THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 9 | Number 4 Article 3

2014

Fighting Child Pornography: A Review of Legal and Technological Developments

Jasmine V. Eggestein
Nova Southeastern University

Kenneth J. Knapp
The University of Tampa

Recommended Citation

Eggestein, Jasmine V. and Knapp, Kenneth J. (2014) "Fighting Child Pornography: A Review of Legal and Technological Developments," *Journal of Digital Forensics, Security and Law*: Vol. 9 : No. 4 , Article 3.
DOI: https://doi.org/10.15394/jdfsl.2014.1191
Available at: https://commons.erau.edu/jdfsl/vol9/iss4/3

FIGHTING CHILD PORNOGRAPHY: A REVIEW OF LEGAL AND TECHNOLOGICAL DEVELOPMENTS

Jasmine V. Eggestein
Nova Southeastern University
Fort-Lauderdale-Davie, Florida 33314
je713@nova.edu

Kenneth J. Knapp
The University of Tampa
Information & Technology Mgt. Dept.
Tampa, Florida 33606
kknapp@ut.edu

ABSTRACT

In our digitally connected world, the law is arguably behind the technological developments of the Internet age. While this causes many issues for law enforcement, it is of particular concern in the area of child pornography in the United States. With the wide availability of technologies such as digital cameras, peer-to-peer file sharing, strong encryption, Internet anonymizers and cloud computing, the creation and distribution of child pornography has become more widespread. Simultaneously, fighting the growth of this crime has become more difficult. This paper explores the development of both the legal and technological environments surrounding digital child pornography. In doing so, we cover the complications that court decisions have given law enforcement who are trying to investigate and prosecute child pornographers. We then provide a review of the technologies used in this crime and the forensic challenges that cloud computing creates for law enforcement. We note that both legal and technological developments since the 1990s seem to be working to the advantage of users and sellers of child pornography. Before concluding, we provide a discussion and offer observations regarding this subject.

Keywords: child pornography, cybercrime, cloud forensics, encryption, U.S. federal law

1. INTRODUCTION

In a famous speech, renowned Supreme Court Justice Oliver Wendell Holmes said, "It cannot be helped, it is as it should be, that the law is behind the times" (Library of Congress, 2010). In the digital age, these words ring truer than ever. In our hyper-connected and ever-evolving technological world, it seems increasingly challenging for the law to keep up with today's technology. This is especially the case with regards to the crime of child pornography.

Child pornography has been the number one child exploitation offense since the early 2000's (Motivans & Kyckelhahn, 2007). While numbers measuring the usage of illegal child pornography are difficult to assess, some have placed the sexual exploitation of children on the Internet to be a $20 billion black market globally (Brockman, 2006). Some assess that the legal and larger pornography industry generates more revenue than many of the largest technology companies including Microsoft, Google, Amazon, eBay, Yahoo! and Apple combined (Family Safe Media, 2013), whereas others conservatively measure the industry at about the size of the U.S. bottled water market (Spencer, 2012). In the United States, an estimated 50,000 people are believed to be actively trading illegal images of child pornography at any given time based on downloads of known prohibited videos and photographs that can be tracked to individual computers (Johnson, 2014). An investigative reporter claimed the vast majority of subscription-based child porn sites operated by a Russian cybercrime organization consists of Americans, paying about $40 per month. These sites are often called “strawberry and Lolita” sites in the Russian criminal underground. One network of these sites attracted more than 100,000 visitors per day while making over $5 million per month (Krebs, 2014). Moreover, the clearance rate for this crime is very low; it is estimated that one in every 15 people caught viewing child pornography is actually arrested (Greenwood, 2013).

The growth of the Internet with its functionality and conveniences has proven immeasurably beneficial to many industries and society at large. However, the expansion of cyberspace has also made the production and distribution of child pornography much easier (Chawki, 2009). In addition, technological developments have allowed offenders to create this material surreptitiously, increasing law enforcement’s difficulties in apprehending and prosecuting offenders. Child pornography is a type of sexual exploitation. U.S. federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor (less than 18 years of age) that includes engaging in graphic bestiality, sadistic or masochistic abuse or sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, whether between people of the same or opposite sex (Cornell LII, 2013b). U.S. federal law prohibits the production, distribution, importation, reception, or possession of any image of child pornography (Department of Justice, 2013). Digital child pornography is also referred to as “online child sexual abuse” in the literature in the United Kingdom and “child sex abuse images” within the United States.

This paper will explore the evolution of both the legal and technological environments surrounding the child pornography market. It will end with a discussion about the relationship between the technological and legal environments along with a section on the contributions and limitations of the paper. A chief goal of our paper is to create more awareness, particularly among policy makers, of the legal and technological challenges faced by law enforcement in fighting child pornography.

2. LITERATURE REVIEW

The area of child pornography is not the only field in which technology seems to outpace the legal realm. With new technologies impacting the fields such as medicine, oil exploration, and the relationship between surveillance and privacy, the law will naturally be reactive in addressing related legal issues. Where computing technology is concerned, however, the law seems especially behind the times.

Our review may be illustrated as a timeline or framework comparing and listing the major legal and technological events relating to digital child pornography. Figure 1 shows how significant technological developments and enablers are frequent occurrences since the 1990s, whereas at the federal level of U.S. law, significant court cases and laws impacting child pornography are less frequent. In this paper, we will unpack this timeline describing first the legal dimension followed by the technological dimension also covering forensics and how they relate to the subject of digital child pornography. Thus, Figure 1 provides an overview and guide of the paper hitting the major points on the temporal scale. The remainder of this paper covers the timeline material in greater detail.

