PROTECTING THE CHILDREN: CHALLENGES THAT RESULT IN, AND CONSEQUENCES RESULTING FROM, INCONSISTENT PROSECUTION OF CHILD PORNOGRAPHY CASES IN A TECHNICAL WORLD

By Francis S. Monterosso*

Cite as: Francis S. Monterosso, Note: *Protecting the Children: Challenges that Result In, and Consequences Resulting From, Inconsistent Prosecution of Child Pornography Cases in a Technical World*, XVI Rich. J.L. & Tech. 11 (2010), http://jolt.richmond.edu/v16i3/article11.pdf.

INTRODUCTION

Of all the sinister things that Internet viruses do, this might be the worst: They can make you an unsuspecting collector of child pornography. Heinous pictures and videos can be deposited on computers by viruses—the malicious programs better known for swiping your credit card numbers. In this twist, it's your reputation that's stolen. Pedophiles can exploit virus-infected PCs to remotely store and view their stash without fear they'll get caught.

* Francis S. Monterosso is a Villanova University School of Law, J.D. candidate 2011, is a member of the Villanova Law Review, and graduated *magna cum laude* in 2008 with a B.S. in economics and finance from Boston College. This note won the 2010 University of Richmond's JOLT Biennial Writing Competition. The author would like to thank the Honorable Ronald C. Nagle for his invaluable guidance and Professor Ann Juliano for her priceless encouragement. The author would also like to thank the members of the Villanova Law Review and the University of Richmond's JOLT. I am forever thankful to my family, both those still living and those who are watching over me, and my friends, who have constantly supported me in all of my endeavors.

> Pranksters or someone trying to frame you can tap viruses to make it appear that you surf illegal Web sites. Whatever the motivation, you get child porn on your computer—and might not realize it until police knock at your door.[1]

Operating under an enormous social impact associated with inconsistently prosecuting child pornography cases, new defenses involving the *possession* requirement under the Child Pornography Prevention Act (CPPA), such as the increasingly raised Trojan Horse Defense, have courts scrambling for clarity when determining the possession element in child pornography cases.[2] Quandaries concerning the element of possession result from discrepancies among courts as to whether or not a child pornography defendant must actively download the pornographic material.[3] While some courts demand the government prove the defendant downloaded the material, other courts consider the discovery of child pornography in the Internet cache of the defendant's

[1] Associated Press, *Framed for Child Porn – by a PC Virus*, MSNBC, Nov. 8, 2009, http://www.msnbc.msn.com/id/33778733/ns/technology_and_science-security/.

[2] *See* United States v. Plugh, 576 F.3d 135, 138 (2d Cir. 2009) (showing defendant initially claimed that his computer was infected with a virus that downloaded child pornography onto his computer); United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002) (addressing what constitutes possession when dealing with Internet child pornography); United States v. Grober, 595 F. Supp. 2d 382, 408 (D.N.J. 2008) (calling dissemination of child pornography a "grave impact on society").

[3] *See* United States v. Shaffer, 472 F.3d 1219, 1220–21 (10th Cir. 2007) (finding defendant guilty under the CPPA for downloading child pornography); United States v. Romm, 455 F.3d 990, 999 (9th Cir. 2006) (citing United States v. Mohrbacher, 182 F.3d 1041, 1048–51 (9th Cir. 1999)) (expressing the court's intent that when defendant physically downloads child pornography that defendant may be prosecuted for possessing child pornography); *Stulock*, 308 F.3d at 925 (finding defendant not guilty because conviction under the CPPA requires that defendant download, not merely view, child pornography); United States v. Navrestad, 66 M.J. 262, 268 (C.A.A.F. 2008) (concluding that where defendant neither downloaded nor saved child pornography to his hard drive, he could not be found guilty under pertinent child pornography laws).

computer sufficient to prove the possession element.[4] Further, many courts refuse to convict defendants who merely viewed the child pornography.[5]

Shedding light on the possession issue is the "intent to view" language the 2008 amendments to the CPPA added to the act.[6] The social impact of inconsistent prosecutions in child pornography cases is immense, and courts must remember the extensive legislative history behind Congress's enactment of the CPPA when determining possession in child pornography cases. Against the amended language, courts should find that downloading child pornography, discovering it in the Internet cache, and/or merely viewing such material all constitute "intent to view" and satisfy the possession requirement of the CPPA.[7]

Through the passage of the CPPA, Congress sought to protect children from becoming victims of sexual abuse via the production, dissemination, and possession of child pornography.[8] More recently, courts have inconsistently decided similar child pornography cases due to novel issues associated with proving the possession element of the CPPA

[4] *See infra* note 18 and accompanying text (further discussion of Internet Cache).

[5] *See, e.g.*, United States v. Kuchinski, 469 F.3d 853, 862–63 (9th Cir. 2006) (upholding precedent that defendants who merely view child pornography and unknowingly save files to the Internet Cache or Temporary Internet Files cannot be convicted of possession of child pornography under the CPPA).

[6] *See* 18 U.S.C. § 2252A(a)(5)(B) (Supp. II 2008).

[7] *See id.*

[8] 18 U.S.C. § 2252A(a)(5)(B) (Supp. II 1996) ("Any person who . . . knowingly possesses any book, magazine, periodical, film, videotape, computer disk, or any other material that contains 3 or more images of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, shall be punished as provided in subsection (b)."); *see* H.R. 3726, 109th Cong. § 2 (2005); H.R. 4331, 104th Cong. § 2 (1996); H.R. 4123, 104th Cong. § 2 (1996); S. 1237, 104th Cong. § 2 (1995) (setting forth the reasons why legislation to protect children from child pornography is imperative).

and difficulties that arise when defendants raise the Trojan Horse Defense.[9] While successful uses of these defenses in England provide the defenses with some legitimacy, it is imperative that courts do not neglect to consider the intent behind Congress's enactment of the CPPA when scrutinizing these cases.[10]

As the Internet continues to expand, so too does the ability of sexual predators to easily produce and propagate child pornography globally.[11] As one commentator notes:

> [C]omputers with Internet access have become a frightful weapon by creating a new avenue for sexual offenders to produce, exploit, and disseminate illicit images, particularly those relating to child pornography. The accessibility, affordability, and anonymity presented by downloading

[9] *See* United States v. Plugh, 576 F.3d 135, 138 (2d Cir. 2009) (discussing defendant's attempt to invoke the Trojan Horse Defense and later admitting that he falsified the claim); United States v. Shiver, 305 F. App'x 640, 643 (11th Cir. 2008) (arguing that a computer virus downloaded child pornography on defendant's computer which resulted in his indictment); United States v. Miller, 527 F.3d 54, 65 (3d Cir. 2008) (discussing how defendant claimed that a computer virus, not defendant, downloaded child pornography); United States v. O'Keefe, 461 F.3d 1338, 1341, 1345 (11th Cir. 2006) (discussing defendant's conviction despite his Trojan Horse Defense); United States v. Bass, 411 F.3d 1198, 1200 (10th Cir. 2005) (convicting defendant despite his argument that a computer virus saved child pornography images on his computer); United States v. Vaughn, Cr. No. F. 05-00482 OWW, 2008 WL 4104241, at *22 (E.D. Cal. Sept. 3, 2008) (rejecting post-trial argument of Trojan Horse Defense).

[10] *See* John Schwartz, *Acquitted Man Says Virus Put Pornography on Computer*, N.Y. TIMES, Aug. 11, 2003, at C1, *available at* http://www.nytimes.com/2003/08/11/technology/11PORN.html?scp=1&sq=%22Acquitted%20Man%20Says%20Virus%20Put%20Pornography%20On%20Computer%22&st=cse (discussing how defendant in England successfully utilized the Trojan Horse Defense in his child pornography case).

