Internet Child Pornography, U.S. Sentencing Guidelines, and the Role of Internet Service Providers

Kathryn C. Seigfried-Spellar[1,*], Gary R. Bertoline[2], and Marcus K. Rogers[2]

[1] Seattle University, 901 12th Ave, Seattle, WA 98122
spellark@seattleu.edu
[2] Purdue University

Abstract. The following review will provide a historical recap of the United States response to child pornography as it relates to the ever-evolving technological world. Specifically, a review of the child pornography laws, at the federal level, as well as the sentencing guidelines will reveal the delicate balance between criminalizing child pornography and upholding the United States' constitution. In addition, discussing the role of Internet Service Providers will expose a trend toward using the same technology, which has proliferated the child pornography industry, to identify and censor the illegal content on the Internet. Finally, the strengths and weaknesses of the current laws and regulation tactics, as well as, the suggested amendments will be discussed.

1 Introduction

The Internet has had a profound impact on the child pornography industry; the increase in child pornography related arrests and prosecutions reflect the Internet's increased accessibility and availability worldwide. Increased prosecutions meant various judicial bodies were seeking information as to the "who, what, and why" of child pornography consumption in order to inform policy and legislative decisions. However, attempts at regulating the Internet child pornography industry through legislation have continuously clashed with the United States' constitution. Child pornography legislation impacts the First Amendment (freedom of speech and expression) and the Fourth Amendment (protection against unlawful search and seizure), to name a few. In addition, the federal laws are constantly responding to the advancements made in technology, many of which have greatly impacted the child pornography industry, such as the availability of computers and the globalization of the Internet. While technology has definitely proliferated the accessibility of child pornography, technology may also assist law enforcement and the community at large by blocking and/or removing the illegal content as well as identifying the consumers.

The following review will provide a historical recap of the United States response to child pornography as it relates to the ever-evolving technological world. Specifically, a review of the child pornography laws, at the federal level, as well as the sentencing guidelines will reveal the delicate balance between criminalizing child

* Corresponding author.

P. Gladyshev and M.K. Rogers (Eds.): ICDF2C 2011, LNICST 88, pp. 17–32, 2012.

pornography and upholding the United States' constitution. In addition, discussing the role of Internet Service Providers will expose a trend toward using the same technology, which has proliferated the child pornography industry, to identify and censor the illegal content on the Internet. Finally, the strengths and weaknesses of the current laws and regulation tactics, as well as, the suggested amendments will be discussed. Overall, the Internet was never intended to become the modern-day playground for exchanging and creating sexualized images of children, but technology has given this "old crime some new tricks."

2 The United States Response to Child Pornography

Since the early 1950s, pornographic materials determined by the courts as "obscene" have been illegal in the United States [1]. Obscene expressions of speech are not protected under the First Amendment, which "generally prevents [the] government from proscribing speech, or even expressive conduct, because of disapproval of the ideas expressed" [as cited by 2, p. 678]. However, pornographic materials that are considered to be "indecent" rather than "obscene" are not prohibited by law, which frequently raises the question of what constitutes indecent versus obscene expressions of speech. Federal legislation currently considers adult pornographic materials, even hard-core depictions of sexual activity, as indecent rather than obscene, so the materials are protected speech under the First Amendment. Rarely is adult pornography considered to be "obscene" materials, with exceptions including cases of consensual adults engaging in sexual activity, which is being surreptitiously recorded [1]. Currently, child pornography is considered to be an "obscene" expression of speech and is not protected by the First Amendment; however, this has not always been the case.

2.1 The Evolving Federal Law of Child Pornography

Children have been treated and viewed as sexual objects and included in erotic literature and drawings long before the invention of the Internet. However, child pornography has only been recognized as a legal problem in the United States for a little over three decades. In the United States, child pornography became a problem due to the lax local legislation as a result of the sexual revolution. In the late 1970s, Congress reacted to the mounting evidence regarding the harmful effects of child sex abuse, and the change in the child pornography industry as it shifted from a "cottage industry" to a form of "organized abuse" for commercial production [3].

In 1978, Congress passed the Protection of Children Against Sexual Exploitation Act, which became the first federal law to criminalize "child exploitation through sexually exploitative live performances and visual depictions of children engaged or engaging in sexual conduct" [as cited by 4, p. 1104]. Specifically, the 1978 Act prohibited the production or *commercial* distribution of "obscene" material depicting individuals under the age of 16 years. At this time, the current standards for determining "obscenity" was set by the *Miller v. California* case [see 5], which established three criteria in order for the materials to be considered obscene by the local community's standards. However, in 1982, the Supreme Court ruled in *New*

York v. Ferber that the *Miller* standards did not apply to child pornography because the material was already inherently obscene.

By labeling child pornography as "obscene," the Supreme Court ruled that child pornography was no longer protected under the First Amendment since the need to prevent child sex abuse and exploitation prevailed over the value of free speech [5], [2]. In response to *Ferber*, congress passed the Child Protection Act of 1984, which redefined "sexual conduct" to include both obscene and non-obscene visual depictions of "intercourse, bestiality, masturbation, sadism, and lascivious exhibition of the genitals" [6, p. 41]. By including "lascivious" in the definition of sexual conduct, the Act of 1984 determined that child pornography did not have to involve obscene behavior, such as sexual activity, but may include the visual depiction of non-obscene behavior. For instance, an image may be considered "lascivious" when it focuses on the clothed genital region of children despite the lack of nudity [1].