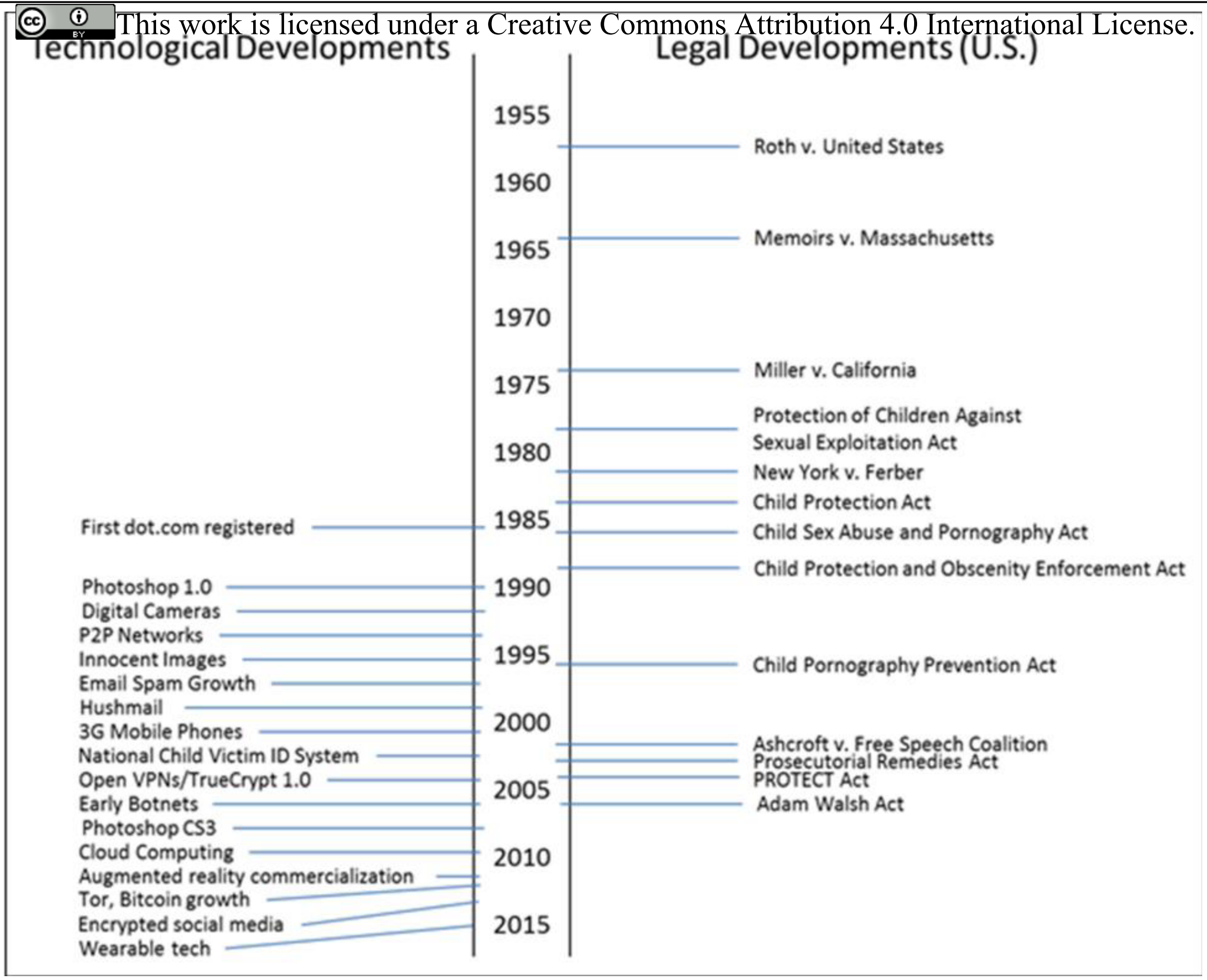

Figure 1. Timeline of Major Technological and Legal Events Affecting Digital Child Pornography.

2.1 Legal Environment

Prior to 1957, the ruling authority in the United States on the production and distribution of materials considered to be obscene came from an English common law termed the “Hicklin Test”. In an 1868 case, *Regina v. Hicklin*, the English court held that all material tending "to deprave and corrupt those whose minds are open to such immoral influences" was obscene, regardless of its artistic or literary merit (*Regina v. Hicklin*, 1868). In 1896, the United States Supreme Court based their opinion in *Rosen v. United States* on the Hicklin Test, thereby officially adopting it as the standard for obscenity (*Rosen v. United States*, 1896). The Hicklin Test remained the standard until 1957, when the Supreme Court adopted a more defined test for obscenity, specifically: "whether to the average person, applying contemporary community standards, the dominant theme of the material taken as a whole appeals to prurient interest" (*Roth v. United States*, 1957). Nine years later, the Court further narrowed this definition to include only those materials which are to be considered "patently offensive" and "utterly without redeeming social value" (*Memoirs v. Massachusetts*, 1966).

In 1973, the United States Supreme Court again changed its definition of “obscene materials” stating that materials “judged to be obscene by the average person, applying contemporary community standards" would not be protected under the

First Amendment. However, addressing the call to protect the freedom of expression, the Court sought to limit state statutes designed to regulate obscene materials and more clearly define "obscenity". In order to do so, the court established a three-pronged test which is still used today. The test includes a set of criteria which must be met in order for a work to be legitimately subject to state regulation: (1) whether the average person, applying contemporary community standards (not national standards, as some prior tests required), would find that the work, taken as a whole, appeals to the prurient interest; (2) whether the work depicts or describes, in a patently offensive way, sexual conduct or excretory functions specifically defined by applicable state law; and (3) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value (*Miller v. California*, 1973).

Four years after the Miller decision, the first federal law against child pornography was enacted: the *Protection of Children Against Sexual Exploitation Act of 1977*. At this time, Congress expressed alarm that child pornography and prostitution had become a national problem and was systematically operated by criminal organizations. This act allowed for the prosecution of individuals found to manufacture or deliver child pornography, but required that the materials be considered obscene under the Miller test and only protected children aged sixteen or younger. The *Child Protection Act of 1984* removed these restrictions and required manufacturers of pornography to keep records ensuring that their performers were of legal age. This Act increased the age of majority from sixteen to eighteen while making criminal all production of child pornography regardless of whether it was produced for transportation in interstate commerce. The *Child Sexual Abuse and Pornography Act of 1986* made advertising child pornography illegal and enabled victims of child pornography to bring civil suits against offenders (Cornell LII, 2013a; Kwan, 2009).

Legislation to specifically criminalize the distribution or transportation of digital child pornography via computer was contained in the *Child Protection and Obscenity Enforcement Act of 1988*. This Act also required the makers of explicit portrayals to preserve individually identifiable records relating to every performer in the portrayals. The *Child Pornography Prevention Act of 1996* criminalized virtual images of child pornography that contained no human actors, banning images and videos in which actors appeared to be children (Jones, 2011) by interdicting, "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture" that "is, or appears to be, of a minor engaging in sexually explicit conduct." Further, Congress expressed the concern that digitally produced images of children would interfere with the prosecution of child pornographers because as technology evolved, it would be progressively difficult to determine which images were produced using a child and which were not (Kwan, 2009). As a response to the United States Supreme Court decision in *Ashcroft v. Free Speech Coalitio*n in 2002, Congress created the *Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act of 2003*, which made illegal any visual depiction of minors engaged in sexually explicit behavior where that image depicts an act that is itself obscene, as defined under the Miller test (Burke & Ford, 2011). Revisions made to this Act in 2008 also criminalize "child pornography that is an adapted or modified depiction of an identifiable minor" (*PROTECT Act of 2008*). Finally, the *Adam Walsh Act of 2006* provided enhanced criminal penalties in cases in which the defendant can be shown to have put the victim through a process called "grooming". This involves providing child pornography to a minor with the intent of encouraging the child to engage in the sexual behavior (Moore, 2011).

While the first federal law criminalizing child pornography was enacted in 1977, it took several years before the courts began upholding these statutes. The first child pornography case brought before the U.S. Supreme Court was *New York v. Ferber.* In this case, the Court was asked to determine whether the First Amendment protected an individual's right to manufacture and distribute images and videos of child pornography. The Supreme Court ruled that the need to protect the emotional and physical well-being of the child superseded First Amendment protections in that distribution of these materials is related to child abuse (*New York v. Ferber*, 1982). Eight years later, in *Osborne v. Ohio*, the Supreme Court held that the First Amendment does not disallow states to outlaw not only the production and distribution of child pornography, but also the mere possession and viewing of the materials. The Court's reasoning behind the opinion was not to prohibit or limit free speech, but rather to decrease the market for child pornography and thereby protect the children involved (*Osborne v. Ohio*, 1990).

In relation to virtual child pornography, the Supreme Court heard *Ashcroft v. Free Speech Coalition* in 2002. The Free Speech Coalition is a non-profit, pornography trade association. In this case, the Court ruled that law enforcement officers who investigate child pornography are responsible for providing proof that the images seized are those of an actual child. This nullified portions of the *Child Pornography Prevention Act of 1996*, which had previously criminalized the possession or viewing of images containing those perceived to be minors engaged in sexual activity. The Court made this decision in an effort to preserve the First Amendment freedom of speech stating that while child pornography is not protected by the First Amendment, virtual child pornography, produced without the use of actual minors, is protected (Hatch, 2012, note 16.). This decision has had significant repercussions for law enforcement and prosecutors seeking to apprehend pedophiles (*Ashcroft v. Free Speech Coalition*, 2002; Moore, 2011). In reaction to the decision, former Attorney General John Ashcroft stated that the court had made the prosecution of child pornographers "immeasurably more difficult" while stating, "I am undeterred in my resolve to do all that I can to protect our children from the pornographers and other predators who would prey on their innocence." The decision was a victory for civil libertarians who feared the Supreme Court would use Internet pornography concerns to narrow the interpretation of the free-speech clause of the First Amendment (Mauro, 2002).

