www.mccanninvestigations.com
(800) 713-7670

Allegations of Child Pornography in the Workplace

November 19, 2013

Summary:
This paper discusses the very serious allegations of possession of child pornography in the workplace and how managers can best deal with the allegations and effect an in depth investigation. Due to the gravity of this type of allegation, the proper steps must be taken in order to ensure that managers conduct sound investigations in order to potentially damaging civil or criminal liability.

Allegations of Child Pornography in the Workplace

Although there are many potentially sensitive topics and issues that fall into the rubric of security or human resources managers' responsibilities, there is none more radioactive than an allegation of child pornography being seen or found in the workplace. How managers deal with the allegation and investigation has wide reaching implications for not only the affected employees but potentially for the company as a whole. How alleged child pornography is brought to management's attention isn't really important, what is important is that it always starts with a claim.

Topics to be discussed:

- Child Pornography Defined
- Issues to Consider Before an Allegation
- Steps to Take After an Allegation
- The Investigation Process
- Examples of Potential Entrapment

Child Pornography Defined

Federal Law

http://www.justice.gov/criminal/ceos/citizensguide/citizensguide_porn.html

Section 2256 of Title 18, United States Code, defines child pornography as any visual depiction of sexually explicit conduct involving a minor (someone under 18 years of age). Visual depictions include photographs, videos, digital or computer generated images indistinguishable from an actual minor, and images created, adapted, or modified, but appear to depict an identifiable, actual minor. Undeveloped film, undeveloped videotape, and electronically stored data that can be converted into a visual image of child pornography are also deemed illegal visual depictions under federal law.

Notably, the legal definition of sexually explicit conduct does not require that an image depict a child engaging in sexual activity. A picture of a naked child may constitute illegal child pornography if it is sufficiently sexually suggestive. Additionally, the age of consent for sexual activity in a given state is irrelevant; any depiction of a minor under 18 years of age engaging in sexually explicit conduct is illegal.

Federal law prohibits the production, distribution, reception, and possession of an image of child pornography using or affecting any means or facility of interstate or foreign commerce (See 18 U.S.C. § 2251; 18 U.S.C. § 2252; 18 U.S.C. § 2252A).

State Law
http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.43.htm

While there are some minor variances between different state statutes governing child pornography, they all basically share the same spirit. For purposes of this discussion the State of Texas will serve as the example.

Sec. 43.26. POSSESSION OR PROMOTION OF CHILD PORNOGRAPHY. (a) A person commits an offense if:
(1) the person knowingly or intentionally possesses visual material that visually depicts a child younger than 18 years of age at the time the image of the child was made who is engaging in sexual conduct; and
(2) the person knows that the material depicts the child as described by Subdivision (1).
(b) In this section:
(1) "Promote" has the meaning assigned by Section 43.25.
(2) "Sexual conduct" has the meaning assigned by Section 43.25.
(3) "Visual material" means:
(A) any film, photograph, videotape, negative, or slide or any photographic reproduction that contains or incorporates in any manner any film, photograph, videotape, negative, or slide; or
(B) any disk, diskette, or other physical medium that allows an image to be displayed on a computer or other video screen and any image transmitted to a computer or other video screen by telephone line, cable, satellite transmission, or other method.
(c) The affirmative defenses provided by Section 43.25(f) also apply to a prosecution under this section.
(d) An offense under Subsection (a) is a felony of the third degree.
(e) A person commits an offense if:
(1) the person knowingly or intentionally promotes or possesses with intent to promote material described by Subsection (a)(1); and
(2) the person knows that the material depicts the child as described by Subsection (a)(1).
(f) A person who possesses visual material that contains six or more identical visual depictions of a child as described by Subsection (a)(1) is presumed to possess the material with the intent to promote the material.
(g) An offense under Subsection (e) is a felony of the second degree.
(h) It is a defense to prosecution under Subsection (a) or (e) that the actor is a law enforcement officer or a school administrator who:
(1) possessed the visual material in good faith solely as a result of an allegation of a violation of Section 43.261;
(2) allowed other law enforcement or school administrative personnel to access the material only as appropriate based on the allegation described by Subdivision (1); and
(3) took reasonable steps to destroy the material within an appropriate period following the allegation described by Subdivision (1).