[11] *See* Emily Brant, Comment, *Sentencing "Cybersex Offenders": Individual Offenders Require Individualized Conditions when Courts Restrict Their Computer Use and Internet Access*, 58 CATH. U. L. REV. 779, 782 (2009) (discussing how laws have been enacted that prevent judges from implementing specific restrictions on sex offenders regarding their ability to access computers connected to Internet and Internet websites).

> child pornography from the Internet has created a "nearly perfect medium for offenders seeking children for sex."[12]

As sexual offenders become more Internet savvy, courts must be armed with knowledge regarding the typical problems associated with these prosecutions and the novel defenses that will likely be raised. Courts should diligently attempt to prosecute these Internet child pornography cases consistently with Congress's intent behind the CPPA to prevent the sexual abuse of children that stems from child pornography.

Although Congress enacted the CPPA in 1996, the Act underwent significant amendments in October of 2008.[13] These amendments are

---

[12] *Id.* at 780 (citing Art Bowker & Michael Gray, *An Introduction to the Supervision of the Cybersex Offender*, FED. PROBATION, Dec. 2004, at 3); *see also* Andrew Bates & Caroline Metcalf, *A Psychometric Comparison of Internet and Non-Internet Sex Offenders from a Community Treatment Sample*, 13 J. SEXUAL AGGRESSION 11, 11 (2007) ("[A]ccess to . . . 'child pornography' . . . has been made much easier than ever before [as a result of the growth of the Internet] . . . .").

[13] Originally, the provision read:

> Any person who . . . knowingly possesses any book, magazine, periodical, film, videotape, computer disk, or any other material that contains 3 or more images of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, shall be punished as provided in subsection (b).

18 U.S.C. § 2252A(a)(5)(B) (Supp. II 1996). As amended in 2008, it reads:

> Any person who . . . knowingly possesses, or knowingly accesses *with intent to view*, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; . . . shall be punished as provided in subsection (b).

notable because of their addition of the language "intent to view."[14] Prior to these amendments, there was no law criminalizing the mere viewing of child pornography in the United States.[15] But despite the 2008 amendments to the CPPA, courts will seemingly still face similar problems concerning the possession requirement and the Trojan Horse Defense.

Compounding the issue of possession is that courts must now determine what constitutes "intent to view."[16] Although Congress has evidently criminalized the mere viewing of child pornography, it has also attempted to expand the CPPA through the language of the 2008 amendments.[17] When a defendant has pornography in his Internet Cache and/or Temporary Internet Files, regardless of whether or not the defendant downloaded or manually saved the child pornography to the computer's hard drive, the CPPA requires the defendant's conviction.[18]

---

18 U.S.C. § 2252A(a)(5)(B) (Supp. II 2008) (emphasis added).

[14] 18 U.S.C. § 2252A(a)(5)(B) (Supp. II 2008).

[15] *See, e.g.*, United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002) (discussing the district court's holding that merely viewing child pornography images without intentionally downloading or saving the images does not satisfy the possession element of the CPPA); United States v. Navrestad, 66 M.J. 262, 268 (C.A.A.F. 2008) (holding that viewing images of child pornography without saving or downloading the images does not constitute possession).

[16] 18 U.S.C. § 2252A(a)(5)(B) (Supp. II 2008).

[17] *See id.*

[18] *See* United States v. Romm, 455 F.3d 990, 993 n.1 (9th Cir. 2006) ("The 'internet cache' or 'internet temporary folder' is a 'set of files kept by a web browser to avoid having to download the same material repeatedly. Most web browsers keep copies of all the web pages that you view, up to a certain limit, so that the same images can be redisplayed quickly when you go back to them.'") (quoting DOUGLAS DOWNING ET AL., DICTIONARY OF COMPUTER AND INTERNET TERMS 149 (8th ed. 2003)); *Stulock*, 308 F.3d at 925 ("The browser cache contains images automatically stored by the computer when a web site is visited so that upon future visits the images need not be downloaded again, thereby improving the response time. Unlike the other files recovered, the images in the browser cache had not been deleted and then recovered."); United States v. Tucker, 305 F.3d 1193, 1198 n.7 (10th Cir. 2002) (defining an Internet cache as "a location on a

Therefore, although Congress attempted to resolve the problems surrounding the possession element of the CPPA through the 2008 amendments, courts will still have to determine how to execute the amendments.

This note untangles courts' problems with the prosecution of child pornography defendants and aims to redirect attention to the social impact associated with these crimes. Part I sets forth the evolution of the CPPA and its goals and shortcomings. Part II further explains the development of child pornography prosecutions in the United States through two cases that illustrate the government's desire to prosecute child pornography defendants.

Moreover, Part II explains the difficulties courts have encountered in the prosecution of child pornography cases due to questions arising out of the possession element of child pornography statutes and from the frequently invoked Trojan Horse Defense. It will clarify problems that courts will continue to face, regardless of the recent amendments to the CPPA, and challenges that courts should understand.

Part III discusses the tremendous impact that child pornography has on society and demonstrates that inconsistent prosecutions of child pornography cases only furthers this negative social impact. Part III also explicates how Congress enumerated many reasons for enacting the CPPA and intended for the Act to be used to decrease and eliminate the dissemination of child pornography in the United States. Finally, Part IV offers a conclusion affirming the struggles that courts face when prosecuting child pornography defendants and the necessity for courts to consider Congress's intent through the enactment of the CPPA and similar laws.

computer's hard drive that contains 'a collection of data images typically that have been gleaned from your travels around the Internet.'").

I. BACKGROUND

A. The Problematic Development of the Child Pornography Prevention Act

Although numerous cases have argued that the CPPA is unconstitutional for overbreadth reasons, the Supreme Court and lower courts have consistently upheld its constitutionality and found that the First Amendment does not protect the production and dissemination of child pornography.[19] The only substantial limitation on the CPPA came from the Supreme Court's decision in *Ashcroft v. Free Speech Coalition*.[20] The *Ashcroft* court determined that the provision of the CPPA that criminalized "virtual child pornography," that is, materials which appear to involve minors partaking in sexual conduct, but which are produced using computer technology or legal consenting adults who look like minors, was substantially overbroad.[21] Regardless of the *Ashcroft*

[19] *See, e.g.*, New York v. Ferber, 458 U.S. 747, 764 (1982) (holding that the First Amendment does not protect child pornography); Free Speech Coal. v. Reno, 198 F.3d 1083, 1097 (9th Cir. 1999) (finding that while certain amendments to the CPPA contain unconstitutionally vague language, "the law is enforceable"); *see also* Osborne v. Ohio, 495 U.S. 103, 111 (1990) (holding that an Ohio statute "may constitutionally proscribe the possession and viewing of child pornography").

[20] 535 U.S. 234, 256, 258 (2002) (finding the CPPA provisions banning virtual child pornography unconstitutional because they violated the First Amendment as overbroad).

[21] *Id.* at 239–41. Prior to the *Ashcroft* decision, the CPPA criminalized receipt, possession, and distribution of child pornography and virtual pornography, which does not utilize real minors. 18 U.S.C. § 2256(8)(B) (Supp. II 1996). The *Ashcroft* court reasoned:

> The CPPA prohibits speech despite its serious literary, artistic, political, or scientific value. The statute proscribes the visual depiction of an idea-that of teenagers engaging in sexual activity-that is a fact of modern society and has been a theme in art and literature throughout the ages. . . . Both themes-teenage sexual activity and the sexual abuse of children-have inspired countless literary works. . . . Contemporary movies pursue similar themes. . . . Whether or not [these contemporary films] violate the CPPA, they explore themes within the wide sweep of the statute's prohibitions. If these films, or hundreds of others of lesser note that explore those subjects, contain a single graphic depiction of

decision, courts have frequently and consistently utilized the CPPA and its amendments.[22]

B. *New York v. Ferber* and Its Expansion in *Osborne v. Ohio*

Not only has Congress established a multitude of reasons for convicting defendants for possession of child pornography, but the Supreme Court has also expressed its opinion on the importance of protecting children from sexual abuse.[23] In *New York v. Ferber*, the Supreme Court outlined five specific reasons why it is imperative to deem child pornography as illegal and unprotected by the First Amendment to United States Constitution.[24]

First, states have an interest "in 'safeguarding "the physical and psychological well-being of a minor."'"[25] Second, child pornography is a "permanent record" of the harmful acts done to minors, and the government aims to prevent further distribution of such illegal material.[26] Third, "[t]he advertising and selling of child pornography" works to

> sexual activity within the statutory definition, the possessor of the film would be subject to severe punishment without inquiry into the work' s redeeming value. This is inconsistent with an essential First Amendment rule: The artistic merit of a work does not depend on the presence of a single explicit scene.

