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

Francis S Monterosso, Villanova University

Available at: https://works.bepress.com/francis_monterosso/1/
PROTECT THE CHILDREN: CHALLENGES THAT RESULT IN, AND CONSEQUENCES RESULTING FROM, INCONSISTENT PROSECUTION OF CHILD PORNOGRAPHY CASES IN A TECHNOLOGICAL WORLD

Note

Francis Stephen Monterosso
fmonterosso@law.villanova.edu
(484) 678-7898
TABLE OF CONTENTS

I. Introduction ........................................ 4
   A. The Problems Associated with Prosecuting Child Pornography Defendants .......... 4
   B. The Enactment of the CPPA of 1996 and its 2008 Amendments ..................... 7
   C. Overview of the Note ................................ 8
II. Background ........................................... 9
   A. The Problematic Development of the Child Pornography Prevention Act ............ 9
III. Analysis ............................................. 12
   A. Problems Associated with Proving the Possession Element of the CPPA ........... 12
      1. Downloading as a Requirement to Convict in United States v. Stulock .......... 13
      2. The Development of Cache as a Fulfillment of Possession in United States v. Tucker and United States v. Romm ............ 16
      3. Prior to the 2008 Amendment, Mere Viewing Did Not Satisfy the Possession Element of the Child Pornography Prevention Act; However, Courts Must
Look to Past Disputes to Determine the Future Course of Action ................... 21

B. The Developing Trojan Horse or Computer Virus Defense Through United States v. Miller ...... 22

1. The Treatment of the Trojan Horse Defense in the United Kingdom .................. 23

2. Hesitance in the Application of the Trojan Horse Defense in the United States through United States v. Miller ................. 24

3. Proposed Factors Courts Should Consider When the Trojan Horse Defense is Raised ......... 27

IV. The Social Impact Associated with Child Pornography and How Consistent Prosecution Recognizes Congress’ Intentions in Enacting the CPPA .................................. 29

V. Conclusion ............................................. 31

VI. Endnotes ................................. 33
I. **Introduction**

A. **The Problems Associated with Prosecuting Child Pornography Defendants**

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. 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.³

The social impact associated with inconsistently prosecuting child pornography cases is great, and courts have been distracted by issues involving the "possession" requirement under the CPPA as well as with the increasingly raised, Trojan Horse or Computer Virus defense.² There may be some legitimacy to these arguments, as illustrated in the successful use of this defense in England.³ However, it is imperative that courts do not neglect to consider the intent behind Congress’ enactment of the CPPA.⁴
Problems concerning the element of possession result from the discrepancies between courts concerning whether or not a child pornography defendant must actively download the pornographic material.\textsuperscript{5} While some courts demand the government prove that the defendant downloaded the material, other courts consider the discovery of child pornography in the Internet Cache as satisfactory to prove the possession element.\textsuperscript{6} Further, many courts refuse to convict defendants who merely viewed the child pornography.\textsuperscript{7} With the additional 2008 amendments, future courts should find that downloading child pornography, discovering it in the Internet Cache, and/or mere viewing of such material, all constitute “intent to view” and satisfy the possession requirement of the CPPA.\textsuperscript{8} 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.\textsuperscript{9}

Through the ratification of the Child Pornography Prevention Act of 1996 (CPPA), Congress sought to protect children from becoming victims of sexual abuse through the production, dissemination, and possession
of child pornography. Recently, courts have inconsistently decided similar child pornography cases, due to issues associated with proving the possession element of the CPPA and difficulties that arise when defendants raise the relatively new Trojan Horse Defense. As the internet continues to expand, so too does the ability of sexual predators to easily produce and propagate child pornography globally. 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 child pornography from the Internet have created a “nearly perfect medium for offenders seeking children for sex.”