Put in plain English, child pornography is any sexual content involving a child under the age of 18, regardless of how it is displayed or stored. The only real difference between the federal statute and state law is that the federal statute requires the activity to involve an interstate or international component. In the age of the Internet, the vast majority of child pornography will fall into realm of federal law, but is typically prosecuted at the state level. This is due to the fact that Assistant U.S. Attorneys usually reserve federal prosecution for organized child pornography distribution or cases that are of an egregious nature.

Issues to Consider Before an Allegation Occurs

In the workplace as well as elsewhere, the most likely scenario of an allegation of possession of child pornography stems from digital content. While the Internet is a wonderful medium of information and data exchange, everyone is aware of the dark underbelly of voluminous sexually related content readily available at will. Combine this with the fact that one of the most common adult search terms is "teen sex", and the nexus is clearly there for a potentially false allegation by some unwitting outcry employee.

When brought to the attention of management one of the first questions that will likely be asked is, "If we look at it, how do we know if its child pornography or not?" This can extremely difficult to determine due to the fact that legal pornographers often use models that appear much younger than their biological age. In court proceeding, whether content is child pornography or not can be determined in multiple ways, with one of the most often used being expert testimony by a physician. (http://www.ndaa.org/pdf/Update_gr_vol1_no2.pdf) To list and explain all accepted methods used to determine age in child pornography investigations would take multiple pages, but suffice to say all of these methods are almost universally unavailable from within any corporation's internal capabilities. In the event that a method of determination is available internally, it would almost certainly be considered forensically unsound for any useful purpose.

Another likely question to be asked by management will be, "Why not just delete it and deal with the employee administratively?" While this option may seem quick and easy, it also could lead to both criminal and civil liability for the company as well as anyone involved in the decision. The government takes child pornography and destruction of related evidence almost as seriously as a murder investigation. Even though the decision makers may feel confident the items they're destroying aren't evidence of a crime, if they turn out to be incorrect the consequences could be severe.

While any pornography found in the work setting may be legitimate grounds for termination of an employee, an ultimately false allegation of possession of child pornography, which is subsequently referred to the police, could potentially expose the

company to disastrous civil action by the wrongfully accused party. This necessitates that companies facing an allegation take very careful steps to ensure that not only their ethical responsibilities to justice are served, but also their due diligence to safeguard their employees and company from false allegations are served as well.

In this maelstrom of societal responsibilities and corporate duties is where a competent and forensically capable private investigative firm can effectively fill the gap and provide an invaluable service for both the company and to society as a whole.

Steps to Take Once an Allegation is Made

While every situation will have its own nuances, there are certain steps that managers should take any time an allegation of this nature is made in the workplace.

As soon as an allegation is made, the manager handling the investigation should contact a competent digital forensics investigations firm and explain that an allegation was made. While there are a few preliminary steps that may be undertaken by someone knowledgeable in information technology, it is imperative to involve a digital forensic professional as early in the process as possible. This will ensure the evidence is handled in a forensically sound manner and shift the burden for the chain of custody into the hands of a person trained to handle digital evidence.

The primary step is to preserve potential evidence. This task may be completed by a competent information technology (IT) professional employed by the company, under the direction of the digital forensic technician. The IT employee should be directed to collect and preserve the suspected device or devices in a forensically sounds manner. This requires the IT personnel to:

- Locate the involved computers or devices.
- Take photographs of the work area and of the computer / device as it was found.
- Disconnect the power source to the computer/device immediately. If the computer is powered on, it should be immediately unplugged and NOT powered down in a normal fashion. If the computer is turned off, leave it turned off.
- Remove the battery or force a hard shut-down of a mobile device. If the device is a cell phone, the device should NOT be powered off normally, but rather the battery removed with it turned on. If the device doesn't have a removable battery, it should be forced to shut down in a hard manner. Failing all of this, the device should be put in "airplane mode", or all network connectivity disabled.
- Remove the device to a secure location under lock and key.
- Preserve "cloud" evidence. If there is "cloud" content on the company's network, a complete backup of the network should be made especially for evidence preservation.