These U.S. Supreme Court cases have significantly impacted lower court decisions across the United States. For instance, a 2013 Texas court decision sited the 'Ashcroft' and 'Reno' decisions. In the 1977 Supreme Court case, *Reno v. ACLU*, the Court struck the anti-indecency provisions of the *Communications Decency Act of 1996*, which prohibited the dissemination of indecent, and not simply obscene, communications to children over the Internet (*Reno v. ACLU*, 1997). The Ashcroft and Reno cases have been used to void state laws that deemed it illegal to communicate in a sexually-explicit manner with a person believed to be a minor with the intent to gratify one's sexual desire. The Texas court, citing these cases, struck down a state law in a concern that the law was overbroad and may have been used to ban literary works that would enrich children (Ex Parte John Christopher Lo, 2013; Hilden, 2013).

2.2 Technological Environment

In the 1980s, child pornography trafficking was nearly eliminated in the United States due to targeted campaigns of law enforcement. The production and distribution of these materials was difficult and perpetrators were numerically few and isolated in society. Today, the child pornography market has expanded rapidly and substantially since the advent of the Internet (Department of Justice, 2013). Law enforcement officials often struggle to maintain a proactive approach to fighting this crime. Offenders are constantly finding innovative methods of committing their crimes, particularly with the goal of generating more revenue at a lower risk. To the advantage of child pornographers, information technology is advancing at an unprecedented rate providing new ways to produce and secretly distribute illegal material. Low-cost innovations such as smart phones and thumb drives have made it easier for offenders to collect, store and trade child pornography. Electronic forums such as social media and virtual worlds have given criminals additional ways to market their imagery. Furthermore, advanced technologies such as strong encryption and peer-to-peer networking have made it increasingly difficult for law enforcement to apprehend child pornographers. In this section, we will cover these topics and the most significant technology advancements that have enabled online child pornography.

2.2.1 Graphic Editing Software

The evolution of Photoshop alone has provided multiple tools for rapid production of higher resolution child pornography. Today, Photoshop is the de facto standard graphics and digital imaging software; it is used across the world in various industries and different contexts. The first version of Adobe's Photoshop was released in 1990 and included only basic photo-editing options. While Photoshop 1.0 was written for Macintosh computers only, Adobe released Photoshop 2.5 for the Windows operating systems in 1992. An upgrade significantly benefitting child pornographers was released in 1999: Photoshop 5.5 allowed for the integration of their software with web hosting, making it easier to use the Internet as a distribution channel. Photoshop Creative Suite CS3 in 2007 included major improvements to image editing options, including the introduction of the Quick Select tool and the Clone Source palette (West, 2010), enabling the overlaying of different sources that clone locations and orientations. The 2012 release of CS 6.0 included enhanced layering and masking tools, a lighting effects gallery, and increased support for web integration (Adobe, 2012; Bjango, 2012; Creative Bloq, 2012) with newer versions to offer cloud hosted software. These capabilities allow for advanced manipulation of digital imagery and media that can make it difficult for law enforcement to prove whether a digital image is that of an actual child. Continued advancement of photo manipulating software, graphics, and multi-media technologies will make both altered photographs of human beings and computer-generated images indistinguishable from raw images of an actual human person.

2.2.2 Strong Encryption

It is widely recognized that properly used modern encryption is exceedingly difficult to crack, making law enforcement's job of deciphering encrypted child pornography evidence nearly impossible without knowing the secret key. Encryption tools that are widely available from the Internet are used in various ways in the child pornography underground. Criminals will visit web servers with encrypted proxy services and view and transport illegal pictures and videos via encrypted virtual private networks. They also use web-based email services such as Hushmail that use strong PGP encryption that is difficult to defeat and designed to keep communications secret (U.S. Sentencing Commission, 2012). Media may be secured with disk encryption products on the open source market. Communication may occur via encrypted social media. Many of these encryption tools use industry standards such as Secure Sockets Layer/Transport Layer Security (SSL/TLS), the Advanced Encryption Standard (AES) and the Triple Digital Encryption Standard (3DES) enciphered with robust, pseudo-random keys, making cryptanalysis (i.e., code-breaking) difficult, if not impossible. Today's encryption technology is so strong that law enforcement often must find ways to get around the encryption. During searches, for example, law enforcement can use ruses such as pretending to repossess an offender's car to draw the person out of his house before carrying out the search and/or arrest warrant so that the computer can be accessed by law enforcement in an unencrypted state (Cryptome, 2010).

2.2.3 Peer-to-Peer Networking

New developments are allowing for easier, faster, and increasingly untraceable methods of digital production and distribution of child pornography. Distribution has now moved beyond older electronic methods such as visiting web sites or sharing email attachments. Today, significantly advanced distributive technologies include peer-to-peer networking and cloud computing. Peer-to-peer networking involves the linking of two or more computers in order to share digital files, including music or video. Peer-to-peer networks are a popular mechanism for the criminal acquisition and distribution of many types of illegal media, including child pornography. Researchers, observing two different file sharing platforms over a one year period, detected about 2.5 million distinct peers from over 100 countries dealing hundreds of thousands of files verified as child pornography (Hurley et al., 2013). One file sharing tool that has been used in distribution is called Ares (Leon & Gonzalez, 2013), which is an open-source, peer-to-peer file sharing application that uses its own decentralized network while supporting the BitTorrent protocol. Together, these technologies allow criminals to automate domain name service updates to hide web sites that host illegal activities such as child pornography and identity theft, among others (ICANN, 2008). Illegal media is also routinely distributed using hacked or zombie computers that may be part of a botnet (a malicious network of compromised computer devices) operated by an organized crime syndicate. Unknown to the user, a compromised computer can then store and distribute illegal materials and serve other functions, such as purchasing web domains for the criminals. The trafficking of this material on peer-to-peer networks appears widespread, representing an enormous challenge to law enforcement.

2.2.4 Cloud Computing Services

Cloud computing is raising new challenges for digital forensic examiners, including those investigating digital child pornography. Cloud computing utilizes hosted services over the Internet, rather than installing a service directly onto a machine. The definition of cloud computing from the National Institute of Standards and Technology (NIST) states, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011). While the cloud can be incredibly valuable for legitimate users, it can cause difficulties for investigators who deal with digital evidence. In a cloud computing system, files run on virtual machines, which use volatile data. Volatile data cannot sustain without power, and is thereby deleted when a virtual machine terminates. A virtual machine may terminate periodically, or may be forced to terminate under an attack, such as a denial-of-service attack. As soon as the virtual machine terminates, any volatile data is erased. This means there is no remote access to the deleted data. Another difficulty in performing digital forensics in the cloud is that storage resources and locations are shared among users. Thus, various user data can be found on the same cloud server, making separation difficult without the potential to unlawfully violate the privacy of others. This creates a challenge in establishing a connection between any particular data and the alleged offender (Zawoad & Hasan, 2013). Further, cloud computing allows users to store information using the Web, and thereby forego traditional geographical limitations, possibly causing the location of the physical data to be unknown. These problems associated with cloud and virtual technologies make it difficult and sometimes even impossible to conduct traditional digital forensics (Coty, 2014). Offenders may store information on a server located abroad, where legal requirements and limitations may be drastically different from those within the United States. As cloud forensics are a relatively new area, there are currently few established forensic tools and procedures for acquiring digital evidence. To sum-up, today's cloud computing architectures are designed for cost-effectiveness through efficient computing and economies of scale and not for digital forensics.