In addition, the Child Protection Act of 1984 criminalized individuals who produced or trafficked non-commercial child pornography, or in other words, individuals with no financial motives [United States Sentencing Guidelines, USSC; 7]. The Act of 1984 also changed the prohibited age of minors in child pornography from under 16 years according to the Protection Act of 1978 to under the age of 18 years. Since 1984, this definition of a minor in child pornography, any person under the age of 18 years, remains unchanged in the United States' federal legislation. Overall, the Child Protection Act of 1984 reiterated the difference between the legal definitions of obscene and indecent material, which not only depended on the "content" (nudity vs. fully-clothed) of the pornographic material but also on the age of the participants (adults vs. minors).

In 1988, Congress passed the Child Pornography and Obscenity Enforcement Act, which became the first federal law to specifically address the use of computers in the implementation of child pornography. This act made it illegal to use a computer to distribute or advertise child pornography [8]. Overall, the federal and state courts recognized child pornography as an emerging criminal offense in the late 1970s. During the 1980s, however, only the production or distribution of child pornography was prohibited or illegal by federal law. It was not until the 1990s that several state courts ignited a legal and social movement, which considered other definitions and behaviors related to child pornography.

In 1990, the possession of child pornography was ruled as a criminal offense in the case of *Osborne v. Ohio*, meaning the private possession of child pornography was not protected under the First Amendment [6]. Even if the individual does not share or distribute the images or photographs to other users, it became illegal to possess the images as a private collection for personal use. According to the Court, the mere possession of child pornography should be illegal because it "springs from a grievous harm" and "pedophiles may use it to seduce new victims or to convince children to submit to sexual violation" [as cited by 6, p. 48]. In a further argument, this ruling stated child pornography was not protected under the First Amendment due to the risk of using the materials for immoral reasons, such as the grooming of children [6].

Although the influence of computers in child pornography was mentioned in the Child Protection and Obscenity Enforcement Act of 1988, it was not until 1996 in the Child Pornography Protection Act (CPPA) that the definition of child pornography was expanded to include virtual images of children. A "virtual image" was considered

to be any image of a minor that was created through the use of technology rather than the actual exploitation or abuse of a real victim. These virtual images included pseudo-photographs and computer-generated images as well as the depiction of individuals who "appeared" to be, but may not actually be, under the age of 18 years. The CPPA argued that child pornography, even if it did not involve the sexual abuse of an actual or real victim, was "evil in and of itself" [as cited in 5, p. 97]. In addition, Congress stated it was necessary to prohibit the use of pseudo-child pornography images because they "inflame the desire of child molesters, pedophiles, and child pornographers" [9, p. 49], [see 5].

In the Child Pornography Protection Act of 1996, the definition of "sexually explicit" was modified to "actual or simulated visual depictions, which convey the impression that they contain sexually explicit depictions of minors" [8, p. 88]. In addition, Congress extended the definition of child pornography to include virtual images to assist prosecutors who were burdened with proving that the pornographic image in question depicted an actual, real victim [see 5]. However, the American Civil Liberties Union (ACLU) argued that the CPPA of 1996 was unconstitutional because it moved away from the original intentions of the Court's ruling in *Ferber*. According to *Ferber*, protecting children from sexual abuse was the prime reason for excluding child pornography as protected speech, or freedom of expression, under the First Amendment [5]. With no real victims, the ACLU argued it was unconstitutional to ban virtual child pornography according to *Ferber*. Again, the Courts rejected the ACLU's argument stating it was the government's intentions to prevent any future sexual abuse of children regardless of whether the images depicted real or virtual victims who appeared to be minors [5].

However, the Child Pornography Protection Act of 1996 was overturned in 2002 in the ruling of *Ashcroft v. Free Speech Coalition*. The Supreme Court determined the phrases "appeared to be a minor" and "conveyed the impression" violated constitutional rights in that they were too broad and vague to be upheld by the judicial system [8]. In addition, computer-generated or pseudo-child pornography were not included as exceptions to freedom of expression, in other words, virtual child pornography was protected under the First Amendment. In response to the Supreme Court's decision, Congress passed the PROTECT Act in 2003 to address the judicial concerns of defendants claiming that the images in question involved virtual and not real children, which burdened the prosecutors to prove otherwise [5]. Congress stated that at the time of *Ferber* technology did not exist which could create computer-generated minors indistinguishable from real or actual child pornography victims [5]; therefore, the PROTECT Act of 2003 allowed prosecutors to proceed in cases where the images depicted "persons who appear virtually indistinguishable from actual minors" [10, p. 119]. In addition, the burden of proof was shifted to the defense if claims were made that the images depicted pseudo or computer-generated minors and not real victims.