Ashcroft, 535 U.S. 246–48. Therefore, the section of the CPPA that corresponded to criminalizing virtual child pornography was stricken as unconstitutional. *Id.* at 258.

[22] *See supra* notes 13–15 (discussing the 2008 amendments to the CPPA).

[23] *See Osborne*, 495 U.S. at 110; *Ferber*, 458 U.S. at 749.

[24] *Ferber*, 458 U.S. at 756–64; *cf.* Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942) (enumerating narrow classes of speech, the prevention of which has never raised a constitutional problem).

[25] *Ferber*, 458 U.S. at 756–57 (quoting Globe Newspaper Co. v. Superior Court, 457 U.S. 596, 607 (1982)).

[26] *Id.* at 759.

continue to promote the economic incentive to the child pornography business.[27] Fourth, there is little to no value associated with child pornography.[28] Fifth, there is a necessity in protecting children.[29] It is therefore imperative that the legislative intent associated with the CPPA not be neglected when courts encounter difficulties either in establishing the possession element of the CPPA or with theoretical defenses.

II. ANALYSIS

A. Problems Associated with Proving the Possession Element of the CPPA

Possession is the most frequently argued element of the CPPA.[30] Because Congress and states refuse to define "possession" in the CPPA and in related state child pornography laws, individual courts each face the task of defining the term.[31] This has led to courts inconsistently determining child pornography cases based on whether or not the defendant "knowingly possessed" the illegal pornographic material under the CPPA and its military and state law equivalents.[32] Some courts convict

[27] *Id.* at 761.

[28] *Id.* at 762.

[29] *Id.* at 763–64.

[30] *See, e.g.*, United States v. Shaffer, 472 F.3d 1219, 1226 (10th Cir. 2007) (discussing mens rea required for "possession" under the CPPA); United States v. Romm, 455 F.3d 990, 1000–02 (9th Cir. 2006) (concluding that defendant satisfied possession element of the CPPA by viewing child pornography and having it stored in Internet Cache).

[31] *See Romm*, 455 F.3d at 999 (determining that "Congress intended to apply traditional concepts of possession" under the CPPA); State v. Scolaro, 910 N.E.2d 126, 133 (Ill. App. Ct. 2009) ("Illinois's child-pornography statute does not define 'possess.'"); Commonwealth v. Simone, 63 Va. Cir. 216, 259 (2003) ("The Virginia child pornography statute does not define 'possession,' nor has this Court found any opinions of Virginia courts addressing this issue.").

[32] *Compare Romm*, 455 F.3d at 1000–01 (concluding that viewing child pornography and storing images in the Internet Cache satisfied the possession element of the CPPA), United States v. Tucker, 305 F.3d 1193, 1205 (10th Cir. 2002) (determining that although defendant never downloaded child pornography he was still guilty under the CPPA

defendants when they merely view child pornography websites that automatically save the material in the viewer's Temporary Internet Files or Internet Cache, while other courts have determined that these situations do not lead to a conviction.[33]

Although the October 2008 amendments to the CPPA include "intent to view" as a form of possession, it is still unclear as to whether the issues related to proving the element of possession have been solved.[34] Therefore, because the fundamental purpose behind the Act is to protect children from sexual abuse, courts should convict when child pornography files are located in the Internet Cache.[35] Courts should especially convict when computer forensic expert examiners discover that the defendant searched for child pornography on the Internet, regardless of whether or not the user physically downloaded any files.[36]

---

because he was aware it was being stored in the web browser's cache), *and Scolaro*, 910 N.E.2d at 131–32 (determining that controlling images in a computer hard drive's Internet Cache satisfied the possession element), *with* United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002) (stating the district court's finding that a defendant cannot be guilty of possession of a picture stored in an Internet browser's cache "without having purposely saved or downloaded the image"), *and* United States v. Navrestad, 66 M.J. 262, 268 (C.A.A.F. 2008) (explaining that defendant could not be convicted of possessing child pornography because although the public computer used to access Internet and illegal pornographic material saved images in Temporary Internet Files, defendant was unaware of this process and was not in control of child pornography).

[33] *See* cases cited *supra* note 32.

[34] For a further discussion on how courts will seemingly continue to face issues associated with the possession element of the CPPA and the Trojan Horse Defense, see *infra* notes 116–118 and accompanying text.

[35] "The Government has a compelling State interest in protecting children from those who sexually exploit them, and this interest extends to stamping out the vice of child pornography at all levels in the distribution chain.". H.R. 3726, 109th Cong. § 2(2)(C) (2005); *see also* H.R. 4331, 104th Cong. §2 (1996); H.R. 4123, 104th Cong. §2 (1996); S. 1237, 104th Cong. §2 (1996); S. 1237, 104th Cong. §2 (1995).

[36] *See Stulock*, 308 F.3d at 926 (8th Cir. 2002) (finding no clear error in the decision that defendant's search for and receipt of child pornography was sufficient to establish possession); *Scolaro*, 910 N.E.2d at 133 (holding that to determine possession the court

1. Downloading as a Requirement to Convict in *United States v. Stulock*

Although the 2008 amendments to the CPPA include an additional way for a person to be convicted for child pornography with the "intent to view" language, courts must still determine if they will require defendants to have downloaded the child pornography in order to satisfy either the possession or "intent to view" elements of the CPPA.[37] Prior to the 2008 amendments, the only way courts consistently convicted child pornography defendants was when the defendants physically controlled the illegal paraphernalia by downloading the material.[38] By concluding that "possession" or "intent to view" can be satisfied only when the child pornography defendant has downloaded the material, courts permit numerous other defendants to bypass conviction under the CPPA.

In *United States v. Stulock*, the court convicted the defendant of receiving child pornography but acquitted him of a charge for possessing child pornography.[39] This outcome illustrates courts' inconsistencies in deciding child pornography cases. If a defendant receives child pornography, he must also possess it.[40]

In *Stulock*, authorities raided a business known to use the Internet to sell child pornography.[41] During the raid, law enforcement officers discovered a customer list that provided names and e-mail addresses of those people who had purchased child pornography from the company.[42]

---

must ask if "defendant specifically [sought] out the prohibited images and [if] he [had] the ability to exercise dominion and control over these images").

[37] 18 U.S.C. § 2252A(a)(5)(B) (Supp. II 2008).

[38] *See supra* notes 30–32 and accompanying text.

[39] 308 F.3d at 925.

[40] *See id.*

[41] *Id.* at 924.

[42] *Id.*

Once Stulock's information was obtained from the confiscated customer list, officers set up a scheme to lure former customers of the raided company into ordering more child pornography.[43] Stulock ultimately purchased some child pornography from the sting operation.[44] Through this purchase, law enforcement obtained a search warrant for Stulock's home and seized his computer.[45]

Upon searching Stulock's computer, agents discovered that Stulock searched for and visited numerous child pornography websites and that he had deleted child pornography files off his computer.[46] Computer forensics recovered these files in the hard drive's Temporary Internet Files.[47] When a computer has images, including child pornography, in the Temporary Internet Files, computer forensic experts infer that the computer user "had either purposely downloaded the image in a ZIP file or had opened an image stored elsewhere on the disk using a viewer that created a temporary copy."[48]

The problem in *Stulock* was that the court, unconvinced by the evidence presented at trial regarding the possession of child pornography charge,[49] required evidence that the defendant had physically downloaded the illegal pornographic material.[50] The defendant argued that he did not

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.* at 926 (acknowledging that "pop-ups and other techniques" might "account for some of the" child pornography).

