LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin®

An ALM Publication

Volume 18, Number 3 • November 2010

Child Pornography On Workplace Computers

By Marjorie J. Peerce and Carolyn Barth Renzin

Possessing child pornography is potentially such a serious crime that institutions take pains to keep it off their premises. New York University, for example, decided last summer not to accept the archives of artist Larry Rivers after it became public that the collection included films and videos of Rivers' two adolescent daughters, naked or topless, being interviewed by their father about their developing breasts. Without deciding whether the films were in fact pornographic, the university played it safe.

So what are the implications of having child pornography on the premises? In businesses, child pornography generally is discovered by IT personnel. Or, if a corporation undergoes an unrelated internal investigation in which all computers, hard drives, e-mail servers, etc. are frozen and searched for responsive material, such a search can to lead to the discovery of child pornography stored on the corporation's server or on an individual's hard drive. What can/must/should be done as a result?

The Law

Federal law (18 U.S.C. § 1466A) criminalizes the knowing production, distribution, receipt or possession with intent to distribute "a visual depiction of any kind, including a drawing, cartoon, sculpture or painting of

continued on page 6

The Courts: Active Players in White-Collar Cases

By Stanley A. Twardy, Jr. and Doreen Klein

In June, the Supreme Court unanimously held that Enron's former CEO Jeffrey Skilling did not commit "honest services" fraud, ruling that the statute under which he was convicted must be limited to bribery and kickback schemes to avoid constitutional concerns over vagueness. *Skilling v. United States*, 130 S. Ct. 2896 (2010). The defense bar was heartened by these restrictions on a statute that federal prosecutors have used aggressively for years against public officials and more recently against corporate officers. The decision should curtail prosecution of a variety of conduct that the government would otherwise seek to criminalize through the statute. In contrast, the courts are expanding the reach of other criminal statutes to encompass conduct previously regarded as outside their scope.

United States v. Kaiser

In *United States v. Kaiser*, 609 F. 3d 556 (2d Cir. 2010), the Second Circuit abruptly lessened the government's burden of proof in securities fraud cases — apparently catching even the government by surprise — holding that the government need not prove that the defendant knew he was violating the securities laws. *Kaiser* arose out of allegations that the defendant fraudulently reported inflated company earnings in violation of securities laws, including § 32(a) of the Exchange Act, which criminalizes "willful" violations. Both the defendant and the government requested that the district court instruct the jury that willfulness requires that the defendant know his conduct is illegal.

Instead, the court charged the jury that the government had to prove the defendant knew the statements were false, that he made them with intent to deceive, and that the defendant was not simply mistaken or in good faith. In upholding the instruction, the Second Circuit drew a distinction between "wrongfulness" and "unlawfulness," and held that it was sufficient for the government to show that the defendant had "an awareness of the general wrongfulness of his conduct." The court acknowledged that, in *United States v. Cassese*, 428 F.

continued on page 2

In This Issue

Child Pornography

continued from page 1

child pornography … " No evil intent or bad motive need be shown to obtain a conviction. Mere knowledge is sufficient. First-time offenders for possession face up to 10 years in prison, and repeat violators face a mandatory minimum sentence of 10 years.

Once a company knows that child pornography is on its servers, it must take action, because it is a federal crime to "knowingly possess … any … material that contains an image of child pornography," 18 U.S.C.A. § 22552A(a)(5)(B). As a practical matter, the corporation can't destroy the images because that could (except for limited circumstances discussed below) arguably constitute knowing destruction of contraband, a different, independent federal crime under 18 U.S.C. § 4 ("Whoever, having knowledge of the actual commission of a felony … conceals and does not as soon as possible make known the same to some … authority under the United States, [shall be guilty of a felony]"). Further, any such destruction could violate Sarbanes-Oxley's anti-shredding laws. *See, e.g., United States v. Russell*, 639 F. Supp.2d 226 (D. Conn.).