Overall, the PROTECT Act amended the previous federal laws to clarify terms as well as take into account advances in technology. The definition of "minor" remained unchanged - any individual under the age of 18 years. However, separate definitions of "sexually explicit conduct" were provided depending on whether the depiction was that of real or computer-generated abuse. In addition, virtual child pornography meant the pseudo-child in the image was "indistinguishable from that of a minor engaging in

sexually explicit conduct" [5]. Finally, the PROTECT Act of 2003 created a cyber hotline where Internet users could anonymously report any information regarding the distribution of child pornography [10].

In 2008, the PROTECT Our Children Act of 2008 created a new offense criminalizing the production or distribution of child pornography which was created from a non-sexual image of an identifiable or real child. Specifically, this act penalized individuals who intended to produce or distribute non-pornography images of real children that were modified or changed to create child pornography with a statutory maximum sentence of 15 years with no mandated minimum. In addition, Congress stated that anyone who "knowingly accesses with intent to view" the broadcast of live images of child sex abuse has "possessed child pornography" [7, p. 50]. Finally, the definition of child pornography was amended to include the "production, distribution, or access of a live visual depiction of child pornography" [7, p. 50].

Currently, the United States federal government criminalizes the possession, distribution, and production of sexually explicit images of individuals (actual or indistinguishable from) under the age of 18 years. According to the federal child pornography statutes, the production of child pornography carries a maximum sentence of 30 years imprisonment with a mandatory minimum of 15 years. In addition, the possession or distribution/trafficking of child pornography carries a maximum sentence of 20 years with a mandatory minimum of 5 years for the distribution offenses. Although the federal legislature determines the minimum and maximum punishment for each child pornography offenses, the courts must determine the appropriate sentence on a case-by-case basis. As indicated in the next section, the federal sentencing guidelines have evolved and amended during the past thirty years to reflect changes in legislation and advances in technology. Despite multiple amendments, the United States Sentencing Commission continues to recommend sentencing guidelines to assist the courts in determining the appropriate level of punishment; the following section will review and summarize the development of the U.S. sentencing guidelines for child pornography-related offenses.

2.2 The History of Sentencing Guidelines for Child Pornography

In a recent report, the United States Sentencing Commission (2009) summarized the history of federal legislation and sentencing mandates for crimes involving child pornography. A year after the Child Abuse Victims' Rights Act of 1986, the United States Sentencing Commission produced its first set of sentencing guidelines with base levels for the following child pornography offenses: production, transportation, distribution, and receipt of child pornography [7]. The intent of the sentencing guidelines was to provide "certainty, uniformity, and proportionality in criminal sentencing . . . and to recognize differences between offenses" [7, p. 2]. In general, each federal offense in the United States is sentenced based on a sliding scale of "base levels" with a minimum and maximum sentence. To determine the appropriate sentence according to these guidelines, the starting base level is first established for the offense in question. Next, any mitigating or aggravating factors are considered which can either decrease or increase the offense's base level for sentencing, respectively. Once all of these factors are considered, the USSC sentencing guidelines

provide the courts with a recommended minimum and maximum sentence for the offense in question, while also considering the specific facts of the case. In the end, the sentencing guidelines are advisory rather than mandatory leaving sole discretion to the judge, and this subjectively may or may not result in uniform and consistent sentences between similar cases and circumstances.

The 1987 United States Sentencing Guidelines set the base level for child pornography offenses anywhere between 13 and 20 depending on the specific offense characteristics. For example, the 1987 USSC guidelines mandated a 2-level increase for cases involving child pornography images of a minor under the age of 12 years. In addition, at least a five level increase was mandated for commercial distribution of images [7]. Therefore, the sentencing base level of 13 could be increased if the case involved images depicting a minor under the age of 12 years (+2) as well as distribution (at least +5) yielding the maximum base level of 20. A year later, the original sentencing guidelines were modified from "minor" to "prepubescent minor" in order to ease the courts ability to assess the specific offense characteristic's criteria of whether the child depicted was under the age of 12 years [7].

However, concerns were raised regarding whether the current sentencing recommendations were in accordance with the increased severity of abuse or victimization portrayed in some of the child pornography collections. In 1990, the USSC responded by amending the guidelines, while maintaining the base level at 13, to include a new specific offense characteristic to be considered by the courts. The base level was to increase by four levels if the offense involved images that depicted "sadistic or masochistic conduct or other depictions of violence" [7 p. 17]. As a reminder to the reader, only the production and distribution of child pornography was illegal in the United States at this time. However, a few weeks after the November 1990 amendments to the USSC sentencing guidelines, Congress passed the Crime Control Act of 1990, which criminalized the possession of child pornography [7]. Consequently, the sentencing guidelines were once again amended only a few months later to include the new child pornography offense, possession.

In May 1991, the USSC set the base level for possession of child pornography at 10 with a two level increase for images depicting a prepubescent minor under the age of 12 years. However, government backlash suggested the USSC was sentencing individuals to a "slap on the wrist" by setting a lower penalty for the possession of child pornography compared to receiving or distribution [7]. In November 1991, the base level for possession was increased to 13, and the baseline level for trafficking offenses was increased from 13 to 15. In addition, two new offense characteristics were adopted: (1) a two level increase for cases involving the "ten or more books, magazines, periodicals, films, video tapes, or other items" (p. 25), and (2) a five level increase "if the defendant engaged in a pattern of activity involving the sexual abuse of a minor" [7, p. 25].