[50] *Id.* at 925.

knowingly possess the illegal material and that "aggressive [I]nternet porn sites" placed child pornography onto his computer.[51] The court concluded:

> Although [aggressive pornography websites and pop-ups] could account for some of the material, viewing the evidence as a whole, [the court could not] say it was clear error to find that Stulock's possession of images containing violent child pornography was an act committed during his search for and receipt of the child pornography video that was the basis of the charged offense.[52]

The *Stulock* court ultimately convicted the defendant for receiving child pornography, but it neglected to consider Congress's intent in enacting the CPPA when the court acquitted Stulock of the possession of child pornography charge.[53] Under the 2008 amendments, with "intent to view" as an additional avenue of convicting a defendant, the *Stulock* court would arguably still struggle to convict the defendant.[54] However, courts facing similar situations should not require evidence that defendants physically downloaded the child pornography in order to convict.

2. The Development of Cache as a Fulfillment of Possession

While some American courts convict child pornography defendants when law enforcement agents seize their computers and discover child pornography in the Temporary Internet Files or Internet Cache of the computer's hard drive, other courts require the defendant to download the illegal material in order to convict.[55] Two fundamental child

---

[51] *Id.* at 926.

[52] *Id.*

[53] *See id.* at 925; *see also* United States v. Romm, 455 F.3d 990, 999 (9th Cir. 2006) (finding congressional intent behind the CPPA was "to apply traditional concepts of possession"); H.R. 3726, 109th Cong. § 2 (2005); H.R. 4331, 104th Cong. § 2 (1996); H.R. 4123, 104th Cong. § 2 (1996); S. 1237, 104th Cong. § 2 (1995).

[54] *See* 18 U.S.C. § 2252A(a)(5)(B) (Supp. II 2008).

[55] *See supra* note 32 and accompanying text.

pornography cases found defendants guilty of possessing illegal pornography when they merely viewed the material and were aware that their computers saved the images in folders known as Temporary Internet Files or an Internet Cache.[56] With the 2008 amendments to the CPPA, regardless of a defendant's knowledge that hard drives automatically save images, including child pornography, to his or her cache files, a defendant should be convicted under the "intent to view" theory.[57]

In *United States v. Tucker*, the defendant, a convicted felon, was charged with possessing child pornography after he showed a friend illegal images on his computer and told the friend that he came across a minor girl, whom he hoped to meet.[58] The friend informed the proper authorities, who then arrested the defendant.[59] Upon inspection of the defendant's computer, a computer forensics officer discovered numerous files the defendant recently deleted from his machine, which were "located in the computer's recycle bin and in 'unallocated' hard drive space."[60] Agents also noticed that the defendant frequented sexual newsgroups with names alluding to child pornography.[61]

The *Tucker* court held that the defendant's knowledge that the child pornography images he viewed were automatically saved in the Internet Cache was sufficient to establish possession and thus upheld his

[56] *See, e.g.*, *Romm*, 455 F.3d at 998; United States v. Tucker, 305 F.3d 1193, 1198–99 (10th Cir. 2002).

[57] *See* Enhancing the Effective Prosecution of Child Pornography Act of 2007, Pub. L. No. 110-358, §203, 122 Stat. 4001 (2008) (codified at 18 U.S.C. § 2252A(a)(4)–(5)) (inserting "knowingly accesses with intent to view" to obtain effective prosecution in child pornography cases); *see also Romm*, 455 F.3d at 999 (determining that Congress intended "to apply traditional concepts of possession," such as the exercise of dominion and control).

[58] *Tucker*, 305 F.3d at 1195–96.

[59] *Id.* at 1196–97.

[60] *Id.* at 1197–98.

[61] *Id.* at 1196–97.

conviction.[62] The court determined that proving the defendant not only viewed the images but also knew they would be saved was essential, because viewing without possession was not sufficient to sustain a conviction under the CPPA.[63] Ultimately, the defendant admitted to knowing that when visiting a website, such as one where he could view child pornography, the information from the website would be "sent to his browser cache file and thus saved on his hard drive."[64] Therefore, the court decided the defendant knowingly possessed the child pornography and convicted him under the CPPA.[65]

In *United States v. Romm*, the Ninth Circuit agreed with the *Tucker* court's holding that child pornography defendants may be convicted when the material is knowingly stored in the Internet Cache, even though the material is not downloaded.[66] In *Romm*, the defendant searched for and

[62] *Id.* at 1205. Nearly 5000 child pornography images were discovered on the defendant's computer *Id.* at 1197. Because Tucker consistently deleted child pornography located in the Internet Cache, the court concluded that he was in control of the pornographic images and therefore possessed them. *Id.* at 1204.

[63] *See id.* (acknowledging the defense that defendant merely viewed the material, but rejecting the claim because defendant's actions demonstrated control and possession).

[64] *Id.*

[65] *Id.* at 1204–05; *see also* Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227, 1242 (2004) (explaining that the court found defendant guilty of knowingly possessing child pornography). Howard explains:

> The court similarly rejected Tucker's claim that he could not possess something without affirmatively downloading it. In particular, the court noted that contrary to Tucker's claims, the Internet neither put the images on his computer on its own, nor exercised any volition. Rather, Tucker himself "purposefully visited Internet sites for the express purpose of viewing child pornography . . . ."

Id. (footnotes omitted).

[66] United States v. Romm, 455 F.3d 990, 998 (9th Cir. 2006) (finding that "a person can receive and possess child pornography without downloading it, if he or she seeks it out and exercises dominion and control over it" (citing *Tucker*, 305 F.3d at 1204)).

viewed numerous images of child pornography and "enlarged them," which automatically saved the material to the Internet Cache.[67] The court ultimately convicted the defendant after law enforcement officers discovered forty illegal images the defendant had deleted from the Internet Cache.[68]

At trial, as in *Tucker*, the defendant contended that he did not knowingly possess the child pornography located on his computer due to its automatic transfer to his Internet Cache.[69] The *Romm* court concluded that because the defendant sought out and searched for the child pornography, viewed it, enlarged the images, could copy and print out the illegal material, and knew about the location of the files in the Internet Cache, he knowingly possessed the images, regardless of whether or not he manually downloaded the images.[70] The *Romm* court inferred the defendant's knowledge that viewing child pornography images automatically saves them in the computer's Internet Cache folder; therefore, the court convicted Romm of knowingly possessing child pornography under the CPPA, although he never purposely downloaded illegal material.[71]

Currently, American courts have encountered similar problems that plagued previous courts such as *Tucker*, *Romm*, and *Stulock*.[72] Until future courts adequately define the phrase "intent to view," similar problems associated with possession will continue to arise.[73] "Intent to view" should

[67] *Id.* at 993.

[68] *Id.*

[69] *Id.* at 999.

[70] *Id.* at 1000–01.

[71] *Id.*

[72] *See, e.g.*, State v. Josephitis, 914 N.E.2d 607, 615–16 (2009) (discussing the inconsistencies in determining possession in child pornography cases).

[73] *See* 18 U.S.C. § 2252A(a)(5)(B) (Supp. II 2008).

be satisfied by any acts that would likely lead a reasonable jury to conclude that the defendant viewed child pornography.[74] This reasoning is in regard to situations where illegal material is found in a defendant's Internet Cache regardless of whether or not the defendant knew that the computer stored images in the Internet Cache.[75] Therefore, even if defendants like those in *Tucker* and *Romm* lack adequate knowledge regarding the location of child pornography in their Internet Cache, courts should still convict the defendants.