Additional Corporate Liabilities

Beyond the potential for criminal liability, if the corporation knows it has child pornography on its system and another employee sees the material, the corporation could face civil liability for sexual harassment. *See Patane v. Clark*, 508 F.3d 106 (2d Cir. 2007) (employee stated sexual harassment claim against corporation for being forced to handle supervisor's pornography). And the corporation could face civil liability under 18 U.S.C. § 2252A(f), which provides a civil remedy to victims of the child pornography able to show by a preponderance of the evidence that the defendant committed the acts described in any of the listed offenses (including possession). *See Smith v. Husband*, 376 F. Supp. 2d 603, 613 (E.D. Va. 2005). Finally, the corporation could face civil liability under a state's sexual harassment laws and common-law tort laws if a child is victimized by the continued possession after the corporation knew of the existence of child pornography on its computers, but did nothing. *Doe v. XYC Corp.*, 382 N.J. Super. 122, 887 A.2d 1156 (App. Div. 2005).

Thus, knowingly leaving child pornography on a corporation's system is not a viable option. However, can a corporation destroy the offending images?

What the Corporation Can Do

Under very limited circumstances, there is an affirmative defense to possession for the person who discovers child pornography and destroys it, but only if the destruction is done quickly, in good faith, without allowing anyone (except law enforcement) to access or copy the material, and then, only if there are fewer than three images. *See* § 18 U.S.C. 2252A(d); *United States v. Hilton*, No. 97-70-P-C, 2000 WL 894679, at *6 (D. Me. 2000). But an affirmative defense is available only at trial, and continues to leave open a risk of conviction.

So, if a corporation that suspects possession of child pornography cannot sit idle but also effectively cannot destroy the images, what can it do? The best answer is to report it to law enforcement. Usually, when a company finds evidence of a crime, the prudent course is to investigate it internally before reporting to law enforcement. However, what a corporation usually does may not apply to child pornography.

If, while an investigation is underway concerning whether an employee possessed child pornography, the employee again views child pornography (or distributes it, or creates more of it) on the company's computer, the company potentially: 1) was on notice at the time of the act but did nothing to stop a child from being harmed; 2) knowingly possessed the existing child pornography; and 3) knowingly possessed (and even created or distributed) the new child pornography. Therefore, the risks of investigating before reporting are great.

Furthermore, in some states, IT employees themselves are required to bypass management and report suspicions of child pornography directly to law enforcement. If IT employees do not do so, they face possible fines or incarceration. *See* Joanne Deschenaux, Experts: Employers Must Have Policies in Place Regarding Child Pornography, 9/30/2009 (citing National Conference of State Legislatures).

Working with the Authorities

Once law enforcement is alerted, prudence dictates that corporations should work in conjunction with the efforts of authorities to further investigate their network and systems and institute proper discipline for the involved employee(s), up to and including immediate termination. *See, e.g., Muick v. Glenayre Elecs.*, 280 F.3d 741, 742-43 (7th Cir. 2002) (suggesting that no corporate punishment, including termination, is too harsh for the child pornography possessor); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996) (no violation of public policy for terminating employee for transmitting unprofessional e-mails over a corporate network).

Unless corporate policies are directly contrary, after notifying law enforcement and with its approval, a corporation's search for additional violative material is virtually unfettered by privacy concerns of affected employees. *See, e.g., United States v. Angevine*, 281 F.3d 1130, 1135 (10th Cir. 2002) (no reasonable expectation of privacy in relation to the computer employee used at work); *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000) (remote, warrantless searches of office computer by public employer did not violate employee's Fourth Amendment rights).

So what are the steps a corporation should take?

First: Avoid the situation if possible:

continued on page 7

Marjorie J. Peerce (Mpeerce@stillmanfriedman.com), a member of this newsletter's Board of Editors, is a member of Stillman, Friedman & Shechtman, P.C. in New York City with a focus on white-collar criminal defense, regulatory matters and complex civil litigation. **Carolyn Barth Renzin** is an associate at the firm.