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. When dealing with highly sensitive child pornography cases, courts must consider Congress’s intent when it enacted the CPPA. Therefore, courts should diligently attempt to prosecute these internet child pornography cases consistently to prevent the sexual
abuse --in the forms of physical and psychological harm -- of children, which results from child pornography.\textsuperscript{16}

B. The Enactment of the CPPA of 1996 and its 2008 Amendments

Although Congress enacted the CPPA in 1996, the Act underwent significant amendments in October of 2008.\textsuperscript{17} These amendments are notable because of their addition of the language, “intent to view.”\textsuperscript{18} Prior to these amendments, mere viewing of child pornography was not criminalized in America.\textsuperscript{19} Regardless of the 2008 amendments to the CPPA, courts will seemingly still face similar problems concerning the possession requirement and the Trojan Horse Defense.\textsuperscript{20}

Further, courts must still determine what constitutes “intent to view.”\textsuperscript{21} Although Congress has clearly criminalized mere viewing of child pornography, Congress also attempted to expand the CPPA through the 2008 amendments.\textsuperscript{22} When a defendant is found with pornography in the defendant’s 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 defendant should be convicted under the CPPA. 23 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. 24

C. Overview of the Note

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. 25 First, Part II sets forth the evolution of the CPPA and its goals and shortcomings. 26 Next, Part III 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. 27

Moreover, Part IV 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. 28
This section clarifies problems that courts will continue to face regardless of the recent amendments to the CPPA and challenges that courts should understand. Further, Part V 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 V also explains 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 America. Finally, Part VI 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.

II. Background

A. The Problematic Development of the Child Pornography Prevention Act

Although there have been numerous cases that argue that the CPPA is unconstitutional for
overbreadth reasons, the Supreme Court and lower courts have consistently upheld its constitutionality and found that the production and dissemination of child pornography is unprotected by the First Amendment.\textsuperscript{33} The only substantial limitation of the CPPA came from the Court’s decision in \textit{Ashcroft v. Free Coalition}.\textsuperscript{34} The \textit{Ashcroft} Court determined that the aspect of the CPPA which criminalized “virtual child pornography” was substantially overbroad.\textsuperscript{35} Regardless of the \textit{Ashcroft} decision, the CPPA has been consistently utilized in a multitude of cases and has undergone amendments.\textsuperscript{36}

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 also has expressed its opinion on the importance of protecting children from sexual abuse.\textsuperscript{37} Both branches of government have taken strong positions in an effort to end the dissemination of child pornography.\textsuperscript{38} In \textit{New York v. Ferber} and \textit{Osborne v. Ohio}, the Supreme Court
outlined five specific reasons why it is imperative for child pornography to be deemed illegal and unprotected by the First Amendment to United States Constitution.  

First, states have an interest in protecting the “physical and psychological well being of a minor.” Second, child pornography is a “permanent record” of the harmful acts and the government aims to prevent further distribution of such illegal material. Third, “the advertising and selling” of child pornography works to continue to promote the economic incentive to the child pornography business. Fourth, there is little to no value associated with child pornography. Fifth, there is a necessity in protecting children. Therefore, it is imperative that the legislative intent associated with the CPPA must not be neglected when courts encounter difficulties related to establishing the possession element of the CPPA and with theoretical defenses.
III. Analysis

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

Possession is the most frequently argued element of the CPPA. Because Congress and states refuse to define “possession” in the CPPA—and in related state child pornography laws—individual courts have been left with the task of defining “possession,” which has led to inconsistent conviction of defendants. Courts have inconsistently determined 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. Some courts convict defendants when they merely view child pornography online and it is automatically saved in the Temporary Internet File or the Internet Cache, while other courts have determined that these situations do not lead to a conviction.

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.
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.\textsuperscript{51} 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 files were physically downloaded by the user.\textsuperscript{52}

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, courts still have to 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.\textsuperscript{53} 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.\textsuperscript{54} 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.\textsuperscript{55}

In \textit{United States v. Stulock},\textsuperscript{56} the defendant was convicted of receiving child pornography, but he was also acquitted of a charge for possessing child pornography.\textsuperscript{57} This outcome illustrates courts’ inconsistencies in deciding child pornography cases.\textsuperscript{58} If a defendant receives child pornography, they must also possess it.\textsuperscript{59}

In \textit{Stulock}, “law enforcement officers raided” a business that was known to dispense child pornography through the internet.\textsuperscript{60} 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.\textsuperscript{61} 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.\textsuperscript{62} Stulock ultimately purchased more child pornography from the sting operation.\textsuperscript{63} Through this purchase, law enforcement
obtained a search warrant for Stulock’s home and seized his computer.\textsuperscript{64}