3. Courts Must Learn and Grow from Past Decisions

Under the original 1996 CPPA, and similar state and military laws, a court would not convict a defendant if it determined that the defendant merely viewed child pornography without downloading the material.[76] It is understandable that Congress wanted to broaden the scope of the Act by adding "intent to view" in the 2008 amendments as a means of convicting defendants of possessing child pornography.[77] Prior to the 2008

[74] "While motive is the inducement to do some act, *intent is the mental resolution or determination to do it*." BLACK'S LAW DICTIONARY 881 (9th ed. 2009) (defining "intent") (emphasis added).

[75] *See supra* Part II.A.2.

[76] *See* United States v. Bass, 411 F.3d 1198, 1207 (10th Cir. 2005) (Kelly, J., dissenting) ("Although reprehensible, *viewing* child pornography is not a crime."); *see also* United States v. Navrestad, 66 M.J. 262, 268 (C.A.A.F. 2008) (stating that when defendant does not save or download child pornography, "viewing alone does not constitute 'control'").

[77] *See* Effective Child Pornography Prosecution Act of 2007, Pub. L. No. 110–358, § 102, 122 Stat. 4001 (2008) (codified at 18 U.S.C. § 2251 note) (explaining Congress's intent of enhancing, effectively, prosecution of child pornography cases). Congress enumerated the reasons for enhancing the CPPA:

> (1) Child pornography is estimated to be a multibillion dollar industry of global proportions, facilitated by the growth of the Internet.
>
> (2) Data has shown that 83 percent of child pornography possessors had images of children younger than 12 years old, 39 percent had images of children younger than 6 years old, and 19 percent had images of children younger than 3 years old.

amendments, many federal and state courts had substantial difficulties in distinguishing the mere viewing of child pornography from convictable possession of the material.[78]

> (3) Child pornography is a permanent record of a child's abuse and the distribution of child pornography images revictimizes the child each time the image is viewed.
>
> (4) Child pornography is readily available through virtually every Internet technology, including Web sites, email, instant messaging, Internet Relay Chat, newsgroups, bulletin boards, and peer-to-peer.
>
> (5) The technological ease, lack of expense, and anonymity in obtaining and distributing child pornography over the Internet has resulted in an explosion in the multijurisdictional distribution of child pornography.
>
> (6) The Internet is well recognized as a method of distributing goods and services across State lines.
>
> (7) The transmission of child pornography using the Internet constitutes transportation in interstate commerce.

Id.

[78] *See* Commonwealth v. Simone, 63 Va. Cir. 216, 262 (2003) (providing analogy to situation of determining mere viewing or possession in child pornography cases). The court in *Simone* explained that:

> By analogy, one might consider the following hypothetical. If a person walks down the street and notices an item (such as child pornography or an illegal narcotic) whose possession is prohibited, has that person committed a criminal offense if they look at the item for a sufficient amount of time to know what it is and then walks away? The obvious answer seems to be "no." However, if the person looks at the item long enough to know what it is, then reaches out and picks it up, holding and viewing it, and taking it with them to their home, that person has moved from merely viewing the item to knowingly possessing the item by reaching out for it and controlling it.

Id. See also Howard, *supra* note 65, at 1265–66 (presenting illustration comparing mere viewing of child pornography and possessing it). Howard questions that if a bookstore patron, Peter Patron, requests child pornography magazines, sits in a chair, and peruses

Furthermore, there was a strong argument that when a person "merely viewed" child pornography, he actually did a great deal more than simply look at illegal material.[79] In order to "merely view" child pornography from the Internet, a defendant must search for, access, and view or enlarge videos or images depicting child pornography.[80] That entire process would have to occur prior to the defendant having the capability of actually viewing the material.[81] Applying the amended version of the CPPA to cases such as *Stulock* would likely lead the courts to find the defendants guilty of possessing child pornography, as the defendants sought out and viewed illegal material on multiple occasions.[82]

---

the magazines, has he possessed the contraband if he does not purchase it? Howard continues:

> But is Peter just looking at the images? Consider an addition to the analogy: after Peter sat down and began looking at the child pornography, police enter the store and immediately approach Peter. With the magazine still in his hand, open to pages with sexually explicit images of children, Peter is arrested for possession of child pornography. Later at trial, Peter's lawyer argues that Peter was merely viewing the images in the magazine and cannot be liable for possessing them. However, the prosecution offers evidence that Peter specifically requested the magazines that he knew contained child pornography and received those magazines. Upon receipt, the magazines were under Peter's dominion and control – he flipped through them, turned them at various angles, unfolded the centerfold, copied them on the bookstore's copy machine, showed them to other patrons, ripped pages from them, attempted to steal the entire magazine by secreting it in his backpack, and so on. Based on that evidence, there seems little doubt that, at the moment the police arrested Peter, Peter knowingly possessed the child pornography.

Id. at 1266.

[79] *See* Howard, *supra* note 65, at 1266–67 (discussing process of viewing child pornography via analogy).

[80] *See id.* at 1267–68 (explaining that it takes effort to view child pornography).

[81] *See id.* at 1268–69 (discussing accidental viewing and that child pornography viewers do not merely stumble across illegal material).

[82] *Compare* United States v. Stulock, 308 F.3d 922, 925–26 (8th Cir. 2002) (affirming the

Therefore, when courts are unsure of whether to convict, they must consider Congress's intent in enacting both the original CPPA and its 2008 amendments, which enhance the prosecution of child pornography defendants.[83]

B. The Developing Trojan Horse Defense

In response to the increase in accessibility of child pornography on the Internet, and therefore a wide array of viruses, child pornography defendants have recently begun raising the Trojan Horse Defense with regularity.[84] A defendant invokes the Trojan Horse Defense in an effort to

---

district court's determination that defendants in child pornography cases cannot be found guilty of possession for merely viewing child pornography), *and* United States v. Navrestad, 66 M.J. 262, 268 (C.A.A.F. 2008) (establishing that like defendants under the CPPA, military members cannot be found guilty of possessing child pornography for merely viewing illegal material), *with* Effective Child Pornography Prosecution Act of 2007, Pub. L. No. 110-358, § 102, 122 Stat. 4001 (2008) (codified at 18 U.S.C. § 2251 note) (explaining Congress's intent of enhancing, effectively, prosecution of child pornography cases).

[83] *See* Effective Child Pornography Prosecution Act of 2007 § 102 (explaining Congress's intention to produce more effective and enhanced convictions of child pornography defendants under the CPPA).

[84] The Trojan Horse Defense is "any defense based on the alleged effects of malware, whether a Trojan horse, virus, worm or other program." Susan W. Brenner et al., *The Trojan Horse Defense in Cybercrime Cases*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1, 11 (2004); *see also* United States v. Plugh, 576 F.3d 135, 138 (2d Cir. 2009) (asserting that defendant lied to agents about "existence of a Trojan virus on his computer"); United States v. McArthur, 573 F.3d 608, 614 (8th Cir. 2009) (disregarding defendant's conflicting argument that a computer virus deposited child pornography in defendant-computer's operating system); United States v. Shiver, 305 F. App'x 640, 643 (11th Cir. 2008) (rejecting defendant's theory that a virus placed child pornography on defendant's computer);United States v. Miller, 527 F.3d 54, 63 & n.8 (3d Cir. 2008) (providing testimony that a virus could download child pornography onto a person's computer); United States v. O'Keefe, 461 F.3d 1338, 1341 (11th Cir. 2006) (rejecting defendant's claim that computer viruses uploaded child pornography onto his websites because the viruses were determined to be incapable of downloading child pornography); United States v. Bass, 411 F.3d 1198, 1200 (10th Cir. 2005) (finding merit in defendant's claim that his computer suffered from a virus that automatically saved illegal child pornography, but determining that defendant was still guilty of possessing the material); United States v. Vaughn, Cr. No. F. 05-00482 OWW, 2008 WL 4104241, at *22 (E.D.

establish a reasonable doubt in the fact-finders' minds by claiming that "Some-Other-Dude-Did-It."[85] A defendant must be found guilty beyond a reasonable doubt to be convicted in a criminal trial; therefore, a successful Trojan Horse Defense will leave the jury reasonably doubtful and lead to the defendant's acquittal.[86] There is a growing concern regarding a defendant's ability to raise this defense to confuse the jury and utilize the jury's ignorance regarding the proper burden of proof.[87]

Cal. Sept. 3, 2008) (discussing defendant's post-trial Trojan Virus Defense theory, which appellate court disregarded and affirmed defendant's conviction of possession of child pornography).