BUSINESS CRIMES HOTLINE

GEORGIA

Botox Manufacturer Agrees To Guilty Plea and Combined Criminal and Civil Penalty

On Sept. 1, the U.S. Attorney's Office for the Northern District of Georgia announced that Allergan Inc., the Irvine, CA-based pharmaceutical manufacturer, had agreed to plead guilty and pay $600 million in connection with the company's off-label promotion of its biological product, Botox. The settlement figure, which remains subject to approval by the district court, includes a criminal fine and forfeiture totaling $375 million and a civil settlement with both the federal government and the states totaling $225 million.

The federal Food, Drug, and Cosmetic Act requires that companies specify the intended use for each biological product in the corresponding products' applications to the FDA, whose approval is then granted for each specified use that is safe and effective. It is a federal crime for manufacturers to promote "off-label" uses, defined as those not approved by the FDA.

Sally Quillian Yates, U.S. Attorney for the Northern District of Georgia, described the settlement, in part, by stating, "The FDA had approved therapeutic uses of Botox for only four rare conditions, yet Allergan made it a top corporate priority to maximize sales of far more lucrative off-label uses that were not approved by FDA. Allergan further demanded tremendous growth in these off-label sales year after year, even when there was little clinical evidence that these uses were effective. The FDA approval process ensures that pharmaceutical companies market their medications for uses that are proven to be effective, and this case demonstrates that companies that fail to comply with these rules face criminal prosecution and stiff penalties."

The government's involvement was prompted by the filing of a False Claims Act (FCA) complaint in Georgia against the company by a consultant and sales representative for the company. This complaint was followed by whistleblower complaints in the Districts of Massachusetts and Maryland, filed by two former Allergan employees and another company sales representative, respectively.

MICHIGAN

$140.9-Million Plea Agreement for Price Fixing By Panasonic Corp. and Whirlpool Corp. Subsidiary

On Sept. 30, the DOJ announced that it had reached an agreement with the Japanese Panasonic Corporation, and a Delaware-based subsidiary of Whirlpool Corporation, Embraco North America Inc., for the companies' respective roles in an international price-fixing conspiracy involving refrigerant compressors used in both residential and commercial applications. The agreement, which requires court approval, includes a guilty plea by each entity to a violation of the Sherman Act, as well as combined payment of $140.9 million in criminal fines. For its part, Panasonic agreed to pay a $49.1 million criminal fine, while Embraco agreed to pay a $91.8 million criminal fine.

—❖—

Child Pornography

continued from page 7

an inappropriate purpose may immediately be reported to law enforcement.

- Give notice of company's unlimited right to discipline employees to the full extent of the law, up to and including immediate termination for suspected inappropriate and/or unlawful use of company property.

Third: Monitor company property:

- Monitor employee technology use with random monitoring program that cannot be anticipated by savvy users.

Fourth: Create and disseminate clear reporting procedures:

- Reporting procedures for all employees should state that any suspicion of child pornography in the workplace must be reported immediately to management and then will be reported to federal and/or state law enforcement. Procedures should account for circumstances where the individual to whom such a report ordinarily would have been made is the alleged perpetrator.
- Advise IT employees — often the first responders — to avoid actions that could result in obstruction charges, tainting evidence, "leaking" facts to other employees or other acts that might increase risk to the individual or corporation.

Fifth: Respond immediately to any indication of child pornography:

- Notify law enforcement (state and/or federal).
- If corporate policies and law enforcement allow it, hire forensic consultants to search the entire network, servers, backup tapes, and home office hard drives owned by the company, etc. for additional illegal material.
- Institute disciplinary measures against the alleged wrongdoing employee.

Conclusion

In short, the brave new electronic world brings with it new problems. As lawyers, we must strive to be ahead of the curve in addressing them. This summer, NYU did not need to address these issues because it avoided any possession of arguably illicit material. Your client or company may not have that option.

—❖—