not a defense.”² As one court put it: “Child pornography is illegal contraband.”³ The company must take steps to minimize its own liability risks from an employee’s illegal access to child porn, and those risks can loom large if the illicit images are mishandled.

What should in-house or outside counsel do when child pornography is found on a company computer? Simply ignoring the problem is not an option, not only from a moral perspective, but also as a legal matter: “doing nothing” could provide a basis for “hostile work environment” claims or may subject the company to civil suit by “any person aggrieved” by the possession of the images.⁴ Significantly, sticking one’s head in the sand also could expose managers to child porn “possession” charges or damage the company’s reputation if unannounced searches and arrests of employees occur at the workplace. Moreover, if three or more child porn images exist, simply deleting them from the offending employee’s computer could be viewed as obstruction of a criminal investigation. Circulating the child porn images internally or to outside experts to elicit multiple views about how to handle the situation may implicate “distribution” issues. Relying on in-house IT staff to investigate the problem also poses potential problems, 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 offending employee, thereby caching more illegal child porn onto the company network.

When child porn is discovered within the company, the safest options are to consult with a digital forensics expert about other possible locations of illegal images, promptly refer the discovery of any images to law enforcement, and cooperate in any further government investigation. The steps undertaken by company counsel should be guided by three fundamental questions.

First, do the graphic files constitute illegal child porn? This is a critical issue and pictures that may be in poor taste or simply show naked children do not cross the line of illegality. Federal statutes provide some guidance. Child pornography is defined as an image that shows a minor engaging in “sexually explicit conduct.”⁵ 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”⁶ 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 or his 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.⁷ In fact, nudity is not required, if “a photographer unnaturally focuses on minor child’s clothed genital area...”⁸

The age of the person portrayed in the image may not be readily apparent, prompting reasonable questions about whether a pornographic image is illegal. Federal

law prohibits possession of sexually explicit images of a “minor.” That term is defined to mean a person “under the age of eighteen years,”⁹ even though a number of 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 may use the so-called “Tanner scale” to analyze body proportions, growth and development to ascertain a subject’s age.¹⁰

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 engaging in such conduct.¹¹ 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,”¹² only to generate another constitutional challenge in the courts.¹³ Meanwhile, the distribution or receipt of “real” or “virtual” images may still be illegal if they are “obscene,”¹⁴ 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.¹⁵

In light of these uncertain and shifting definitions, the pictures at issue should be treated as suspected child porn until an experienced government law enforcement official evaluates the images and confirms they are or are not contraband. Depending upon the jurisdiction, law enforcement may be willing to view the images onsite where they were originally found.

Once the suspected graphic images are determined to be child porn, three overlapping federal criminal statutes are relevant to the handling of these digital files. 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.”¹⁶ Violations are punishable by a mandatory minimum term of imprisonment for five years and up to twenty years,¹⁷ except for mere possession, which is punishable for up to ten years.¹⁸

Second, after discovering potentially illegal images on corporate computers, counsel should ask: Are those images anywhere else on the corporate network? This is important because the amount and location of child pornography may dictate how those images are handled, if at all.

Criminal liability may be triggered by the knowing possession of a *single* child porn image or “distribution” or transfer of illegal images. Notably, the scienter requirement for the possession crime is “knowingly” – no bad motive or evil intent is required.¹⁹ 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.²⁰ This statutory affirmative defense is not available if three or more images are found. Usually where there is one such image, there are dozens or hundreds more. If this is the case, the affirmative defense evaporates, and handling or even destroying the images may expose the company to criminal liability.

In short, discovery of child porn on a specific company computer may be just the tip of the iceberg and should trigger other investigatory queries:

- Did the offending employee send child porn to other employees, whose workstations should be examined?
- Are the child porn images only on the employee's workstation computer or is there evidence on that workstation that the images were transferred from or to external hard drives, CDs or other removable media or even an online storage area?
- Were the child porn images found in a location subject to system back-ups?
- Were the child porn images found in a format that suggests further stores of child pornography may exist on company computers in encrypted, hidden, or re-named form?

A company may find itself between the proverbial rock and a hard place when, to minimize the risk of possession liability, it undertakes an investigation of the corporate network to find any other caches of child porn and, at the same time, due to the distribution prohibition, cannot transfer the media where the illicit images are found to outside experts for analysis or purging. Dealing with this conundrum may require creative solutions such as employing forensic analysis on-site or crafting concrete technical protocols that can be sanctioned by law enforcement.

A forensic examination of the computer on which the child porn was found will help determine whether the illegal images were sent via e-mail to other employees using workstations in the office and may reveal whether the illegal images were printed or copied onto removable media, such as thumb-drives, floppy disks or CDs. In situations where multiple employees may have access to office computers, forensic examination may also help identify the user responsible for bringing the child porn into the company. In addition, this examination 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 with .doc or .wpd extensions.

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.²¹

One predicament that can confound counsel is the unearthing of child porn in the course of electronic discovery. During that process the graphic files may also have been included in data produced to counsel for review or uploaded onto a litigation review database. In those circumstances, the media polluted by the child porn images may be accessible to many people and, at the same time, may be critical to meeting legal obligations of the company. This highlights the importance of maintaining accurate records that track both the origin and disposition of data as it is collected and processed in electronic discovery projects. Moreover, evaluating the file types necessary for extraction and processing at the outset of an electronic discovery project -- and excluding graphic file formats from processing and upload to the litigation review database -- can spare the company any issue that the database has been polluted with child porn. In the worst case scenario, however, where copies of contraband images have found their way into litigation-critical media or databases, counsel can work out a protocol with law enforcement to purge the copies of the images with minimal disruption to the review process.