Upon searching Stulock’s computer, agents uncovered that Stulock searched for and visited numerous child pornography websites and that he also deleted child pornography files off of his computer.\textsuperscript{65} These files were recovered in the hard drive’s Temporary Internet File through computer forensics.\textsuperscript{66} When a computer has images, including child pornography, in the Temporary Internet File, 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.”\textsuperscript{67}

The problem that arose in \textbf{Stulock} was that the court was dissatisfied with the evidence presented at trial regarding the possession of child pornography charge.\textsuperscript{68} The \textbf{Stulock} Court required evidence that would reveal that the defendant had physically downloaded the illegal pornographic material.\textsuperscript{69} The defendant argued that he did not knowingly possess the illegal material and that “aggressive internet porn sites” and pop-ups placed child pornography onto his computer.\textsuperscript{70} The court ultimately concluded that,
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.\textsuperscript{71}

Although the \textit{Stulock} Court ultimately convicted the defendant for receiving child pornography, it neglected to consider Congress’s intent in enacting the CPPA when the district court acquitted Stulock of the possession of child pornography charge.\textsuperscript{72} Under the 2008 amendments, with “intent to view” as an additional avenue of convicting a defendant, the \textit{Stulock} Court would arguably still struggle with convicting the defendant.\textsuperscript{73} However, courts facing similar situations should not require evidence that defendants physically downloaded the child pornography in order to convict.\textsuperscript{74}

2. The Development of Cache as a Fulfillment of Possession in \textit{United States v. Tucker} and \textit{United States v. Romm}

While some American courts have begun convicting child pornography defendants when law enforcement
agents seize their computers and child pornography is discovered in the Temporary Internet File or Internet Cache of the computer’s hard drive, other courts require the defendant to download the illegal material in order to convict. Two fundamental child pornography cases established the precedent that defendants can be found guilty of possessing illegal pornography if they merely have viewed the material and are aware that their computers save the images in folders known as Temporary Internet Files or Internet Cache. With the 2008 amendments to the CPPA, regardless of a defendant’s knowledge that hard drives automatically save images --including child pornography --to their cache files, a defendant should be convicted under the “intent to view” theory.

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 met a minor girl and was hoping to meet up with her. Consequently, the friend informed the proper authorities and the defendant was arrested. Upon inspection of the defendant’s computer, a computer forensics officer discovered numerous files that the
defendant recently deleted from his machine, located in the “computer recycle bin” and in “unallocated hard drive space.” Agents also noticed that the defendant frequented sexual newsgroups with names alluding to child pornography.

The Tucker Court determined that it would only convict the defendant if the prosecution proved that the defendant was aware that the child pornography would automatically be saved into the Internet Cache. Without proving that the defendant not only viewed the images, but also knew they would be saved, the Court stated that it would be convicting the defendant for mere viewing, which was not permissible under the CPPA. 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.” Therefore, the court decided that the defendant knowingly possessed the child pornography and was convicted under the CPPA.

Further, in United States v. Romm, the Ninth Circuit agreed with the Tucker Court’s holding that child pornography defendants may be convicted when the defendant does not download the material, but the
material is knowingly stored in the Internet Cache.\textsuperscript{88} In \textit{Romm}, the defendant searched for and viewed numerous images of child pornography, “enlarged them,” and, consequently, his computer automatically saved the material to the computer’s hard drive.\textsuperscript{89} The defendant was ultimately charged when law enforcement officers discovered forty illegal images that the defendant had deleted from the Internet Cache.\textsuperscript{90}

At trial, as in \textit{Tucker}, the defendant contended that he did not knowingly possess the child pornography located on his computer because it was automatically transferred to his Internet Cache.\textsuperscript{91} The \textit{Romm} Court concluded that because the defendant sought out and searched for the child pornography, viewed it, enlarged images, could print out the illegal material, copy the images, 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.\textsuperscript{92} The \textit{Romm} Court inferred that the defendant knew that the child pornography images he viewed would automatically be saved in his computer’s Internet Cache folder; therefore, Romm was convicted of knowingly possessing child pornography.
under the CPPA, although he never purposely downloaded illegal material.\textsuperscript{93}