In 1996, Congress received a report from the USSC, *Sex Offenses Against Children: Findings and Recommendations Regarding Federal Penalties*, which analyzed the sentences of child pornography cases between 1994 and 1995 [7]. Of the 66 cases involving trafficking or distribution offenses, the average sentence length was 28.5 months compared to an average sentence length of 15.4 months for the 24 cases involving possession. The USSC also acknowledged the escalating use of computers in the child pornography cases. As a result, the sentencing guidelines for

child pornography offenses were adjusted in November 1996 by raising the base level for both trafficking and possession by two levels yielding 15 and 17, respectively. In addition, for the trafficking offense, if the case involved the use of a computer to distribute or advertise the child pornography images, the base level was to be increased by two levels. For the possession offense, there was a two level increase if the defendant obtained the material as a result of using a computer [7].

In 1998, Congress passed the Child Protection Act, which addressed cases involving the production of child pornography using materials either mailed, shipped, or transferred in interstate or foreign commerce [Protection of Children from Sexual Predators Act, PCSP; 11]. Recognizing the ease of distribution, especially due to the increase availability of the Internet, the USSC responded by amending the child pornography trafficking offense to include the following specific offense characteristics: (1) increase at least five levels for commercial distribution, (2) increase five levels expected to receive something of value in return, other than monetary gain, (3) increase five levels for distributing to a minor, (4) increase by seven levels if the distributing materials to minor with intentions of grooming or sexual conduct, or (5) increase two levels for distribution not otherwise specified [7]. Overall, these changes to the sentencing guidelines intended to further differentiate the possession from distribution child pornography offenses, to acknowledge the accessibility of child pornography due to technological advances, and to punish those individuals who distributed obscene materials to minors.

Next, Congress passed the PROTECT Act of 2003 which provided directives to set the mandatory minimum for trafficking to five years while increasing the statutory maximum from 15 to 20 years. In addition, the Act increased the statutory maximum for possession of child pornography from five to 10 years. For the first time in history, Congress directly amended the USSC sentencing guidelines through the PROTECT Act of 2003 to include a new specific offense characteristics under the trafficking child pornography offense [7]. The additional case characteristic increased the base level depending on the amount and content of the child abuse images: (1) 10 to 149 images, increase by two levels, (2) 150 to 299, increase by three levels, (3) 300 to 599, increase by four levels, or (4) 600 or more, increase by five levels [7].

However, the sentencing guidelines implemented by the PROTECT Act of 2003 were amended by the USSC in November 2004 to consolidate the trafficking/ distribution and possession offenses into one sentencing guideline. The base levels for possession and trafficking of child pornography were changed from 15 to 18 and 17 to 22, respectively, and changes occurred to the specific offense characteristics for possession and distribution/trafficking of child pornography. First, the base level should be decreased from 18 to 16 if the offense only involved the "simple" possession of child without intent to distribute [7]. In addition, the suggested increase in base level remained the same, seven, if the offense included the distribution of child pornography materials with the intent to encourage or facilitate the travel of a minor to engage in illegal sexual conduct. However, an additional specific offense characteristic was added which increased the base level by six for all other illegal intentions for distributing child pornography to a minor, which was not otherwise specified. Finally the specific offense characteristic describing the "use of a computer" to distribute child pornography was changed to the "use of a computer or an interactive computer service" [7].

In 2008, the PROTECT Our Children Act created a new offense criminalizing the intent to produce or distribute modified or morphed child pornography images of an identifiable minor. In response, the United States Sentencing Commission determined that the new offense was different from the current offenses involving the production or distribution of child pornography, which involve the sexual abuse of an *actual* victim [7]. Effective November 2009, the USSC determined the base level for the distribution of pseudo child pornography should be set at 18 rather than 22, which was the current distribution/trafficking offense base level, due to the lack of a real child victim. The lower base level reflected Congress' decision to set a lower penalty, a maximum term of 15 years with no mandatory minimum sentence, compared to the current penalty for distribution, which carries a maximum sentence of 20 years with a mandatory minimum of 5 years. Finally, the specific offense characteristic involving the use of a computer to distribute child pornography was amended to include "accessing with the intent to view" [7]. This new characteristic increases the base level by two if the offense included the use of a computer to access with intent to view or distribute images of child pornography. As a reminder, this characteristic might be applied to cases involving both real and pseudo images of child pornography.

In summary, the current United States sentencing guidelines have base levels set on a continuum, which reflect the recommendation of harsher sentences, for offenses involving the production, distribution, and/or possession of child pornography images, respectively. Since every criminal case involves different circumstances, the USSC included offense specific characteristics, which either increase or decrease the offenses base level to provide a more case-specific sentencing recommendation. The United States sentencing guidelines also recommended harsher sentences for child pornography offenses involving collections with a large quantity of images with 10-149 images at the lower end of the spectrum and more than 600 images at the polar end [7]. In addition, the federal sentencing guidelines consider the content of the images by increasing the base level for cases involving violent images of child sexual victimization (e.g., sadism). Overall, the USSC will continue to amend the sentencing guidelines for child pornography related-offenses so long as new legislation is passed and technological advancements are made.