- Document their actions and forward the report and photos to the associated manager.

If there are any uncertainties related to this step in the process, the manager should request this task be undertaken by the digital forensics technician. Mistakes in this part of the process can sometimes prove irrecoverable if done incorrectly.

In order to protect the integrity of the investigation, the accused employee should not be notified immediately. If necessary, the employee should be told his computer or device had to be taken out of service for repairs or updates.

Investigation Process

Chain of Custody

One of the most important aspects of any legitimate investigation is establishing the chain of custody of evidence. The chain of custody is the logging of the transfer and movement of evidence from the time of collection to the time the evidence is returned to the client. This process proves the evidence was handled in the correct manner and not tainted or changed in any way. In this example, the chain of custody would begin with the collection of the computers or devices by the Digital Forensics Technician from the assigned company manager.

Forensic Imaging

Once back at the digital forensics lab, the technician will make forensic images of all devices. A forensic image is a complete copy of all contents of the device's storage media. This copy includes some deleted information, as well as all unallocated space on the storage media. This process normally takes several hours, but can take much longer on large hard drives. Once all computers and devices are imaged, they can be returned to the client for secure storage.

Forensic Analysis

While there can be no analysis without imaging, the imaging is the easy part of the process. Forensic analysis is as much an art form as it is a science. Forensic analysis is the interpretation and documentation of the data collected in the imaging process. This step in the investigative process can take hours and sometimes days of work. In almost all cases when forensic analysis finds evidence of an accusation, it also uncovers additional evidence unknown to the client. This is likely due to the fact that the discovery, no matter what the accusation, is rarely the first or only time the target had used his or her computer to accomplish their nefarious designs.

Interviews

Interviewing witnesses and targets, while just good old-fashioned investigative work, is also just as important as the digital forensic analysis to the case. In almost all cases, the witnesses will be interviewed first. This is due to the fact that investigators want as much information as possible before talking to the accused. After all witness interviews are complete, the accused will be invited to speak with the investigator. The voluntary nature of the target interview is extremely important, but it doesn't keep the employer from making their participation a condition of continued employment.

Follow-up Forensic Analysis

While this step doesn't always occur, there are many times when witness and suspect interviews uncover information that requires additional analysis of the digital forensic images.

Final Report

After all evidence is collected and analyzed, and all witness and targets are interviewed, the final report can be prepared. In addition to a case summary, timeline, investigative report, background checks, the digital forensic reports are supplied as well. Often digital copies of all interviews will be supplied as well. The digital forensic report contains both a summary, which is easily understood, as well as the actual forensic report that is meant for evidentiary purposes only and is not easily understood by those outside the craft.

Because the digital forensics firm is hired by the client, all data recovered from the computers or devices remains the property of the client throughout and after the investigation is concluded. All remaining copies of case related digital content will be forensically wiped by the investigative firm or turned over to the client for their use and storage.

At the point of the final report, no matter the findings, the client will then need to engage with their legal counsel to determine the proper course of action on tackling the issue in the way to best protect their interests.

Examples of Potential Entrapment

WeAreChange.org
(http://www.youtube.com/watch?v=zislzpkpvZc)

On July 4, 2013, political activist Luke Rudkowski of WeAreChange.org received an email from an anonymous sender to his personal email address. Its notable that it went to his

personal email address because Mr. Rudkowski has maintained this email address since he was in high school, and it is not published publicly or widely known outside of close friends and family.