2.2.5 Anonymizers & Hosting Services

Today, a wide array of new programs offer anonymous hosting services on the Internet. A prominent example, once an acronym for "The Onion Router" network, Tor leads Internet traffic across a global network of relays to hide a user's activity and whereabouts from surveillance and discovery. It is believed that Tor, with its layers of routing and encryption, has prevented surveillance organizations like the U.S. National Security Agency (NSA) from easily reading its traffic. In slides provided by former NSA contractor Edward Snowden, the NSA stated, 'We will never be able to de-anonymize all Tor users all the time but with manual analysis we can de-anonymize a very small fraction of Tor users" (The Guardian, 2013). Allegedly operated by Eric Eoin Marques, Freedom Hosting has been accused of storing large amounts of child pornography on the Tor network. Freedom Hosting was a provider of Tor hidden services, which are sites using the top-level domains of ".onion". The site was accused of hosting 95 percent of the child pornography on the Tor network with sites attracting thousands of users (Poulsen, 2013). The take-down of Marques, a dual U.S.-Ireland citizen described as the "largest facilitator of child pornography on the planet," provided a look into the dark side of the Tor network (Poulsen, 2014).

Criminals can also compromise legitimate business servers in order to host illegal material. Child pornography dealers can hack into vulnerable servers and web sites to create orphan folders that cannot be accessed from a site's navigation system of links and menus. Unsuspecting small to medium sized businesses (SMBs) that do not usually maintain savvy technology and security professionals on staff can be especially vulnerable. In one case, a furniture store was hosting hundreds of images of extremely violent child abuse in an orphan folder that was only accessible to those who knew the direct web address (ITV, 2013). These hacked sites also serve as a redirect destination, tricking visitors to legal (adult) pornography sites into clicking on a disguised web link that takes their browser to the illegal child imagery. The criminal's goal would be to get visitors interested in viewing more and possibly addicted to the child depictions. Moreover, the use of orphan folders hosted on web sites is a way to circumvent any pornography-blocking content filters, since the web address would be that of a legitimate business (Internet Watch Foundation, 2013). SMBs need to be aware of these dangers and secure their servers to prevent this type of illegal activity.

2.2.6 Social media

Child pornography is often traded using electronic forums, newsgroup advertisements, social media, and email spam (Wikileaks, 2009). Social media sites such as Twitter and Facebook can be used to exchange illegal digital content. In one case, Google+ was accused by Consumer Watchdog that online child predators used its service. In a press release, the organization claimed that "hundreds of suspected pedophiles and sexual predator rackets who traffic in highly sexual and exploitive images of their child victims appear to be both using Google+ and posting these images to the social network" and that "Google+ is also being used by suspected pedophiles to troll for underage users in order to engage them in sexually suggestive/sexually explicit online conversations, texts, and even videos." (Consumer Watchdog, 2013).

It has been reported that public Twitter accounts have been used to share imagery of a young boy being raped (Barfe, 2012). Another case involved an individual who used Tumblr to find and share child pornography described by a local district attorney as images of "...children being raped...this is children being sexually assaulted...(images) dating back to the 70s and 80s" and traded by people who view the images and thus create a market demand for more imagery. In this case, the person was caught, found guilty and sentenced to three years in prison. After a local media request, Tumblr made a statement, saying, "Tumblr does not tolerate inappropriate content involving minors, and has taken aggressive efforts to prevent and combat child exploitation. We remove or prevent upload of such content immediately upon detection, and report instances of child exploitation to the National Center for Missing and Exploited Children" (Dowty, 2013).

In other instances, social media may be used by predators to make contact with victims so they can be groomed for abuse to include the creation of child pornography. To find and potentially groom victims, predators will go to the websites that children visit, including chat rooms, gaming sites and social media sites. Additionally, predators go to social media sites of individuals that have publically open profiles looking for photographs of children posted by parents, for example. Seemingly innocent photos of a child perhaps taking a bath or in the sand at the beach can be shared and traded on the "dark web". In addition, technologies such as the above mentioned Photoshop can enable criminals to insert these innocent images of real children into a scene depicting sexual acts. Other social media sites such as Wickr that enable strong encryption and provide short-lived text messages may also provide new challenges to law enforcement and opportunities for predators as they find ways to manipulate social media services.

The Center for Missing and Exploited Children has been on the leading edge in the United States in the fight against child pornography. They operate an office in Silicon Valley to help educate technology leaders and organizations about how the Internet is used in sex trafficking. They also tap into mainstream social networks, including Facebook and Instagram, looking for evidence of illegal content. Many digital photographs, for example, carry detailed metadata that can identify the application used to distribute a photograph, the GPS location coordinates, time taken, and even the account name of the person who posted an image (Bowles, 2014). This metadata can then be given to law enforcement.

2.2.7 Virtual Worlds

A type of massively multiplayer online game (MMOG), a virtual world is a simulated, computer-generated setting that is based in the digital realm (i.e., cyberspace). These virtual environments have faced moral criticisms to include accusations of child abuse and child pornography in virtual depictions of avatars, some that may appear as minors or have childlike features. While considered 'protected speech' by the U.S. Supreme Court, some European countries have given more attention to virtual child rape and sexual abuse in virtual worlds. In Germany for example, prosecutors investigated an incident where anonymous players were buying sex with other players posing as children, as well as selling child pornography (Connolly, 2007). Linden Labs, which operates the virtual world site *Second Life*, responded by clarifying that, "real-life images, avatar portrayals, and other depictions of sexual or lewd acts involving or appearing to involve children or minors are not allowed within *Second Life*...Any images, chat, or other conduct that leads us to believe actual minor children are involved will lead to swift action, including reporting to the appropriate authorities" (*Second Life* Wiki, 2014).

A related technology is *augmented reality*, which produces computer-generated imagery, graphics, and depictions that overlay a person's view of the real world; reality is integrated with aspects of a virtual world. A fear exists that the pornography industry will lead the popular use of augmented reality and will integrate it with wearable technology. Wassom (2012) states that, "You can always count on the military and the pornography industry to push technology forward" and that "wherever society finds pornography, child pornography is not too far behind". A logical expectation is that a product like Google Glass or a competing product could enable child predators to augment their reality for nefarious and pornographic purposes. As of this writing, Google has limited many operations on Google Glass in an attempt to prevent users from distributing pornographic materials via the new technology. For example, Google Glass does not allow users to search for pornography or view pornographic websites. However, Google is not able to place restrictions on the types of videos users can record and share (Kleinman, 2013). An app exists that allows users to record sex acts from both partners' point of view and then watch or even share the videos directly from Google Glass (Thomas, 2014). These types of applications extend the viewing experience of any video into the realm of virtual reality. While an advancement for modern technology, it also gives rise to further questions and implications regarding the potential for digital child abuse.

2.2.8 Payment Systems

New avenues exist today for criminals to anonymously exchange currency. Traditional methods such as credit card payment systems are proactively scanned to ban child pornography merchants from the payment card systems. Moreover, many credit card companies such as Visa work with law enforcement to identify these pornography merchants (MacCarthy, 2010). However, systems such as Bitcoin enable greater anonymity in dealing with currency exchange. Known as a cryptocurrency, Bitcoin is based on a peer-to-peer payment arrangement that uses strong encryption for money transfers. Bitcoin has been scrutinized due to its use in illicit activity and may facilitate the sale of child pornography (Aizescu, 2014). Other cryptocurrencies are emerging with various levels of anonymity. Toward the future, it is likely that organized crime will gravitate towards one that offers the best protection from identification.