[85] *See* Brenner et al., *supra* note 84, at 10–15 (discussing how Trojan Horse Defense attempts to prevent prosecution from establishing guilt beyond a reasonable doubt). A child pornography defendant who "raises the possibility that a Trojan horse or other variety of malware is responsible for the crime with which he is charged, the prosecution must, in effect, prove a negative beyond a reasonable doubt." *Id.* at 12; *see also* BLACK'S LAW DICTIONARY 1518 (9th ed. 2009) (defining the SODDI – Some-Other-Dude-Did-It – Defense as "a claim that somebody else committed a crime").

[86] *See* Brenner et al., *supra* note 84, at 9–10 (explaining defendant's reasoning in attempting to establish Trojan Horse Defense in conjunction with the SODDI Defense). Brenner stated:

> When defense counsel invites the jury to conclude that the defendant is not guilty because he did not actually do the physical acts charged, or at least the government has not proved beyond a reasonable doubt that he did, defense counsel will almost inevitably have to present at least some suggestion as to who might have done the acts instead. The typical juror will be less likely to develop reasonable doubts in the abstract, than if the defense is able to sketch out some "reasonable" alternative theory that will permit jurors to satisfy their natural human curiosity about dramatic events, and also their sense that real events must have some real-life explanation. As its moniker ("some other dude") implies, the SODDI defense usually attributes the commission of the crime to some unknown perpetrator.

Id. (citing W. William Hodes, *Seeking the Truth Versus Telling the Truth at the Boundaries of the Law: Misdirection, Lying, and "Lying with an Explanation*," 44 S. TEX. L. REV. 53, 59 n.18 (2002)).

[87] *See id.* at 12–14 ("In a criminal prosecution, at least in the United States, the

1. The Treatment of the Trojan Horse Defense in the United Kingdom

The Trojan Horse Defense first proved successful in cases tried in the United Kingdom.[88] In these initial cases, defendants argued that because their computers were infected with viruses that could potentially download illegal material or advertisements, the prosecution was unable to convict them.[89] The defense has likely been successful because jurors fear being similarly situated to the defendant, since Trojan Horse viruses are both easily disguised and common.[90]

government must prove the defendant's guilt beyond a reasonable doubt. This means that if a defendant . . . raises the possibility that a Trojan horse or other variety of malware is responsible for the crime with which he is charged, the prosecution must, in effect, prove a negative beyond a reasonable doubt. That is, to survive a directed verdict of acquittal and persuade the jury to convict such a defendant, the prosecution must disprove the possibility the defense has raised beyond a reasonable doubt. As . . . case[s have] demonstrated, this can be very difficult to do. At least for the present foreseeable future, the availability of the defense raises concerns that defendants will be able to use a jury's ignorance, and likely suspicion, of technology to obtain an acquittal even when the evidence overwhelmingly supports a conviction.").

[88] *See id.* at 8 (discussing defendant, Karl Schofield, who was acquitted of possessing child pornography by raising Trojan Horse Defense); *id.* at 7 & n.17 (citing Schwartz, *supra* note 10) (describing another situation where virus was blamed for downloading child pornography)); *see also* Don Mackay, *Trojan 'Virus' Left Kid Porn on My PC: Karl Cleared After Two-Year Ordeal*, MIRROR (U.K.), Apr. 18, 2003, at § News, *available at* 2003 WLNR 13123469 (explaining first recorded successful invocation of Trojan Horse Defense).

[89] *See* Brenner et al., *supra* note 84, at 8 (asserting early arguments raised by child pornography defendants who raised Trojan Horse Defense).

[90] *See id.* at 4 (explaining how Trojan horse viruses may appear to users as harmless programs). Brenner and her colleagues assert that "[a] Trojan horse program, a variety of malware, is 'a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality.' Malicious functionality could include anything from downloading contraband files to attacking other computers." *Id.* at 4 (quoting ED SKOUDIS & LENNY ZELTSER, MALWARE: FIGHTING MALICIOUS CODE 251 (2004)) (defining Trojan virus).

In most child pornography cases where the Trojan Horse Defense is raised, computer forensic experts are the defendant's only evidence.[91] The Trojan Horse Defense has caused courts and countries, domestically and internationally, to question how child pornography will be argued in the near future.[92] It is imperative that courts are aware of and understand the Trojan Horse Defense because it will immensely impact how child pornography will be prosecuted, and therefore, have a direct effect on the social impact of child pornography.[93]

2. Hesitance in the Application of the Trojan Horse Defense

Although United Kingdom courts have accepted the Trojan Horse Defense as a successful means of acquitting a child pornography defendant, the United States has not followed suit.[94] Only rarely has the

[91] *See* Brenner et al., *supra* note 84, at 8 (discussing how computer forensics was utilized in prosecution of Karl Schofield); *supra* note 9 (discussing cases that utilized computer forensic testimony to discuss the Trojan Horse Defense).

[92] *See* Jamie Smyth, *Can a Virus Put Porn on Your PC?*, IR. TIMES, Jan. 19, 2005, § Features, *available at* 2005 WLNR 718976 (discussing proposals for changes in statutes in cases concerning Trojan Horse Defense).

[93] *See infra* notes 116–123 and accompanying text (discussing how the Trojan Horse Defense has impacted child pornography cases).

[94] *See, e.g.*, United States v. Plugh, 576 F.3d 135, 138 (2d Cir. 2009) (finding that defendant fabricated testimony regarding virus on his computer); United States v. McArthur, 573 F.3d 608, 614 (8th Cir. 2009) (determining evidence insufficient to support defendant's invocation of Trojan Horse Defense); United States v. Shiver, 305 F. App'x 640, 643 (11th Cir. 2008) (determining evidence sufficient to convict defendant of possessing child pornography despite his use of Trojan Horse Defense); United States v. Miller, 527 F.3d 54, 63 n.8, 66 (3d Cir. 2008) (finding evidence sufficient to support inference that defendant downloaded child pornography despite defendant's Trojan Horse Defense); United States v. O'Keefe, 461 F.3d 1338, 1341–45 (11th Cir. 2006) (showing defendant's raising of Trojan Horse Defense insufficient to overcome conviction by jury on possessing child pornography under the CPPA); United States v. Bass, 411 F.3d 1198, 1200–01 (10th Cir. 2005) (finding by jury that defendant was guilty of knowing possession of child pornography though defendant said computer was infected with virus); United States v. Vaughn, Cr. No. F. 05-00482 OWW, 2008 WL 4104241, at *22 (E.D. Cal. Sept. 3, 2008) (determining that Trojan Horse Defense did not lead to a reversal of lower court's decision to convict defendant of possessing child pornography

Trojan Horse Defense been successful in United States courts.[95] Regardless of whether domestic courts have acquitted child pornography defendants based on the Trojan Horse Defense, it is imperative for courts to understand the defense because of its recently frequent usage.[96]

In *United States v. Miller*, the court ultimately found that the convictions against the defendant violated the double jeopardy clause.[97] The court's analysis of the Trojan Horse Defense, however, did not lead to the reversal of Miller's possession of child pornography conviction.[98] The FBI discovered a zip disk in Miller's home that held between 1200 and 1400 images, twenty of which constituted child pornography.[99] The day after Miller's home was searched and the pornography was discovered, the defendant contacted the interviewing FBI agent, Agent Kyle.[100] Miller informed Agent Kyle that the child pornography was likely a result of a virus that had infected Miller's computer a year before the search.[101]

---

under the CPPA).