The email sender claimed to be a whistleblower wanting to give him sensitive information of a political nature. Fortunately for Mr. Rudkowski, his email provider, Yahoo, provides miniaturized previews of attached photos prior to being downloaded. Mr. Rudkowski looked closely at the previews and quickly realized the photos were not political at all but were of a sexual nature.

Fearing he was being set-up, Mr. Rudkowski did not open or download the attachments, and instead contacted a digital forensics professional. This technician trapped the email in a digital sand-box and examined its contents. It was confirmed the attachments were explicit child pornography, and were sent from the anonymous email service known as Tor Mail.

Had Mr. Rudkowski opened or downloaded the attachments, his computer would have then contained child pornography subjecting him to possible criminal and civil penalties. It is easy to see how this scenario could play out in the work place setting and potentially be used to entrap an innocent person into being a suspected pedophile.

Padnaunite.Org
(http://www.youtube.com/watch?v=XYVvuDRstDw)

About three weeks after the above incident on July 25, 2013, another political activist, Dan Johnson, received an email purported to be from a known friend and colleague, Stewart Rhodes. The email had Mr. Rhodes name as the sender and even had Mr. Rhodes normal signature block in the body.

This email had attachments, but they were all in Adobe PDF format, which do not provide a preview. Luckily, Mr. Johnson observed the email emanated from the Tor Mail service, which was inconsistent with previous contacts with Mr. Rhodes. Mr. Johnson knew about the above episode involving Mr. Rudkowski and referred this incident to an internet security firm for forensic processing. The internet security firm later confirmed the PDF attachments contained child pornography.

This case is even more disturbing than the first for two reasons. First, the sender pretended to be a person known to the target, which would normally make someone less suspicious of the email contents. Secondly, the sender concealed the illegal pornography in a file format that made early detection less likely.

Direct Placement of Content

Internet security expert, Brett Dearman, a digital forensics professional with McCann Investigations in Houston, Texas, states that there multiple ways for a person to surreptitiously place information on a target's computer.

One way would be to infect the computer with a virus that would either download the content from another location or allow back-door access for the content to be directly placed on the target's computer. This virus could be hidden inside an otherwise innocuous email, or placed directly on the target's computer via a thumb drive. Another way would be to directly place files on the target's hard drive and then conceal the placement by manipulation or deletion of log files.

The most important aspect of these methods is that even if the person placing the content does nothing to conceal their activities, once the illegal content is placed on the target's computer the target becomes vulnerable to being investigated or convicted for a serious felony.

Mr. Dearman believes this makes proper computer security protocols and prompt forensic investigation (once an allegation is made) paramount to protecting employees from being wrongly accused.

Conclusion

Due to the clearly radioactive nature of an allegation of child pornography in the workplace, managers must consider the issues in advance of their actual happening so they're prepared to take immediate and proper steps to protect all parties involved. Should a company find themselves facing an issue like this, it is only through the engagement of a qualified investigative firm that they'll be armed with the proper tools and advice to effectively navigate the minefield of potential civil and criminal liability.

For more information, contact McCann Investigations at: (800) 713-7670

McCann Investigations is a fully licensed Private Investigations firm with offices in Texas, New York and New Jersey. McCann Investigations computer forensics experts find and expose the digital fingerprints left behind in emails, internet histories, files and networks. McCann Investigators are fully licensed and have provided expert testimony on various matters in Texas, New York and New Jersey. Cases in which McCann Investigators have testified or investigated include cases involving divorce, child custody, fraud, embezzlement, intellectual property theft, network breach, non-compete enforcement, and claims of child pornography.

McCann Investigations is a one-source solution for comprehensive case management. Often investigations go beyond digital forensics and when this happens McCann utilizes traditional private investigations tools such as surveillance, background investigations and undercover work to optimize the gathering of evidence. McCann Investigations was

founded by Jack McCann over 25 years ago in New York, New York, and has provided private investigative services to law firms, public companies, private companies, government agencies, and individuals.