2.3 Digital Forensics: Using Technology to Investigate Crimes

Having reviewed both the legal and technological developments involving child pornography, we now extend our examination to digital forensics as it applies to this subject. It is not only the criminals who take advantage of modern and accessible information technology, but law enforcement also uses technology to investigate and apprehend online sexual exploiters. During investigations, law enforcement must assess if an image is that of an actual child. Because of ongoing advancements in image creation and editing tools, it has become difficult to visually distinguish between real and fake images. For this reason, the field of digital forensics and its use in child pornography cases is developing rapidly.

Three main methods that digital forensic investigators use to detect whether an image has been altered include tampering detection, hidden messages recovery, and source identification (Rocha, Scheirer, Boult, & Goldenstein, 2011).

Tampering detection uses techniques such as pixel examination to detect evidence of cloning, healing, retouching and splicing. Pixel examination involves using digital tools to ensure that the image originally included in the picture has not been modified, nor were images added. This technique is accomplished by examining enlarged images and comparing the pixels, looking for any blurring or smudging that would indicate doctoring (Moore, 2011). However, pixel examination may soon be rendered useless if image enhancement technologies continue to improve. In an effort to combat this trend, a relatively new branch of digital forensics named Triage intends to provide investigators with advanced intelligence through digital media inspection, and describes a new interdisciplinary approach that merges digital forensics techniques with machine learning principles and data mining algorithms (Fabio & Tacconi, 2013).

Hidden message detection involves the use of robust algorithms to detect the act of stenography, or camouflaging information within a seemingly innocuous message. Child pornographers often use stenography to conceal an illegal image by embedding it within another image, giving it a harmless appearance (Rocha, Scheirer, Goldstein, & Boult, 2008). Digital forensic experts with advanced algorithmic knowledge are able to perform forensic steganalysis to detect and recover hidden messages. However, forensic steganalysis is often only able to confirm the presence of a hidden image, but is not able to recover the hidden image (Rocha et al., 2011). In many cases of child pornography, law enforcement is unable to recover proof that images are of an actual underage human and therefore cannot prosecute the offender.

Lastly, source identification involves the use of forensics software which allows law enforcement officials to compare digital images with images from a known child pornography database. These source databases can be critical in investigations since they are often the only proof of an offense due to the lack of forensic software that can estimate the age of humans in digital images (Prat, Psych, Chudzik & Réveillère, 2013). Using mathematical algorithms, the images in the database are assigned a hash value, or digital signature. Every file that has the same data will contain the same hash value. Comparing hash values can provide sufficient evidence that an image is an actual piece of child pornography, rather than an altered adult image (Federal Bureau of Investigation, 2003). One important tool that uses this method is the Immigration and Customs Enforcement's database of child pornographic images. The National Child Victim Identification System (NCVIS) was launched in 2002 and contains images contributed by local, state, federal, and international law enforcement organizations. Law enforcement officers submit copies of seized child pornography images to Child Victim Identification Program (CVIP) analysts, who then review the images and videos to determine whether these files contain previously identified child victims. As of 2012, analysts had reviewed more than 77 million images and videos (National Center for Missing and Exploited Children, 2013). This number has increased to more than 100 million in the past two years (Johnson, 2014). The NCVIS serves two purposes: (1) to confirm that a pornographic image involves an actual child in order to obtain a conviction in court, and (2) to identify and rescue these children (U.S. Department of Homeland Security, 2009). In the twelve years since the creation of CVIP, about 5,400 victims have been identified (Johnson, 2014). While the NCVIS database is exhaustive, individuals who possess and distribute child pornography often manufacture their own images, thereby diminishing the value of these types of databases. This is becoming increasingly common with the consumer availability of digital cameras and image modification software.

Another source database is the FBI's online child exploitation investigation agency system called “Innocent Images”. It is a multi-agency investigative operation that focuses on combating the proliferation of child pornography and exploitation not only in the United States, but worldwide (Federal Bureau of Investigation, 2012). Since its inception, Innocent Images has continued to grow exponentially, seeing an increase from approximately 80 pending cases in 2001 to roughly 5,900 through 2012. Also, between the years of 2001 to 2011, Innocent Images led to over 11,400 child exploitation convictions (Federal Bureau of Investigation, 2013). Google has joined the fight against child pornography as well and has begun to proactively scrub the results for over 100,000 queries in over 100 languages that might be related to child abuse and pornography. In reviewing photos deemed to be child pornography, Google assigns a digital fingerprint to each photo (Schmidt, 2013) that is similar to the NCVIS database method.

One of the more creative methods law enforcement has started using to apprehend offenders is through investigative stings called “honeypots” or more elaborate “honeynets” that consist of multiple interconnected honeypot sites. A honeypot is typically a web server configured to look attractive to an attacker when in fact the server is set to detect and identify the attacker. In the context of this topic, a honeypot is a fake web site offering or suggesting to offer child pornography in a way to lure a person with malicious intent to the web site. These honeypot sites may be operating on cloud servers. Once at the honeypot site, if the suspect continues to proceed through a sufficient number of pages, he would be informed that he had committed an offense and may face criminal charges and an arrest. Law enforcement may use other online techniques to entice a criminal to visit the honeypot, such as online chatting with agents posing as minors (U.S. Sentencing Commission, 2012).

Cloud platforms, while advancing the capabilities of child pornography distributors, also give local police departments the benefit of using large-scale computing, which represents a forensics opportunity not previously available. In the constant chase to adapt to the latest technologies, local police will need to utilize cloud services. Many of the steps involved in digital forensics are tasks that benefit from large-scale computers–something that is not readily available at most local police departments. Eventually, legislation will need to be passed regulating cloud service providers, requiring service level agreements and record-keeping to facilitate digital forensics (Sammons, 2012) for as much as the technology will allow. However, it may be several years before the law catches up to technology in this area.

3. DISCUSSION & COMMENTARY

Having provided a review of the literature containing the major developments of the legal and technological environments as it impacts child pornography, we now offer a discussion about the topic.

The production and distribution of child pornography has exploded in the Internet age. As the Internet continues to permeate global society, child pornography will become more commonplace. Debate exists on the degree that legal pornography is addicting (see Franklin, 2014). Some experts argue that a pornography viewer’s compulsion is similar to that of harmless ‘addiction’ to chocolate, while others see it as destructive to marriages and dangerous to the children who view this material while forming their character. Yet, some studies have concluded that pornography addiction leads to the same brain activity as other potent drug addictions (Withnall, 2013). In a 2013 Cambridge University study, lead scientist Dr. Valerie Voon stated, “When an alcoholic sees an ad for a drink, their brain will light up in a certain way and they will be stimulated in a certain way. We are seeing this same kind of activity in users of pornography." On the more focused topic of this study, the dangerous behavior of the addict clearly results in the abuse of children by creating a market for child pornographic imagery. Research results indicate that wide access to the Internet has enabled persons to access child pornography who would never have been able to previously. We conclude that, as Internet access continues to permeate global society and with the wide availability of easy-to-use anonymizing tools, the global market for child pornography will increase.