3 The Proliferation of Child Pornography on the Internet

As evident in the past 30 years, as technology evolves so follows government directives, judicial legislation, and sentencing guidelines for offenses involving child pornography. Government protocols must consider how technology has impacted the child pornography industry, for research clearly suggests the possession, distribution, and production of child pornography has greatly increased as a result of the globalization of the Internet. Not only are individuals involved in these offenses, but more often than not, child pornography cases involve the use of technology and third-party vendors, such as Internet Service Providers (ISPs). Accordingly, legislation must determine the role played by Internet Service Providers while also assessing whether the same technological advancements, which have increased the prevalence of child pornography, can be controlled or manipulated to stop the proliferation of this crime.

3.1 The Role of Internet Service Providers

In 1998, the Protection of Children from Sexual Predators Act (PCSP) amended the Victims of Child Abuse Act of 1990 to require electronic communication service providers to notify any known incidents of child pornography to law enforcement agencies. This act stated that electronic service providers had a "duty to report as soon as possible" any knowledge or information of child pornography offenses [11]. The bill notified the electronic service providers of the appropriate source of contact, and also stated that a failure to willingly report any known incidents of child pornography offenses would result in fines up to $50,000 for an initial failure and up to $100,000 for subsequent failures. In addition, the Protection of Children Act of 1998 stated the electronic service providers had no civil liability, meaning they could not be held accountable for any third party information [11]. Finally, the electronic service providers were not required to monitor or restrict any communication or content; however, to assist inquiries involving minors, the Act of 1998 allowed law enforcement agencies to subpoena electronic service providers for client information (name, address).

Overall, this act required electronic service providers to report any knowledge of child pornography offenses, but they were not required to monitor or restrict electronic communication and could not be held liable for the illegal activities of users, subscribers, and customers. In 2008, the PROTECT Our Children Act identified the CyberTipline of the National Center for Missing and Exploited Children (NCMEC) as the contact agency for reporting information about child pornography offenses [12]. In addition, the electronic service providers must report the identity and location of the individual suspected of violating the law as well as the esoteric child sex abuse images. Specifically, the suspected child pornography images are to be treated as evidence to be later turned over to law enforcement by the NCMEC. Thus, the electronic service provider is no longer reporting the incidents directly to law enforcement; rather, the NCMEC is responsible for contacting the designated law enforcement agency [12]. Again, the NCMEC and the electronic service providers are granted limited immunity from civil and criminal liability so long as all "good faith" attempts were made to report all known or suspected incidents of child pornography [no intentional misconduct, recklessness, or malice; 12]. Finally, the NCMEC may notify the electronic service providers of the child pornography images in order to stop or block their transmission on the Internet [12].

Filtering. Researchers agree the amount of child pornography available via the Internet is unknown, and its complete removal remains impossible [13]. However, filtering software and self-regulatory initiatives may "reduce the volume, make it more difficult or risky to access, and [help] to identify and arrest the more serious perpetrators" of Internet child pornography [13, p. 37]. For example, Congress passed the Children's Internet Protection Act of 2000 (CIPA) which required libraries receiving government grants or discounts to implement filtering software in order to protect minors from accessing illegal or questionable materials, including both adult and child pornography. CIPA did not violate First Amendment rights since adults may request that the library's filtering software be disabled when valid reasons are provided [14]. Thus, the courts determined that CIPA simultaneously protected

minors from viewing or accessing inappropriate content while protecting the freedom of speech and expression for adults. In CIPA, the courts directly impacted the library and public school systems, but parents are increasingly using filtering software on household computers to block as well as monitor their children's activities on the Internet [see 15].

Although filtering software attempts to block the minors' access to inappropriate content, research indicates that underblocking (failing to block obscene content) and overblocking (blocking legal content) occurs raising important concerns on its effectiveness and constitutional feasibility [14]. For example, a report by the National Research Council in 2002 determined that filtering software tools will always remain the victims of underblocking and overblocking; therefore, "social and educational strategies . . . are more useful . . . Parents, teachers, and librarians all share the responsibility in guiding children . . . [and] delegating this responsibility to technology protection devices such as filters is not sufficient" [as cited by 14 p. 2978].

Another consequence of filtering software tools is the "digital divide" [see 16], which refers to the "difference in access to digital information that separates the information-rich from the information-poor" [14, p. 2980]. By thwarting the knowledge accessible at the library or even in some public schools, those individuals who are most likely to use these computers may be at an information disadvantage. For example, certain minorities and lower income families are more likely to rely on public computers, and when the information is being filtered, free speech advocates question "what's left" [14]?

Overall, filtering or blocking access to the Internet compromises the openness of the Internet, which is a fundamental concern for free speech activists and advocates for the free-flow of knowledge. According to Morris and Wong, "The new media must be open, decentralized, and abundant . . . a loss of openness or neutrality would pose serious challenges to free speech online" [15, p. 114]. Still, the current trend in national and international policy is the implementation of filtering tools to block user access to Internet child pornography images.