[95] *See* Brenner et al., *supra* note 84, at 8 n.22 (citing Patricia Dedrick, *Auditor: Virus Caused Errors*, BIRMINGHAM NEWS (Ala.), Aug. 26, 2003, § News, at 142, *available at* 2003 WLNR 15960131 (explaining rare case – tax fraud – where defendant successfully raised Trojan Horse Defense; the jury acquitted the defendant, who blamed a virus for his underreporting over $630,000 in income over a few years).

[96] *See O'Keefe*, 461 F.3d at 1340 (explaining that defendant was appealing district court convictions for receiving, advertising, and possessing child pornography under the CPPA). O'Keefe, a high school math teacher, created two child pornography websites, "hctweens" and "modelquest," which he said he developed to entrap child predators, but "his crusading efforts were thwarted when the websites were hacked into and altered by computer viruses to include pornographic images of children." *Id.* at 1340–41.

[97] *Miller*, 527 F.3d at 73–74.

[98] *Id.* at 66–69.

[99] *Id.* at 58.

[100] *Id.* at 65.

[101] *Id.*

The government's expert witness presented a record that revealed the dates that the pornographic images were created, written, and accessed on the zip disk, substantiating the government's claim that Miller downloaded the material.[102] One agent testified that he was unable to prove sufficiently whether Miller or a virus accessed the images.[103] The *Miller* court used four factors, with a totality of the circumstances approach, to determine that the defendant downloaded and accessed the child pornography.[104] The first factor was "whether images were found on the defendant's computer."[105] The second factor was the number of images of child pornography that were found.[106] The third factor was "whether the content of the images 'was evident from their file names.'"[107] The fourth factor was the "defendant's knowledge of and ability to access the storage area for the images."[108]

At trial, the court convicted Miller of receiving and possessing child pornography.[109] The computer forensic experts in *Miller* "[b]oth . . . acknowledged the possibility that child pornography could be unknowingly downloaded onto a hard drive as the result of a virus, or 'spyware.'"[110] However, the experts disagreed as to whether it was likely that this possibility occurred in Miller's case. "Agent Price testified that he

[102] *Id.*

[103] *Id.*

[104] *Id.* at 67.

[105] *Id.* (citing United States v. Irving, 452 F.3d 110, 122 (2d Cir. 2006)).

[106] *Id.*

[107] *Id.* (quoting United States v. Payne, 341 F.3d 393, 403(5th Cir. 2003)).

[108] *Id.* (citing United States v. Romm, 455 F.3d 990, 997–1001 (9th Cir. 2006)).

[109] *Id.* at 58, 72.

[110] *Id.* at 63 n.8.

was unaware of there ever being . . . 'any reports of a child porn dropping virus.'"[111]

Further, the FBI agent in *Miller* strongly disagreed with the defendant's computer forensic expert's testimony that a virus could download only child pornography, because the agent maintained "that such a virus would have to 'take the zip diskette out of the case, put it into the computer . . . , take the zip out, put it back in the case and delete the original images off the computer.'"[112] Agent Price could only point to the defendant as the cause of the presence of the child pornography.[113] The *Miller* court determined that the defendant's Trojan Horse Defense and accompanying computer forensic expert testimony were too weak to acquit the defendant of the charges; however, due to a double jeopardy violation, the court could not convict Miller for possession of child pornography.[114]

3. Proposed Factors for Analyzing the Trojan Horse Defense

A number of academics and courts have suggested possible ways courts could address situations where a defendant raises the Trojan Horse Defense in order to obtain justice.[115] When considering the Trojan Horse Defense, courts should consider the "repeat behavior model," which

[111] *Id.*

[112] *Id.* Agent Price did not believe that a computer virus would be capable of performing this complex series of functions; therefore, as an expert, he believed that the Trojan Horse Defense was inadequate of leading to an acquittal for Miller. *See id.*

[113] *Id.* at 63 n.8, 66.

[114] *Id.* at 66–69, 73–74.

[115] *See, e.g.*, Brenner et al., *supra* note 84, at 21–37 (explaining ways for prosecution to rebut the Trojan Horse Defense); Note, *Child Pornography, the Internet, and the Challenge of Updating Statutory Terms*, 122 HARV. L. REV. 2206, 2224 (2009) (discussing repeat behavior model, that courts can utilize when presented with the Trojan Horse Defense); *see also Miller*, 527 F.3d at 67 (discussing a four-factor test to determine whether defendant knowingly received child pornography).

contemplates the consistency, if any, of the defendant's actions.[116] If a defendant can pinpoint when the virus began infecting the computer, computer forensic experts can compare the infection date with the date when the computer acquired the illegal images.[117]

Another method of handling Trojan Horse Defense invocations is to determine the defendant's level of "computer expertise."[118] Defendants who are shown to be proficient with computers are unlikely to fall victim to computer viruses and Trojan Horses.[119] Finally, courts can determine if the defendant has computer software programmed for the purpose of removing images and clearing the defendant's browsing history.[120] If these

---

[116] *See* Note, *supra* note 117, at 2224 ("Courts should look not to whether multiple images have appeared on a user's computer during a concrete period of time when the computer was infected, but to whether images have been obtained on several separate occasions over time. A virus can, for example, persistently download images, but it seems unlikely that an individual would obtain viruses that collect child pornography on multiple separate occasions. By isolating the time frame in which the user claims his computer was infected, courts can determine if there are other periods in which images were transferred to the computer.").

[117] *See id.*

[118] Brenner et al., *supra* note 84, at 22.

[119] *See id.* Brenner explains that:

> [I]t seems likely that those who invoke the Trojan horse defense will claim they know little, if anything, about computer technology and were therefore vulnerable to being exploited by an unknown hacker who used their computer for unlawful purposes without their knowledge. If such a claim is part of defendant's invocation of the defense, the prosecution may be able to rebut the defense by showing that the defendant is, in fact, knowledgeable about computers and what is required to protect them. Such evidence can be used to cast doubt on a defendant's claim that he must have been infected by Trojan horses or other types of malware when he opened suspicious emails or suspicious email attachments.

Id. (citing *Program Put Child Porn Pics on My PC*, GET READING (U.K.), Apr. 16, 2003, http://www.getreading.co.uk/news/s/6541_program_put_child_porn_pics_on_my_pc).

[120] *See* United States v. Bass, 411 F.3d 1198, 1202 (10th Cir. 2005).

programs are located on the defendant's computer, it is likely that they were downloaded or installed to prevent authorities from tracing the defendant's illegal activity.[121] Courts must thoroughly understand the Trojan Horse Defense to prevent confusion, which frequently results from the highly technical evidentiary aspects associated with the defense.[122] Furthermore, when faced with the Trojan Horse Defense, courts must also consider how the acquittal of a child pornography defendant leads to severe social impacts.

III. THE SOCIAL IMPACT ASSOCIATED WITH CHILD PORNOGRAPHY AND HOW CONSISTENT PROSECUTION RECOGNIZES CONGRESS'S INTENTIONS IN ENACTING THE CPPA

The acts of producing, viewing, and disseminating child pornography are considered incredibly evil and punishable in the eyes of society.[123] It is not surprising, then, that few defenses are successful during criminal proceedings of child pornography defendants.[124] Society and

[121] *See id.* ("However, the jury here reasonably could have inferred that Bass knew child pornography was automatically saved to his mother's computer based on evidence that Bass attempted to remove the images. There is ample evidence that Bass used two software programs, "History Kill" and "Window Washer," in an attempt to remove child pornography from the computer. Bass admitted he had used both "History-Kill" and "Window Washer" to delete child pornography because "he didn't want his mother to see those images . . . .").