Noting the effortless availability and use of technological tools that embolden child pornographers, the need exists to create and uphold laws that equip law enforcement to apprehend and convict these criminals. Few would argue that child pornography does not cause grave harm to children and society, and it seems that advancing technology is working to the criminals' favor. Besides the fact that digital technology makes it difficult to distinguish between the actual and the virtual, newer end-user devices like technology eyewear (e.g., digital glasses, smart contact lenses) could enable a person to use augmented reality applications to commit virtual crime (e.g., child rape) with images obtained from public spaces. It follows that such persons will confuse the difference between the actual and virtual, considering that modern technology will increasingly produce life-like human depictions. Based on current U.S. law, virtual child rape may be protected "speech" if the depiction is derived and not of an actual person, unless additional legislation limits the use of such applications.[1]

A discrepancy exists here between the U.S. Supreme Court's 2002 decision in Ashcroft and the *child pornography* provisions of the PROTECT Act developed by Congress in 2003 and revised in 2008. While the PROTECT Act does not state that the depiction of sex acts with or between fictional minors is inherently illegal, it does specify that the images will be considered illegal if they depict actions or situations that would be considered "obscene" under the Miller test. This Act was created to address the growing difficulty in distinguishing images that are digitally created from those of actual children (Department of Justice, 2003). While this task has become even more difficult, the U.S. Supreme Court has not confirmed the Constitutionality of the PROTECT Act as it applies to digital versus real child pornography. In fact, in *United States v. Williams* (2008), the Court upheld its decision in *Ashcroft v. Free Speech Coalition* (2002), stating that in regards to the pandering of child pornography, "A crime is committed only when the speaker believes or intends the listener to believe that the subject of the proposed transaction depicts real children". The authors of this paper hope that legislators and judges look beyond the free speech doctrine on the issue of digital child pornography, and recognize that based on current technology trends, computer-generated images and those of an actual person will soon be indistinguishable. Moreover, with augmented reality technology and the widespread use of wearable technology, we face a future where pornographic addicts may be walking in the general public while privately viewing their material on a personal device. It seems that this eventuality represents a grave enough danger to the general public to supersede free speech concerns, no matter whether the imagery is computer-generated.

While the laws in place regarding computer-generated child pornography are of concern, we do not suggest that changes in these laws alone will address every challenge law enforcement faces. Rather, as developments in technology make it more

[1] We say this with due respect for the relevant amendments of the U.S. Constitution. We leave the debate of the proper balance among free speech, privacy and security of citizens for other forums.

and more difficult to determine whether an image is computer-generated, adapting the law to meet these changes may be an appropriate place to start. Moreover, there are several other areas in which the law needs to catch up to the technology, and there are bound to be more as technological developments continue. A recent case highlighted another such issue. According to *The Child Protection and Sexual Predator Punishment Act of 1998*, service providers that become aware of the storage or transmission of child pornography are required to report this activity to law enforcement (Easttom, 2014). As technology develops however, it becomes easier for criminals to cross jurisdictional borders whilst engaging in criminal behavior. This modern development has recently presented a dilemma for the United States court system, such as for the U.S. district judge who decided in July of 2014 that Microsoft Corp, among other companies, was legally obligated to turn over a customer's emails to the U.S. government (The Guardian, 2014). Because the emails were stored in a data center in Ireland, this case raised concerns not only about privacy and warrant requirements, but also about jurisdiction. While this particular case did not involve child pornography, it is easy to see how such concerns about the intersection of technology and law could be involved in a child pornography case.

A point can be made that law enforcement may find it easier to catch child pornography users if the aggregate number of users increases. For instance, if users without due care view child pornography without using encryption technology, it might be easier for police to actually find and catch these offenders. Conversely, child pornographers who use heavy encryption will be much more difficult for police to catch, creating a dichotomy concerning the types of users who are actually apprehended. Thus, we could argue that a technologically-savvy criminal who knows how to mask their tracks can be very difficult to convict. This topic could be a potential future research study if the aggregate number of virtual child pornography users continues to increase over time.

After conducting a thorough review of the literature available, the authors consulted a police officer and polygraph examiner with over ten years' experience specializing in sexually deviant criminal behavior. Officer David Bryant commented on the authors' conclusions, confirming that he has witnessed technology's effect on the child pornography market. When asked whether technological developments have led to a growth in the production and dissemination of child pornography, Bryant said:

> There is absolutely no doubt that technology has increased the amount of child pornography. The Internet allows those interested in child pornography to meet with likeminded collectors of contraband to trade like never before. In the past, it was far more difficult and much riskier to make contact with sources. Transmitting photos or films required mailing and [thereby] knowing addresses. Now, any Internet connection gives access to the whole world for instant transmission and even live feeds for those interested. Technology allows anyone with a cellular telephone to produce and share child porn with ease (Personal communication, July 25, 2014).

When asked about the potential effects of viewing child pornography and its level of harm to children, Bryant stated:

> While the majority of those who view child pornography will not actually molest a child themselves, the potential is certainly there and these individuals are at a significantly higher risk for becoming sex offenders (Personal communication, July 25, 2014).

Bryant also shared concerns regarding the confusion and difficulty placed on law enforcement officials by current policies regarding digital child pornography. As an example, he mentioned a case he encountered with a man on probation for a child sexual offense who was using his artistic talent to draw digital images of child pornography.

Bryant concluded by saying, “Unfortunately, the law has not kept pace with the technology and the increase of child pornography cases.” (Personal communication, July 25, 2014). While the authors acknowledge that the word of one officer neither proves nor disproves any positions put forth in this paper, we do find it notable that law enforcement officials are aware of the discrepancy between the current technology and the law, and that this discrepancy increases the difficulty of apprehending and prosecuting child pornography offenders.

4. CONTRIBUTIONS AND LIMITATIONS

There is not a significant amount of scholarly research in the information systems and digital security field relating to child pornography. This is understandable because the topic is cross-disciplinary, primarily involving the legal domain, and of a sensitive nature. After our extant search, we did not find a similar published review of the literature in the information systems and security academic domain. We believe our paper’s contribution is that it may be the first of its kind comparing technological and legal developments concerning the topic of child pornography in a technology and security academic journal.

This paper’s scope is limited in that we did not address all laws concerning child pornography. For instance, in 2003 the Supreme Court upheld the constitutionality of the *Children’s Internet Protection Act* (CIPA) which requires schools and libraries that received federal funds to filter access to the Internet to block material that is ‘harmful to minors’ such as child pornography, or pornography in general. While CIPA is an important law, its focus is different in that it addresses protecting children from harmful or lewd material (Thornburgh & Lin, 2004). Our research focus instead was on laws and cases impacting the creation, distribution or supply of child pornography. A further limitation, our paper is not intended for a purely legal audience as the authors are not trained lawyers. Instead, we trace how both the legal and technological environments have made it significantly easier for the production and distribution of child pornography in the United States. We also focus our literature study to the United States and do not, for example, address the significant European efforts such as the *Cospol Internet Related Child Abusive Material Project* (CIRCAMP), which includes blocking and filtering methodologies to minimize the dissemination of child pornography.

5. CONCLUSION

As cyberspace and online file sharing expands, a new generation of criminals has turned to their computers to assist in producing and concealing their illegal activities. The age of digital communications has created the new area of digital child pornography which is recognized by governments around the world as a growing concern. This illegal market is expanding and will continue to do so as technologies spread globally. In order to fight online child exploitation, law enforcement agencies will need to maintain intelligence on technological advancements which might be of advantage to offenders, in order to take a proactive approach in apprehending digital criminals. From our review, it seems clear that both the legal and technological developments since the 1990s are creating a challenging environment for law enforcement. Further, considering that technology advances rapidly, we can predict that information technologies will further enable child pornographers in committing crimes.

We hope that our paper will create greater awareness of the challenges faced by law enforcement in this area.

Overall, the authors of this paper hope to bring greater awareness of the gap in technology and the law to both law enforcement and policy makers alike. In this sense, law enforcement officials should be made mindful of the need to remain educated on current technologies; not only those used by child pornographers, but also those technologies which may assist law enforcement in apprehending online child predators. Finally, if policy makers are made aware of the need for adaptation, the policies in place can be clarified or modified to meet the challenges posed to law enforcement by modern technologies used by child pornographers.