Blocking. Along with filtering software, some Internet Service Providers are getting involved in the fight against child pornography. In 2008, three of the world's largest Internet Service Providers, Verizon, Sprint, and Time Warner Cable, agreed to block access to child pornography newsgroups and websites [17]. As discussed previously, Internet Service Providers are required by law to report any knowledge of child pornography offenses, but they are not required to actively monitor or restrict electronic communication. In other words, they are not required to "block" websites disseminating child sex abuse images unless directed by the NCMEC. Although not required by law, Internet Service Providers are being pressured, both socially and politically, to become "child porn cops" [18]. According to the *New York Times*, several complaints regarding the transmission of child pornography were made to Verizon, Sprint, and Time Warner Cable; however, it was only after political threats were made that the three ISPs agreed to cooperate and block access to current and future child pornography websites [17].

A few months later, AOL received a proposal from the New York's attorney general regarding the use of a new software tool being developed in the United States called CopyRouter by the Australian company, Brilliant Digital Entrainment Ltd [18].

According to the developer, any web searches, attachments, or sharing of files using peer-to-peer networks would be scanned and compared to known child pornography images, which have a unique digital fingerprint or "hash value." If CopyRouter locates a file with the same hash value as a known child pornography image, the file will be blocked and the individual will receive a warning screen stating the material was identified as child pornography. In addition, the developer admittedly states that the software will only compare the hash values and not "read the content of the files – it couldn't tell a love note from a recipe" [18, p. 4].

However, Internet Service Providers need to be careful in that they do not truly become "child porn cops" or "agents of law enforcement" due to the United State's Fourth Amendment [18, p. 9]. The Fourth Amendment prohibits unlawful search and seizure by the government, therefore, ISPs who act as a law enforcement agency or government entity while searching the attachments and web files for child pornography will violate the United States constitution. Supporters of CopyRouter state the ISPs will remain a "company" rather than a "law enforcement agency" since they will not have access to the child pornography list maintained by law enforcement [18]. Instead, CopyRouter will act as the "middleman" by consulting with law enforcement to maintain an up-to-date list of known child pornography files, and ISPs will remain a company that employs rather than manages the filtering software.

However, according to the Center for Democracy and Technology, filtering software like CopyRouter "constitutes an illegal wiretap" by invading users privacy without approval from the proper channels [18, p. 14]. In addition, the Center argues that blocking the images prior to their receipt inhibits communication, which again violates the First Amendment. Although no one argues that images of child sex abuse should be tolerated, the Center for Democracy and Technology reminds policy makers and the public that "you still have to follow the constitution" [18, p. 14].

Deleting. Internet child pornography is an international problem, and other countries are toying with various tactics for decreasing the accessibility and availability of Internet child pornography. Along with the United States, the trend to filter, monitor, or block websites disseminating child pornography is prominent in the European Union, a supranational organization consisting of 27 Member States [5]. Recently, the European Union created, but to date has not passed, a directive to block websites containing child sex abuse images. In addition, Germany has refused to implement this directive citing the only effective measure against Internet child pornography websites is their complete *removal or deletion* [19]. Experts and opposing Member States argue blocking websites only creates a "smokescreen for political failure" [20, p. 111], and the only way to stop the proliferation of child pornography is to take down or delete the websites all together [21].

According to McNamee, blocking user access to websites containing child pornography merely masks rather than eliminates the problem [20]. As previously discussed, filtering or blocking tools are not perfect, and "if anybody wants to deliberately access these Web sites, they will somehow find the technological means" [21, para. 8]. In addition, McNamee compares child pornography images to photographs of murder, both of which are evidence of a crime scene, but policy makers would never advocate the "blocking" of websites disseminating images of a murder or crime scene; instead, "all possible efforts would be made to identify the

victims and prosecute the murderers" [22, para. 4]. Although blocking might stop the unintentional access to websites containing child pornography, McNamee argues this method does not consider that websites can change addresses and locations, which makes it easy to evade blocking thereby allowing users to gain deliberate access to the illicit sites [22].

Overall, the current trend to filter or block websites distributing child pornography appears more problematic than useful in the fight against child sex abuse. In fact, research indicates filtering software and blocking tactics are not only imperfect and easily evaded, but they border on violating the constitutional rights to freedom of speech and unlawful search and seizure. Instead, the National Association to Protect Children argues resources should be spent to directly tackle the sexual abuse of children, meaning the producers of child pornography; the government should be "funding cops to rescue children" rather than "outsourcing the job" [18, p. 15]. In essence, society as a whole needs to avoid the "moral panic" surrounding child pornography, and no matter how horrible this crime may be, the true focus of policy makers should be the protection of children.

4 Avoiding Moral Panic and Embracing Science

Academic researchers agree the current laws and sentencing guidelines nationally and internationally are the result of a "panic-led policy debate" [5 p. 139] by which the consumers of child pornography are treated as child sex offenders or pedophiles [23]. Contrary to public opinion, not all consumers of child pornography are sexually attracted to children and at risk of crossing over to hands-on child sex abuse. Instead, the motivations and reasons are just as diverse as the user, and child pornography consumers cannot be "lumped" into one homogenous category of offenders. Rather, the law should be flexible enough to recognize the different risk factors associated with child pornography use, hands-on child sex abuse, and rates of recidivism [see 23]. Research acknowledges a difference between these groups of offenders, and if the United States federal laws and sentencing guidelines intend to be led by science rather than moral panic, then *change* is the only way to achieve due justice.