Currently, American courts have not encountered similar problems that plagued previous courts such as in Tucker, Romm, and Stulock.\textsuperscript{94} Until future courts adequately define the phrase “intent to view,” similar problems associated with possession will continue to arise.\textsuperscript{95} “Intent to view” should be satisfied by any acts that would likely lead a reasonable jury to conclude that the defendant viewed child pornography.\textsuperscript{96} This reasoning is in regards to situations where illegal material is found in a defendant’s Internet Cache regardless of whether or not the defendant knew that the computer stores images in Internet Cache.\textsuperscript{97} 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.\textsuperscript{98}
3. Prior to the 2008 Amendment, Mere Viewing Did Not Satisfy the Possession Element of the Child Pornography Prevention Act; However, Courts Must Look to Past Disputes to Determine the Future Course of Action

A defendant charged under the original 1996 CPPA, and similar state and military laws, was not convicted if a court determined that the defendant merely viewed child pornography without downloading the material. It is clear that Congress wanted to broaden the scope of the Act by adding “intent to view” to the 2008 amendments as a means of convicting defendants of possessing child pornography. Prior to the 2008 amendments, many federal and state courts had substantial difficulties in distinguishing mere viewing of child pornography from convictable possession of the material.

Furthermore, there was a strong argument that when a person “merely viewed” child pornography, they actually did a great deal more than simply looking at illegal material. 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.\textsuperscript{103} That entire process would have to occur prior to the defendant having the capability of actually viewing the material.\textsuperscript{104} Applying the amended version of the CPPA to cases such as \textit{Stulock}, would likely lead the courts to find the defendants in both cases guilty of possessing child pornography, as both defendants sought out illegal material on multiple occasions and viewed it on computers.\textsuperscript{105} Therefore, when courts are unsure whether or not to convict, they must consider Congress’s intent in enacting both the original CPPA and its 2008 amendments, that is, to enhance the prosecution of child pornography defendants.\textsuperscript{106}

B. The Developing Trojan Horse or Computer Virus Defense Through \textit{United States v. Miller}

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 and frequently begun raising the Trojan Horse Defense.\textsuperscript{107} The Trojan Horse Defense is invoked by the defense in an effort to establish a reasonable doubt in the fact finders’ minds by claiming that
“Some-Other-Dude-Did-It.” 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. 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.

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

The first cases to successfully raise the Trojan Horse Defense were tried in the United Kingdom in 2003. 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. The defense has likely been successful because jurors fear being similarly situated to the defendant, as Trojan horse viruses are both easily disguised and common.
In most child pornography cases where the Trojan Horse Defense is raised, computer forensic experts are the defense’s only evidence. The Trojan Horse Defense has caused courts and countries, domestically and internationally, to question how child pornography will be argued in the near future. It is imperative that courts are aware of and understand the Trojan Horse Defense, as it will immensely impact how child pornography will be prosecuted and, therefore, will have a direct effect on the social impact of child pornography.

2. Hesitance in the Application of the Trojan Horse Defense in the United States through United States v. Miller

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. Only rarely has the Trojan Horse Defense been successful in United States courts. Regardless of whether or not United States courts have acquitted child pornography defendants based on the Trojan Horse Defense, it is imperative
for courts to understand the defense as it has been consistently raised recently.¹¹⁹

In United States v. Miller,¹²⁰ the court ultimately found that the convictions against the defendant violated the double jeopardy clause; however, the court’s analysis of the Trojan Horse Defense did not lead to the reversal of Miller’s possession of child pornography conviction.¹²¹ The FBI discovered a zip disk in Miller’s home that was holding between 1200 and 1400 images --twenty of which constituted child pornography.¹²² The day after Miller’s home was searched and the pornography was discovered, the defendant contacted the interviewing FBI agent, Agent Kyle.¹²³ Miller informed Agent Kyle that the child pornography was likely a result of a virus that infected Miller’s computer a year prior to the search.¹²⁴

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.¹²⁵ One Agent testified that he was unable to sufficiently prove whether Miller or a virus accessed the images.¹²⁶

²⁵
court utilized four factors, with the totality of circumstances, to determine that the defendant downloaded and accessed the child pornography. The first factor was "whether images were found on the defendant’s computer." The second factor was the number of images of child pornography that were found. The third factor was whether the content of the images "was evident from their file names." The fourth factor was the defendant’s knowledge of and ability to access the storage area for the images.