REFERENCES

Adobe Systems Incorporated. (2012). Adobe Photoshop CS6. Retrieved from http://www.adobe.com/products/photoshop.html.

Aizescu, S. (2014, Jan 16). Bitcoin: Innovative new currency, or tool for terror? *Haaretz*. Retrieved from www.haaretz.com/business/1.569042.

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

Barfe, L. (2012, Aug 13). Twitter is failing to police child pornography efficiently. *The Guardian.* Retrieved from http://www.theguardian.com/commentisfree/2012/aug/13/twitter-failure-child-pornography.

Bjango. (2012). Adobe Photoshop CS6 improvements. Retrieved from http://bjango.com/articles/photoshopcs6.

Brockman, J. (2006, Apr 6). Child sex as Internet fare, through eyes of a victim. *New York Times*. Retrieved from www.nytimes.com/2006/04/05/washington/05porn.html.

Bowles, N. (2014, Jan 3). Tapping into Silicon Valley tech to fight child porn. *SFGate*. Retrieved 3 January, 2014, from www.sfgate.com/news/article/Tapping-into-Silicon-Valley-tech-to-fight-child-5112571.php.

Burke, D., & Ford, J. (2011). When a lie is the truth: Pandering child pornography. *Journal of Legal, Ethical & Regulatory Issues*, 14(2), 117-139.

Chawki, M. (2009). Online child sexual abuse: The French response. *Journal of Digital Forensics, Security, and Law, 4*(4).

Connolly, K. (2007, May 8). Germany investigates Second Life child pornography. *The Guardian*. Retrieved from www.theguardian.com/technology/2007/may/08/secondlife.web20.

Consumer Watchdog (2013, Dec 18). Google's social network is playground for online predators. *PRNewsire Press Release*. Retrieved from www.sacbee.com/2013/12/18/6010648/googles-social-network-is-playground.html.

Cornell Legal Information Institute (LII), Cornell University. (2013a). 18 USC § 2251 - Sexual exploitation of children. Retrieved 26 June 2013, from www.law.cornell.edu/uscode/text/18/2251.

Cornell Legal Information Institute (LII), Cornell University. (2013b). 18 U.S. CODE § 1466A - Obscene visual representations of the sexual abuse of children. Retrieved 26 June 2013, from www.law.cornell.edu/uscode/text/18/1466A.

Coty, Stephen. (2014). Computer forensics and incident response in the cloud. RSA Security Conference, San Francisco, CA, February 2014.

Creative Bloq. (2012). Adobe Photoshop CS6 hands-on review. Retrieved from www.creativebloq.com/photo-editing/adobe-photoshop-cs6-review-1233260.

Cryptome. (2010). Anonymous author. Catch him with his encryption down: Counter-encryption techniques in child exploitation investigations. Retrieved from http://cryptome.org/isp-spy/crypto-spy.pdf.

Department of Justice. (2013). Child exploitation and obscenity section. Retrieved May 18, 2014, from www.justice.gov/criminal/ceos/subjectareas/childporn.html.

Department of Justice. (2003). Fact Sheet Protect Act, April 30, 2003. Retrieved 20 May 2014, from www.justice.gov/opa/pr/2003/April/03_ag_266.htm.

Dowty, D. (2013, Nov 13). Social media site Tumblr says it 'does not tolerate' child pornography after Martin J. Rothschild case. *Syracuse.com.* Retrieved from www.syracuse.com/news/index.ssf/2013/11/social_media_site_tumblr_says_it_does_not_tolerate_child_pornography_after_marti.html.

Easttom, C. (2014). *System Forensics, Investigation, and Response*, 2nd ed. Burlington, MA: Jones and Bartlett Learning.

Ex Parte John Christopher Lo (2013), NO. PD-1560-12 (Tex. Crim. App., 2013).

Fabio, M., & Tacconi, S. A Machine Learning-based Triage methodology for automated categorization of digital media. *Digital Investigation*, *10*(2), 193-204. Retrieved from http://dx.doi.org/10.1016/j.diin.2013.01.001.

Family Safe Media. (2013). Pornography statistics, 2006 Worldwide Pornography Revenues. *Family Safe Media.* Retrieved from www.familysafemedia.com/pornography_statistics.html.

Federal Bureau of Investigation. (2003). Privacy Impact Assessment (PIA) Child Victim Identification Program (CVIP) Innocent Images National Initiative (IINI). (May 9, 2003). Retrieved from www.fbi.gov/foia/privacy-impact-assessments/cvip.

Federal Bureau of Investigation. (2012). Innocent images. Retrieved November 2013, from www.fbi.gov/stats-services/publications/innocent-images-1.

Franklin, K. (2014). “Pornography Addiction:” Science or naked rhetoric? *Psychology Today.* Retrieved 30 April 2014, from www.psychologytoday.com/blog/witness/201404/pornography-addiction-science-or-naked-rhetoric.

Greenwood, C. (2013, 9 June). Only one in 15 online child porn suspects is arrested: Chief Constables accused of treating offences as a ‘low priority’. Updated 10 June 2013. *MailOnline.* Retrieved from www.dailymail.co.uk/news/article-2338613/Only-15-online-child-porn-suspects-arrested-Chief-constables-accused-treating-offences-low-priority.html.

Hatch, O. (2012). Fighting the pornification of America by enforcing obscenity laws. *Stanford Law & Policy Review*, *23*(1), 1-18.

Hilden, J. (2013, Dec 23). Why a Texas Appellate Court struck down a ban on certain sexual communications online. *Justia.com.* Retrieved from verdict.justia.com/2013/12/23/texas-appellate-court-struck-ban-certain-sexual-communications-online

Hurley, R., Prusty, S., Soroush, H., Walls, R.J., Albrecht, J., Cecchet, E., Levine, B.N., Liberatore, M., Lynn, B., & Wolak, J. (2013). Measurement and analysis of child pornography trafficking on P2P Networks. Proceedings of the International World Wide Web Conference Committee (IW3C2). Rio de Janeiro, Brazil, May 2013.

Immigration and Customs Enforcement. (2012). Child exploitation/operation predator. *Department of Homeland Security.* Retrieved from www.ice.gov/predator/.

Internet Watch Foundation (IWF). (2013, Aug 5). Websites hacked to host “the worst of the worst” child sexual abuse images. *IFW News.* Retrieved from www.iwf.org.uk/about-iwf/news/post/367-websites-hacked-to-host-the-worst-of-the-worst-child-sexual-abuse-images.

ICANN Security and Stability Advisory Committee. (2013). SAC-025. SSAC advisory on fast flux hosting and DNS. Retrieved December 2013, from www.icann.org.

ITV. (2013, 5 August). *Firms hacked to host ‘the worst of the worst’ images.* Retrieved 30 April 2014, from www.itv.com/news/update/2013-08-05/firms-hacked-to-host-the-worst-of-the-worst-images.

Johnson, K. (2014, March 5). Clandestine websites fuel 'alarming' increase in child porn. *USA Today.* Retrieved from www.usatoday.com/story/news/nation/2014/02/19/child-pornography-dark-web/5184485/.

Jones, G. (2011). Children and development III. *Progress in Development Studies, 11*(2), 145-149.

Kleinman, A. (2013, July 24). Professional Glass porn is here and Google can't stop it. *The Huffington Post.* Retrieved from www.huffingtonpost.com/2013/07/24/google-glass-porn_n_3644321.html.