First, a review by Malamuth and Huppin suggests the possession of virtual child pornography should only be illegal for convicted child sex offenders since empirical research does *not* suggest that being a child pornography consumer (hands-off) is a risk factor for crossing over to child sex abuse [hands-on; 23]. Although, a single study suggests Internet child pornography users sampled from a self-select treatment program were more likely to commit a hands-on child sex offense, it remains unknown whether "child pornographers who self-select for treatment differ from offenders with similar offenses who decline to participate in treatment" [24, p. 189]. In addition, the study acknowledges "the vast majority of the participants in our treatment program report that they committed acts of hands-on abuse *prior[sic]* to seeking child pornography via the Internet" [24, p. 189]. Convicted child sex offenders are more likely to consume child pornography and are at greater risk for reoffending [see 23]. However, if the court's purpose of criminalizing pseudo or computer-generated child pornography is to protect children by "whetting the appetites of pedophiles," then the courts should only penalize those offenders who are convicted child molesters. Malamuth and Huppin stress this amendment to the current law is constitutionally sound in that it passes the Eighth

Amendment, which bans cruel and unusual punishment from "criminalizing a person's status as a member of a group" [23, p. 821]. Therefore, if a child sex offender is found to be in possession of virtual child pornography, then prohibiting virtual child pornography is valid since the behavior rather than the status of the individual led to the additional penalty [23].

Similar to the current federal laws on child pornography, the sentencing guidelines have been criticized for embodying the moral panic of society rather than the available scientific evidence. According to Basbaum, the current sentencing guidelines are based on "unsubstantiated assumptions about recidivism potential" rather than the academic literature on pedophilia, child pornography use, child molestation, and non-offenders [25, p. 17]. For example, possessors of child pornography are harshly punished due to the fear of crossing over to hands-on child sex offenders, but as previously discussed, there is no scientific support for viewers of child pornography being at a higher risk for crossing over to hands-on child sex abuse. In addition, as far as the Bourke and Hernandez [24] study, Hessick argues "if child pornography offenders are seeking out pornography only *after* sexually abusing children, then increasing the punishment for possessing child pornography…will not protect children from sexual abuse" [26, p. 28].

The current sentencing also guidelines suggest increasing the base level for offenses involving electronic distribution of images and large collections of images. However, Basbaum argues these sentence enhancements should be amended in order to "incorporate a realistic understanding of how file-sharing works and [how] evolving technology permits defendants to download massive numbers of images with little effort or even intent" [25, pp. 3-4]. The number of images and use of electronic means for distribution may not reflect the offender's risk for recidivism or level of dangerousness toward children. Technological advances have clearly impacted the prevalence of child pornography by making it easier and more readily available compared to the pre-Internet era. Consequently, the post-Internet child pornography consumer may be different from the pre-Internet child pornography user who had a more difficult and risky time accessing the materials [see 26]. Overall, "a defendant [may] download large numbers of child pornography images not so much out of a specific desire . . . but simply because it is easy to do so" [25, p. 21].

Basbaum recommends the United States Sentencing Commission reduce the base level for the possessors of child pornography with no history of hands-on or contact offenses [25]. In addition, the specific offense characteristic involving the distribution of child pornography via electronic means should not enhance cases of simple possession using file-sharing. Finally, the characteristic that enhances the base level sentence for offenses involving large quantities of images should be modified to reflect the ease of which images are available and accessible due to the Internet [25]. The suggested amendments to the current sentencing guidelines take into account the available scientific literature thereby justifying base levels and sentence enhancements on *empirical evidence* rather than *moral panic*.

4.1 Conclusion

The United States federal laws, sentencing guidelines, and Internet censoring tactics mirror the social and political moral panic in response to the globalization of Internet

child pornography. However, the underlying psychological and physical abuse associated with the production of child pornography remains the same regardless of whether it occurred during the pre or post-Internet era. Child pornography involves the recording of a sexual crime against minors, and any technological advances, such as the Internet, are not creating a "new crime" but rather "modernizing" an ancient behavior [see 3]. The United States federal laws and sentencing guidelines need to reevaluate the reasons behind punishing possessors, distributors, and producers of Internet child pornography. If child pornography is not protected under the First Amendment in order to prevent the sexual abuse of children, then this rationale does not easily apply to criminalizing pseudo or computer-generated images. After all, research suggests those individuals who possess child pornography images are not at a greater risk for becoming child sex offenders. Instinctively, one might assume this relationship would exist, however, without empirical backing, this assumption remains intuitive – and society deserves just and unbiased laws, which are not based on emotions and gut-reactions. The authors are not arguing Internet child pornography should be legal, but as difficult as it may be, future legislative, judicial, and social opinions should focus on the facts of the offense rather than the underlying emotions it draws.