At trial, Miller was convicted of receiving and possessing child pornography. The computer forensic experts in Miller “both acknowledged the possibility that child pornography could be unknowingly downloaded onto a hard drive as the result of a virus, or ‘spyware.’” However, the experts disagreed as to whether it was likely that this possibility occurred in Miller’s case. Agent Price “testified that he was unaware of there ever being . . . ‘any reports of a child porn dropping virus.’”

Further, the FBI Agent in Miller strongly disagreed with the defendant’s computer forensic expert’s testimony, that claimed a virus could download only child pornography, because the Agent
claimed 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.’”

Agent Price could only point to the defendant as the cause of the presence of the child pornography. 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, Miller was not convicted for possession of child pornography.

3. Proposed Factors Courts Should Consider When the Trojan Horse Defense is Raised

A number of academics and courts have suggested possible ways courts could address situations where the Trojan Horse Defense is raised in order to obtain justice. When considering the Trojan Horse Defense, courts should consider the “repeat behavior model,” which contemplates the consistency, if any, of the defendant’s actions. 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 illegal images were acquired by the computer.\textsuperscript{140} 

Another method of handling Trojan Horse Defense invocations is to determine the defendant’s level of “computer expertise.”\textsuperscript{141} Defendants who are shown to be proficient with computers are unlikely to fall victim to computer viruses and Trojan horses.\textsuperscript{142} Finally, courts can determine if the defendant has computer software programmed for the purpose of removing images and clearing the defendant’s browsing history.\textsuperscript{143} If these programs are located on the defendant’s computer, it is likely they were downloaded or installed to prevent authorities from tracing the defendant’s illegal activity.\textsuperscript{144} Courts must thoroughly understand the Trojan Horse Defense to prevent confusion, which frequently results from the highly technical evidentiary aspects associated with the defense.\textsuperscript{145} 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.\textsuperscript{146}
IV. The Social Impact Associated with Child Pornography and How Consistent Prosecution Recognizes Congress’ Intentions in Enacting the CPPA

Producing, viewing, and disseminating child pornography are considered to be incredibly evil and punishable in the eyes of society. That is likely a reason why there are so few defenses that can be successfully raised during criminal proceedings of child pornography defendants. Society and Congress have taken strong positions in the fight against child pornography. This stance is illustrated through the numerous acts and amendments denouncing child pornography; however, these laws have been inconsistently executed in the court system due to difficulties in proving the possession element and new defenses.

Realizing the importance of preventing the expansion of child pornography, Congress enacted the first anti-child pornography legislation in 1977. This initial ban on child pornography signified the beginning of a battle that has continued to rage on for three decades. As technology expanded, and
accessibility to child pornography continued to become easier, Congress continued to intensify and extend the outlawing of child pornography through amendments. Since Congress originally enacted the CPPA in 1996, the Act has undergone significant amendments to reflect society’s increasing reliance on the internet; however, these amendments have not yet been fully tested. 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 how it is defined by future courts.

During the development of the CPPA, Congress enumerated many reasons for protecting children against sexual abuse through child pornography. 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. Through the enactment of the CPPA, Congress took a vital step in its efforts to end child pornography in America. The ratification of the Act signaled Congress’s and the government’s compelling interest in eliminating such a heinous practice.
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. In order to strengthen the fight against child pornography, courts must reflect on the Congressional intentions and legislative history associated with the CPPA.

V. Conclusion

Although courts have struggled with consistently prosecuting child pornography defendants, Congress continues to attempt to clarify its goals by amending the CPPA. 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. It is imperative that courts do not get confused by the possession element of the CPPA and by technical defenses such as the Trojan Horse Defense because of the severe impact child pornography has on society.
In order to fully protect our children from sexual abuse, courts should convict defendants when they merely view child pornography or even when law enforcement agents locate evidence of the illegal material in a defendant’s Internet Cache. Courts must consider the reasons for which Congress enacted the CPPA and those acts that Congress previously ratified to prevent sexual abuse against children. Courts that are prepared to confront the problems associated with the possession element of the CPPA and the Trojan Horse Defense will be capable of applying the CPPA properly. Accurate application of the CPPA will lead to consistent execution of Congress’s intent, and our children will be better protected against sexual abuse through child pornography.