Krebs, B. (2014). Spam nation: The inside story of organized cybercrime--from global epidemic to your front door. Naperville, Illinois: Sourcebooks.

Kwan, O. (2009). From the Protection of Children against Sexual Exploitation Act of 1977 to the Adam Walsh Child Protection and Safety Act of 2006: How congress went from censoring child pornography to censoring protected sexual speech. *Hastings Constitutional Law Quarterly*, *36*(3), 489. Retrieved from www.hastingsconlawquarterly.org/archives/V36/I3/Kwan.pdf.

Leon, A., & Gonzalez D. (2013, Jul 11). Sunrise man wanted on child pornography charges: FBI. *NBC, Miami.* Retrieved from www.nbcmiami.com/news/local/Sunrise-Man-Wanted-on-Child-Pornography-Charges-FBI-214914161.html.

Library of Congress. (2010). *Respectfully quoted: A dictionary of quotations.* Mineola, NY: Dover Publications, Inc., 192.

MacCarthy, M. (2010). What payment intermediaries are doing about online liability and why it matters. *Berkeley Technology Law Journal*, *25*(2), 1037-1120.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing: Recommendations of The National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Memoirs v. Massachusetts, 383 U.S. 413 (1966).

Miller v. California, 413 U.S. 15 (1973).

Moore, R. (2011). *Cybercrime: Investigating High-Technology Computer Crime.* Burlington, MA: Anderson Publishing.

Motivans, M. & Kyckelhahn, T. (2007). *Federal prosecution of child sex exploitation offenders, 2006.* Retrieved from Bureau of Justice Statistics: http://bjs.ojp.usdoj.gov/content/pub/pdf/fpcseo06.pdf.

National Center for Missing and Exploited Children. (2013). *Child Victim Identification Program.* Retrieved from www.missingkids.com/CVIP.

New York v. Ferber, 458 U.S. 747 (1982).

Holmes, O. W. (1934). *Speeches.*

Mauro, T. (2002). High court rejects child-porn law that 'turns the First Amendment upside down'. *Freedom Forum.* Retrieved 29 December 2013, from www.freedomforum.org/templates/document.asp?documentID=16082.

Obscene Publications Act. (2013). In *Encyclopaedia Britannica.* Retrieved from www.britannica.com/EBchecked/topic/423999/Obscene-Publications-Act.

Osborne v. Ohio, 495 U.S. 103 (1990).

Poulsen, K, (2013, 13 Sep). FBI admits it controlled Tor servers behind mass malware attack. *Wired.* Retrieved from www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/.

Poulsen, K. (2014, 27 January). If you used this secure Webmail site, the FBI has your Inbox. *Wired.* Retrieved 30 April 2014, from www.wired.com/2014/01/tormail.

Prat, S., Bertsch, I., Chudzik, L. and Réveillère, C. (2013), Developing software to estimate age in child pornography images for forensic purposes: Relevance and limitations in psychocriminology. *Journal of Forensic Sciences*, *58*: 845–846. doi: 10.1111/1556-4029.12082.

PROTECT Act of 2008, Pub, L. 110-401, 122 Stat. 4229, codified as amended at § 304. (2008). Retrieved from https://www.icactaskforce.org/Documents/2008ProtectAct.pdf.

Regina v. Benjamin Hicklin, Law Reporter 3 Queen's Bench 360 (1868).

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).

Rocha, A., Scheirer, W., Goldstein, S., & Boult, T. (2008). The unseen challenge data sets. *International CVPR Workshop on Vision of the Unseen.* IEEE, Anchorage, USA, 1-8.

Rocha, A., Scheirer, W., Boult, T., & Goldenstein, S. (2011). Vision of the unseen: Current trends and challenges in digital image and video forensics. *ACM Computing Surveys, 43*(4), 1-47.

Rosen v. United States, 161 U.S. 29 (1896).

Roth v. United States, 354 U.S. 476 (1957).

Schmidt, Eric (2013, Nov 19). Protecting children from sexual abuse. Retrieved February 1, 2014, from http://googlepolicyeurope.blogspot.com/2013/11/protecting-children-from-sexual-abuse.html.

Schuster, L. (2002). Regulating virtual child pornography in the wake of Ashcroft v. Free Speech Coalition. *Denver University Law Review, 80*(2), 429-462.

Sammons, J. (2012). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics.* Waltham, MA: Syngress.

Second Life Wiki. (2014). Linden Lab Official: Clarification of policy disallowing ageplay. *Official Information and Policies Portal.* Retrieved May 7, 2014, from http://wiki.secondlife.com/wiki/Official_Information_and_Policies_Portal.

Spencer, S. (2012). How big is the pornography industry in the United States? *Covenant Eyes.* Retrieved from http://www.covenanteyes.com/2012/06/01/how-big-is-the-pornography-industry-in-the-united-states/.

The Guardian (2013, Oct 4). 'Tor Stinks' presentation. *The Guardian*. Retrieved from www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document.

The Guardian (2014, July 31). Microsoft ordered to produce overseas customer email addresses by US judge. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2014/jul/31/microsoft-must-handover-overseas-emails-judge.

Thomas, T. (2014, January 21). Google Glass sex app lets you watch, record yourself in the act. *The Huffington Post.* Retrieved from www.huffingtonpost.com/2014/01/21/google-glass-sex_n_4637741.html.

Thornburgh, D., & Lin, H. (2004). Youth, pornography, and the Internet. *Issues in Science and Technology*, 43-48.

United States v. Williams, 128 S.Ct. 1830 (2008). No. 06-694. Supreme Court of United States.

U.S. Department of Homeland Security. (2009). *National Child Victim Identification System (NCVIS).* Retrieved from www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_ncvis_august_2009.pdf.

U.S. Postal Service. (2012). U.S. postal inspectors protect children. *U.S Postal Inspection Service.* Retrieved from https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/ce/CE.aspx.

U.S. Sentencing Commission. (2012). Report to the Congress: Federal child pornography offenses. Retrieved December, 2012, from www.ussc.gov/news/congressional-testimony-and-reports/sex-offense-topics/report-congress-federal-child-pornography-offenses. 468 pages.

Wikileaks. (2009). An insight into child porn. *Anonymous letter.* Translated from German. Retrieved on February, 26, 2009, from http://wikileaks.org/wiki/.

Withnall, A. (2013, 22 September). Pornography addiction leads to same brain activity as alcoholism or drug abuse, study shows. *The Independent.* Retrieved 26 April 2014, from www.independent.co.uk/life-style/health-and-families/health-news/pornography-addiction-leads-to-same-brain-activity-as-alcoholism-or-drug-abuse-study-shows-8832708.html.

West, A. (2010). *20 years of Adobe Photoshop.* Retrieved from www.webdesignerdepot.com/2010/02/20-years-of-adobe-photoshop/.

Wassom, B. (2012). Five predictions for augmented reality law in 2012, Law of Social & Emerging Media, *Wassom.com.* (n.d.). Also quoting Rampolla, Joe. Retrieved from www.wassom.com/5-predictions-for-augmented-reality-law-in-2012.html.

Zawoad, S., & Hasan, R. (2013). Digital forensics in the cloud. *The Journal of Defense Software Engineering. 26*(5), 17-20.

AUTHOR BIOGRAPHIES

Jasmine V. Eggestein is a graduate student earning a degree in Information Security at Nova Southeastern University. She earned her Bachelor's degree in Criminology with a minor in Management Information Systems at The University of Tampa. She is employed as an IT specialist at Entia Ventures. Her focus is in the area of cybercrime and computer forensics.

Kenneth J. Knapp is an Associate Professor at The University of Tampa. He has published in numerous journals in the area of information systems and security.