Finally, when the matter is referred to law enforcement, how can confidential, business-related data be protected when that data is located on the same hard drive with the child porn? Companies may be reluctant to make law enforcement referrals in part due to the distraction of cooperating with a criminal investigation and the potential for bad publicity, but they are also greatly concerned that such cooperation will require disclosure of confidential business information. 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.

Segregating business data from the suspected child porn images to be turned over to law enforcement may not be possible. Law enforcement will likely want to take custody of the entire hard drive or other media on which the contraband was found. If a company is concerned about privileged documents or sensitive business records that exist on a hard drive that is being turned over to law enforcement, a company may want to negotiate a protocol with the investigating law enforcement agency to maintain a copy of the business-related data. Alternatively, the company may want to negotiate a protocol to redact its business-related data from the media before turning it over to law enforcement, or restrict law enforcement’s examination just to the images at issue. In any of these scenarios, company lawyers and law enforcement may want to seek direction from the court.²² Separate from any handling protocols, 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 dissemination of data from the hard drive by the government to other government offices or third parties.

If the computer hard drive containing child porn is turned over to law enforcement when additional information must be extracted from the hard drive for business or litigation purposes, stringent controls may be placed on access to the computer. A recent amendment to federal law requires that “in any criminal proceeding,” child porn materials must “remain in the care, custody, and control of either the Government or the court.”²³ Even when the company is cooperating and provides a hard drive voluntarily, the controls on access to its data will be stringent and may include requiring that examination of the hard drive take place at law enforcement offices, that a government official be allowed inspect any files that are copied or removed from the computer to ensure that the files are not contraband, or that the company or its expert certify that no contraband has been copied.

Current criminal laws governing the distribution and possession of child pornography pose substantial risks to companies that discover such contraband on their computers or networks. When child porn is discovered during the course of an electronic discovery project, companies and their counsel confront a host of issues that must be addressed, despite the distraction from the project at hand. The company and its counsel must proceed with caution and may find it prudent to hire a forensic expert in order to ascertain: 1) if the offending images actually constitute contraband, 2) where else such images may exist on the corporate network, 3) how to work with law enforcement in order to remove the child porn securely, and 4) what procedures may be employed to access and protect any business data that may be co-mingled with the child porn.

¹ Ms. Howell is the Executive Managing Director and General Counsel of Stroz Friedberg, a consulting and technical services firm specializing in digital forensics, electronic discovery and cyber security investigations, and a Commissioner on the U.S. Sentencing Commission. The views expressed in this article are solely those of the author and do not represent the views of any government agency.

² *United States v. Gallagher*, NMCCA 200400151, 2007 CCA Lexis 53, n. 3 (U.S. Navy-Marine Corp Court of Criminal Appeals Feb. 28, 2007) (defense of innocent possession of child porn to destroy it rejected); *United States v. Mathews*, 209 F.3d 338 (4th Cir. 2000)(conviction upheld of investigative reporter who claimed receipt and distribution of child pornography for news story).

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

⁴ 18 U.S.C. § 2252A(f).

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

⁶ 18 U.S.C. § 2256(2) (A).

⁷ *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). *See also United States v. Wages*, 2008 U.S. Dist. LEXIS 3116, *3 (E.D. Ok. Jan. 14, 2008).

⁸ *United States v. Knox*, 32 F. 3d 733, 750 (3d Cir. 1994).

⁹ 18 U.S.C. § 2256 (1) (2004).

¹⁰ *United States v. Pollard*, 128 F. Supp. 1104, 1113-16 (E.D. TN 2000); *United States v. Rodriguez-Pacheco*, 475 F.3d 434, 450, n. 18 (1st Cir. 2007) (dissent cites Arlan L. Rosenbloom & James M. Tanner, Letter to the Editor, *Misuse of Tanner Puberty Staging to Estimate Chronological Age*, 102 *Pediatrics* 1494 (1998) that “the Tanner scale is properly used to estimate sexual maturation, not for the purpose of estimating specific chronological age”).

¹¹ *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).

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

¹³ *United States v. Hilton*, 363 F.3d 58, 65 (1st Cir. 2004) (finding the new definition unconstitutional), *vacated by and opinion withdrawn on other grounds by United States v. Hilton*, 386 F.3d 13 (1st Cir. 2004).

¹⁴ *See e.g.* 18 U.S.C. §§ 1462, 1466(a).

¹⁵ *Free Speech Coalition*, *supra*, 535 U.S. at 240.

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

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

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

¹⁹ *United States v. Gallagher*, *supra*, n. 2 (“As a general matter, no evil intent need be shown to prove an offense under 18 U.S.C. § 2252, as long as the accused knowingly possessed child pornography”); *see also 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).

²⁰ 18 U.S.C. §§ 2252 (c), 2252A (d).

²¹ *See. e.g. United States v. Tucker*, 305 F.3d 1193, 1198 (10th Cir. 2002), *cert. denied*, 537 U.S. 1123 (2003).

²² *United States v. Hill*, 2004 U.S. Dist. LEXIS 11116, at 10-11 (C.D. CA).

²³ 18 U.S.C. § 3509 (m). *See also United States v. Flinn*, 2007 U.S. Dist. LEXIS 80773, *16-17 (E.D. CA 2007) (defense expert must review computer drives at FBI office subject to certain safeguards).