For a further discussion of this legislative history, see infra note 10 and accompanying text.

See United States v. Shaffer, 472 F.3d 1219, 1221 (10th Cir. 2007) (finding defendant guilty under CPPA for downloading child pornography); see, e.g., 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 court’s “clear . . . intent” that when defendant physically downloads child pornography, that defendant may be prosecuted for possessing child pornography); United States v. Stulock, 308 F.3d 922, 924 (8th Cir. 2002) (requiring defendant to download child pornography to convict under CPPA; therefore, defendant was not guilty since he merely viewed 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).

For a further discussion of Internet Cache, see infra note 23 and accompanying text.

See United States v. Kuchinski, 469 F.3d 853, 863 (9th Cir. 2006) (reasoning that when defendants in child pornography cases do not know about cache files and merely view child pornography files, defendants lacks possession of child pornography and cannot be properly convicted under CPPA). The defendant was
determined to be involved in child pornography by the Federal Bureau of Investigation (FBI). See id. at 856 (providing background of case which led to defendant’s conviction). The FBI obtained a search warrant and, upon execution of the warrant, discovered “between 15,120 and 19,000” child pornography images on the defendant’s computer. Id. (discussing number of illegal images discovered). A majority of these illegal files were discovered in “Deleted Temporary Files” or “Active Temporary Internet Files.” Id. (explaining location of child pornography in defendant’s computer). Although the defendant originally agreed to plead guilty, he ultimately did not, and attempted to argue that “because all elements of possession of child pornography were incorporated into . . . elements of receipt of child pornography,” being convicted under both charges would violate double jeopardy. Id. (asserting court’s decision). The defendant was found guilty through a bench trial decision. See id. (explaining that defendant’s theories did not succeed and defendant was guilty under both charges). On appeal, the court determined that it was clear that the defendant received and possessed child pornography that he had downloaded; however, child pornography discovered in Internet Cache could not lead to further convictions. See id. at 861-62 (asserting decisions set forth prior courts). The Court upheld established precedent that when a defendant unknowingly saves child pornography to the defendant’s hard drive’s Internet Cache or Temporary Internet File, the defendant cannot be convicted of possessing child pornography under the CPPA. See id. (citing Romm, 455 F.3d at 998; United States v. Tucker, 305 F.3d 1193, 1205 (10th Cir. 2002)).

8 For a further discussion of the 2008 amendments to the CPPA, see infra note 17 and accompanying text.

9 For a further discussion of the legislative history behind the enactment of the CPPA, see infra note 10 and accompanying text.

Any person who knowingly possesses 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 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 [will be convicted under CPPA].


11 See, e.g., United States v. Plugh, 576 F.3d 135, 138-39 (2d Cir. 2009) (discussing how defendant attempted to invoke Trojan Horse Defense; but then later admitted falsifying those claims); United States v. Shiver, 305 F. App’x 640, 643 (11th Cir. 2008) (arguing that computer virus downloaded child pornography on defendant’s computer which resulted in his indictment); United States v. Miller, 527 F.3d 54, 63 (3d Cir. 2008) (discussing how defendant claimed that computer virus downloaded child pornography rather than defendant); United States v. O’Keefe, 461 F.3d 1338, 1350 (11th Cir. 2006) (concluding that defendant’s Trojan Horse Defense was false); United States v. Bass, 411 F.3d 1198, 1200 (10th Cir. 2005) (arguing that defendant’s possession of child pornography was caused by a computer virus); United States v. Vaughn, Cr. No. F. 05-00482 OWW, 2008 WL 4104241, at *22 (E.D. Cal. Sept. 03, 2008) (rejecting post-trial argument of Trojan Horse Defense).
See Emily Brant, “Cybersex Offenders”: Individual Offenders Require Individualized Conditions when Courts Restrict Their Computer Use and Internet Access, 58 Cath. U. L. Rev. 779, 782 (Spring, 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); see also Black’s Law Dictionary 1199 (8th ed. 2004) (defining “child pornography”). Child pornography is “material depicting a person under the age of [eighteen] engaged in sexual activity. See id. (providing definition of child pornography). Child pornography is not protected by the First Amendment --even if it falls short of the legal standard for obscenity --and those directly involved in its distribution can be criminally punished.” Id.