Legal policy makers should continue to search for and encourage empirical research, which assesses the relationship between the offense behaviors (e.g., possession) and the individual's motivation or intentions (e.g., curiosity). Also, the size and content of the collections might indicate a general need or addiction to sexual stimuli, such as other forms of deviant pornography, rather than an intense sexual arousal toward children (pedophilia). Finally, filtering software and the blocking techniques used by Internet Service Providers are creating a "house of mirrors" by distorting the real problem – the sexual abuse of children. This trend only provides the public with a false sense of security, and government policy and legislation is not enough to combat this war in cyberspace. Instead, self-regulation is needed on behalf of the ISP and the general public who can anonymously report suspected child sex abuse websites to various cyber tip hotlines and law enforcement agencies. In addition, children who want to gain access to inappropriate material will, so guardians need to establish an open line of communication about the materials available on the Internet rather than shifting the parenting role to a filtering software tool. Overall, national and international legislation should focus on funding law enforcement initiatives to end the sexual abuse of children while encouraging citizens and ISPs to self-monitor and report the existence of child pornography to hotlines and child protection agencies.

References

1. Jenkins, P.: Beyond tolerance: Child pornography on the internet. New York University Press, New York (2001)
2. Duncan, K.: Child pornography and First Amendment standards. Mississippi Law Journal 76, 677–703 (2007)
3. Tate, T.: Child Pornography: An Investigation. Methuen, London (1990)

4. Michaels, R.: Criminal Law – The insufficiency of possession in prohibition of child pornography statutes: Why viewing a crime scene should be criminal. West New England Law Review 30(3), 817–866 (2008)
5. Akdeniz, Y.: Internet child pornography and the law: National and international responses. Ashgate Publishing Company, Burlington (2008)
6. Adler, A.: The perverse law of child pornography. The Columbia Law Review 101(2), 209–273 (2001)
7. United States Sentencing Commission. The history of the child pornography guidelines (2009), http://www.ussc.gov/general/20091030_History_Child_Pornography_Guidelines.pdf (retrieved)
8. Mota, S.A.: The U.S. Supreme Court addresses the Child Pornography Prevention Act and Child Online Protection Act in Ashcroft v. Free Speech Coalition and Ashcroft v. American Civil Liberties Union. Federal Communications Law Journal 55(1), 85–98 (2002)
9. Akdeniz, Y.: The regulation of pornography and child pornography on the internet. Journal of Information, Law, and Technology 1 (2002), http://ssrn.com/abstract=41684 (retrieved) or doi:10.2139/ssrn.41684
10. PROTECT Act, S. 151, 108th Cong. (2003), http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=108_cong_bills&docid=f:s151enr.txt.pdf (retrieved)
11. Protection of Children From Sexual Predators Act of 1998, H.R. 3494, 105th Cong. (1998), http://thomas.loc.gov/cgi-bin/query/C?c105:./temp/~c105xXcSuG (retrieved)
12. PROTECT Our Children Act of 2008, S. 1738, 110th Cong. (2008), http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=110_cong_bills&docid=f:s1738enr.txt.pdf (retrieved)
13. Wortley, R., Smallbone, S.: Child pornography on the internet. Problem-Oriented Guides for Police Problem-Specific Guides Series No. 41. Retrieved from the U.S. Department of Justice, Office of Community Oriented Policing Services website (2006), http://www.cops.usdoj.gov
14. Sutton, L.: Internet filtering software and its effects. Encyclopedia of Library and Information Sciences 3, 2977–2982 (2010), doi:10.1081/E-ELIS3-120044425
15. Morris, J.B., Wong, C.M.: Revisiting user control: The emergence and success of a First Amendment theory for the internet age. First Amendment Law Review 8, 109–137 (2009)
16. Bartow, A.: Open access, law, knowledge, copyrights, dominance and subordination. Lewis & Clark Law Review 10(4), 869–884 (2006)
17. Hakim, D. Net providers to block sites with child sex. The New York Times (June 10, 2008), http://www.nytimes.com (retrieved)
18. Dedman, B., Sullivan, B.: ISPs are pressed to become child porn cops: New Law, new monitoring technology raise concerns about privacy (October 16, 2008), http://www.msnbc.msn.com (retrieved)
19. Combating child abuse on the web: Germany resists EU plans to block child porn sites. Spiegel Online (March 3, 2010), http://www.spiegel.de/international (retrieved)
20. McNamee, J.: Out of sight, out of mind. Index on Censorship 39(1), 108–117 (2010), doi:10.1177/0306422010362320
21. Bowen, K.: Blocking access to child porn doesn't help victims, expert says. Interview by S. Sinico (August 6, 2009), http://www.dw-world.de (retrieved)

22. McNamee, J.: Pointless action on child pornography: Blocking websites that show images of child abuse doesn't work – but EU politicians still think it is a better policy than deletion. The Guardian (March 29, 2010), http://www.guardian.co.uk (retrieved)
23. Malamuth, N., Huppin, M.: Drawing the line on virtual child pornography: Bringing the law in line with the research evidence. N.Y.U. Review of Law and Social Change 31, 773–790 (2007)
24. Bourke, M.L., Hernandez, A.E.: The 'Butner study' redux: A report of the incidence of hands-on child victimization by child pornography offenders. Journal of Family Violence 24, 183–191 (2009)
25. Basbaum, J.P.: Sentencing for possession of child pornography: A failure to distinguish voyeurs from pederasts. Hastings Law Journal 61, 1–24 (2010)
26. Hessick, C.B.: Disentangling child pornography from child sex abuse. Washington University Law Review 88 (2010)