[122] *See* United States v. Miller, 527 F.3d 54, 63 n.8, 65–67 (discussing conflicting expert testimony and the difficulty of determining whether a virus or a user accessed the images of child pornography).

[123] Ashcroft v. Free Speech Coal., 535 U.S. 234, 244–45 (2002) ("The sexual abuse of a child is a most serious crime and an act repugnant to the moral instincts of a decent people. In its legislative findings, Congress recognized that there are subcultures of persons who harbor illicit desires for children and commit criminal acts to gratify the impulses.").

[124] *See* United States v. Shiver, 305 F. App'x 640, 643 (11th Cir. 2008) (rejecting defendant's claim that a virus downloaded images of child pornography onto his computer); United States v. O'Keefe, 461 F.3d 1338, 1341, 1350 (11th Cir. 2006) (finding defendant guilty despite his Trojan Horse Defense); *Bass*, 411 F.3d at 1200 (convicting defendant despite his argument that a computer virus saved child pornography images on his computer); United States v. Vaughn, Cr. No. F. 05-00482

Congress take strong positions in the fight against child pornography.[125] The multitude of laws on this topic illustrates this claim; however, courts are often inconsistent in executing these laws because of the possession element and the new defenses.[126]

Upon realization of the importance of halting the expansion of child pornography, Congress enacted the first anti-child pornography legislation in 1977.[127] This initial ban on child pornography signified the beginning of a battle that continued to rage on for three decades.[128] As technology expanded, and accessibility to child pornography became easier, Congress continued to intensify and to extend the bans on child pornography through amendments.[129] Since its original enactment in 1996, the CPPA has undergone significant amendments.[130] These amendments reflect society's increasing reliance on the Internet.[131] However, the

OWW, 2008 WL 4104241, at *22 (E.D. Cal. Sept. 3, 2008) (rejecting post-trial argument of the Trojan Horse Defense).

[125] *See, e.g.*, *Ashcroft*, 535 U.S. at 244–45; *see also* New York v. Ferber, 458 U.S. 747, 764 (1982) (determining that child pornography is illegal and unprotected by the First Amendment to the United States Constitution).

[126] *See* cases cited *supra* note 32; Brenner et al., *supra* note 84, at 12–14 (describing how courts must be aware of potential problems associated with defendants' ability to invoke the Trojan Horse Defense).

[127] *See* Note, *supra* note 115, at 2208 (citing Protection of Children Against Sexual Exploitation Act of 1977, Pub. L. No. 95-225, 92 Stat. 7 (1978)).

[128] *Id.* at 2208–09; *see also* 18 U.S.C. § 2252A(a) (Supp. II 1996) (criminalizing transportation, possession, receiving, and producing of child pornography).

[129] *See* Note, *supra* note 115, at 2208; *see also* 18 U.S.C. § 2252A(a)(5)(B) (Supp. II 2008) (providing amended statutory provisions relating to the expansion of laws against child pornography).

[130] *See* Note, *supra* note 115, at 2208–10 (explaining how Congress amended the CPPA, but courts may still encounter questions regarding its application).

[131] *See id.* at 2206.

amendments have not yet been fully tested.[132] The inclusion of "intent to view" was an important congressional step toward extending the prohibition against child pornography, but the amendment's significance will depend on what definition future courts provide the phrase.[133]

During the development of the CPPA, Congress enumerated its reasons for protecting children against sexual abuse through child pornography.[134] Congress sought to criminalize child pornography because it invades children's privacy and interests by haunting the depicted children, and it strengthens pedophiles' deviant sexual desires.[135]

---

[132] *See supra* notes 13, 32 (discussing the amendments to the CPPA and how courts have inconsistently interpreted the possession element).

[133] *See* Note, *supra* note 115, at 2206–07 (instructing that when courts are faced with questions regarding the CPPA, they must consider the congressional intent to enhance prosecution of child pornography offenders under the 2009 amendments).

[134] H.R. 4123, 104th Cong. § 2 (1996).

[135] *Id.* Reasons outlined by Congress include:

> (7) The creation or distribution of child pornography which includes an image of a recognizable minor invades the child's privacy and reputational interest, since images that are created showing a child's face or other identifiable feature on a body engaging in sexually explicit conduct can haunt the minor for years to come;
>
> (8) [because of] the effect of visual depictions of child sexual activity on a child molester or pedophile using that material to stimulate or whet his own sexual appetites, or on a child where the material is being used as a means of seducing or breaking down the child's inhibitions to sexual abuse or exploitation; . . .
>
> (10)(A) [because] the existence of and traffic in child pornographic images creates the potential for many types of harm in the community and presents a clear and present danger to all children; . . .
>
> (11)(A) [because] the sexualization and eroticization of minors through any form of child pornographic images has a deleterious effect on all children by encouraging a societal perception of children as sexual objects and leading to further sexual abuse and exploitation of them; and

Through the enactment of the CPPA, Congress took a vital step towards ending child pornography in the United States.[136] Further, the passage of the Act signaled Congress's and the government's compelling interest in eliminating such a heinous practice.[137]

When confronted with these delicate situations, courts must consider the legislative concerns articulated by Congress when enacting the CPPA. While Congress and society have vehemently opposed child pornography, courts have had considerable difficulty consistently prosecuting child pornography defendants.[138] In order to strengthen the fight against child pornography, courts must consider the congressional intentions and legislative history associated with the CPPA.

CONCLUSION

Although courts struggle for consistency in prosecuting child pornography defendants, Congress strives to clarify its intent through continuous amendments of the CPPA.[139] In the near future, courts will have the opportunity to define "intent to view" and will likely be confronted with similar possession problems that have plagued courts for decades.[140] Because of the severe impact of child pornography on society,

---

> (B) this sexualization of minors creates an unwholesome environment which affects the psychological, mental and emotional development of children and undermines the efforts of parents and families to encourage the sound, mental, moral, and emotional development of children[.]

Id.

[136] Note, *supra* note 115, at 2208.

[137] *See generally* H.R. 4123 § 2 (illustrating the government's interest in ending child pornography in the United States).

[138] *See* cases cited *supra* note 32.

[139] *See* 18 U.S.C. § 2252A(a)(5)(B) (Supp. II 2008) (amending statutory provisions to expand the law against child pornography).

[140] *Compare* United States v. Stulock, 308 F.3d 922, 923–25 (8th Cir. 2002) (affirming

it is imperative that courts wade through the technical defenses overcome any confusion about the possession element of the CPPA.

To provide children with copious protection from sexual abuse, courts should convict defendants for mere viewing of child pornography or when law enforcement agents find evidence of the illegal material in the defendant's Internet Cache.[141] Courts must consider the reasons why Congress enacted the CPPA and those acts that Congress previously passed to prevent sexual abuse against children.[142] Courts that are prepared to confront the problems associated with the possession element of the CPPA and the Trojan Horse Defense will be better able to apply the CPPA properly. Accurate application of the CPPA will lead to consistent execution of Congress's intent, and children will be better protected against sexual abuse through child pornography.

that defendant was innocent of possessing child pornography because he did not download material), *with* United States v. Tucker, 305 F.3d 1193, 1204–05 (10th Cir. 2002) (holding that defendant satisfied the possession element of the CPPA by merely viewing child pornography and thus storing it in the Internet Cache).

[141] *See* United States v. Grober, 595 F. Supp. 2d 382, 408 (D.N.J. 2008) (referring to child pornography as a "grave impact on society"); United States v. Farris, No. 2:08cr145, 2008 WL 1944131, at *8 (W.D. Pa. May 1, 2008) (discussing significant physical and psychological harm associated with child pornography).

[142] *See* Ashcroft v. Free Speech Coal., 535 U.S. 234, 241 (2002); New York v. Ferber, 458 U.S. 747, 749 (1982).