See Brant, supra note 11, at 779 (citing Art Bowker & Michael Gray, An Introduction to the Supervision of the Cybersex Offender, 68 Fed. Probation 3, 3 (Dec. 2004)). See also Andrew Bates & Caroline Metcalf, A Psychometric Comparison of Internet and Non-Internet Sex Offenders from a Community Treatment Sample, 13 J. of Sexual Aggression 11, 12 (2007) (explaining how some laws have prevented courts from imposing specific sentences on sex offenders regarding their ability to access internet).

For a further discussion on how child pornography impacts society and how consistently prosecuting defendants aids in recognizing Congress’s legitimate goals in enacting the CPPA, see infra notes 135-155 and accompanying text.

For a further discussion of this legislative history, see supra note 10 and accompanying text.

For a further discussion of this legislative history, see supra note 10 and accompanying text.


Any person who—knowingly possesses 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 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.


[K]nowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer . . . .

Id. (asserting current version of CPPA) (emphasis added).

18 § 2252A(a)(4)(B) (establishing CPPA with 2008 amendments).

19 See United States v. Stulock, 308 F.3d 922, 924 (8th Cir. 2002) (determining that merely viewing child pornography images and not intentionally downloading or saving the images does not satisfy elements of the CPPA). See also United States v. Navrestad, 66 M.J. 262, 268 (C.A.A.F. 2008) (deciding that viewing images of child pornography does not constitute possession where defendant does not save nor download images).

20 For a further discussion on how courts will seemingly continue to face issues associated with the possession element to the CPPA and the Trojan Horse Defense, see infra notes 82-90 and accompanying text.
§ 2252A(a)(4)(B) (providing CPPA with its 2008 amendments).

See id. (stating amended CPPA).

See United States v. Romm, 455 F.3d 990, 993 n.1 (9th Cir. 2006) (explaining that “[t]he ‘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 (Barron’s 8th Ed. 2003))). See, e.g., Stulock, 308 F.3d at 925 (explaining that “[t]he 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 internet cache). Internet Cache is

[A] location on a computer's hard drive that contains “a collection of data images typically that have been gleaned from your travels around the Internet.” [The witness] explained that upon visiting a Web page, a Web browser immediately caches or saves the images on that page in the cache file. If a user selects an image on a Web page in order to enlarge the image, the larger image is also cached. The Web browser automatically caches such images; no act is required of the user. The purpose of caching is to allow already-visited pages to forego the necessity of loading pictures and thus allow visits to these pages to be processed much faster.

Id. See also People v. Scolaro, 910 N.E.2d 126, 130 (Ill. App. Ct. 2009) (noting that Internet Cache is “a storage mechanism designed to speed up the loading of
Internet displays. When a user views a Web page, the Web browser stores a copy of the page on the computer's hard drive in a folder or directory. The folder is known as the ‘cache,’ and the individual files in the cache are known as ‘temporary Internet files.’ (citing 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, 1229-30 (2004)).

24 See United States v. Bass, 411 F.3d 1198, 1201 (10th Cir. 2005) (defining “possession” as “the holding or having something (material or immaterial) as one’s own, or in one’s control.”) (citing Oxford English Dictionary (2d ed. 1989)). See, e.g., Black’s Law Dictionary 37 (8th ed. 2004) (defining “act of possession” as “1. The exercise of physical control over a corporeal thing, movable or immovable, with the intent to own it. 2. Conduct indicating an intent to claim property as one's own . . . ”).

25 For a further discussion on the negative social impact created by the creation and dissemination of child pornography, see infra notes 134-149 and accompanying text.

26 For a further discussion of the intentions and problems associated with CPPA, see infra notes 32-36 and accompanying text.

27 For a further discussion of how specific cases illustrate the government’s attempt at protecting children through CPPA, see infra notes 37–45 and accompanying text.

28 For a further discussion of how the CPPA was utilized, defined, and confused through child pornography cases and Trojan Horse Defense, and the government’s intention to prosecute child pornography defendants consistently, see infra notes 46-124 and accompanying text.

29 For a further discussion of a clarification of the CPPA, and the government’s intention to prosecute child pornography, see infra notes 46-124 and accompanying text.
For a further discussion regarding the social impact associated with child pornography and therefore, inconsistent prosecutions, see infra notes 134-149 and accompanying text.

For a further discussion regarding the social impact associated with child pornography, see infra notes 134-149 and accompanying text.

For a further discussion of a conclusory affirmation that courts must prosecute child pornography cases consistently and that the new 2008 amendments reveal government’s strong desire to do so, see infra notes 150-154 and accompanying text.

For a further discussion of the determination that the CPPA is constitutional, see infra note 36 and accompanying text.

535 U.S. 234, 256-57 (2002) (finding that although “trade association of businesses” that produced and sold pornography may be convicted under CPPA provisions, provisions associated with “virtual child pornography” were held unconstitutional).

See Ashcroft, 535 U.S. at 234 (stating that “virtual child pornography” are materials which appear to involve minors partaking in sexual conduct; however, pornographic material was produced through utilizing computer technology or legal, consenting adults who merely look like minors). Prior to the Ashcroft decision, the CPPA criminalized receipt, possession, and distribution of child pornography, and also “virtual pornography” which did not utilize real minors. See id. at 234 (describing 1996 version of CPPA and what it criminalized). Respondents, Free Speech Coalition, filed this suit challenging the CPPA for being overbroad, and therefore, unconstitutional. See id. at 241 (citing 18 U.S.C. § 2256(8)(B), which is section of CPPA that criminalizes “virtual child pornography”). The Ashcroft Court determined that:

Our society, like other cultures, has empathy and enduring fascination with the lives and destinies of the young. Art and
literature express the vital interest we all have in the formative years we ourselves once knew, when wounds can be so grievous, disappointment so profound, and mistaken choices so tragic, but when moral acts and self-fulfillment are still in reach. Whether or not the films we mention 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 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.

Id. at 248. Therefore, the section of the CPPA that corresponded to criminalizing “virtual child pornography” was stricken as unconstitutional. See id. at 265, 267 (deciding that where CPPA is overbroad and criminalizes “virtual child pornography,” it should be “str[uck] down”). See also United States v. Richardson, 304 F.3d 1061, 1063 (11th Cir. 2002) (indicating that “virtual child pornography” is pornography involving virtually created children, produced through “computer-imaging technology”). See also United States v. Hersh, 297 F.3d 1233, 1254 n.31 (11th Cir. 2002) (noting that Ashcroft decision only applies to “virtual child pornography” rather than CPPA in its entirety). As the defendant was found to be in possession of child pornography involving actual minors, Ashcroft’s denunciation of CPPA section banning “virtual child pornography” was irrelevant. See id. (explaining that Defendant’s argument that his guilt in his possession of child pornography charge was correct). See, e.g., United States v. Wyatt, 64 F. App’x 350, 351 (4th Cir. 2003) (asserting that Ashcroft decision did not invalidate entire CPPA, but specific sections, including criminalization of “virtual child pornography”) (citing United States v. Kelly, 314 F.3d 908, 911 (7th Cir. 2003)) (rejecting defendant’s contention that Ashcroft determination made entire CPPA unconstitutional).
For a further discussion of the 2008 amendments to the CPPA, see supra note 9 and accompanying text.

For a further discussion of the Supreme Court’s intent to further Congress’s goals of protecting children from sexual abuse through child pornography, see infra notes 38-43 and accompanying text.

For the Supreme Court’s five reasons why child pornography should be criminalized, see infra notes 38-43 and accompanying text.

See New York v. Ferber, 458 U.S. 747, 764 (1982) (asserting basic principles behind Court’s reasoning to criminalize child pornography). See also U.S. Const. amend. I (announcing freedoms for all Americans). The Constitution states that “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.” Id. See also Osborne v. Ohio, 495 U.S. 103, 110 (1990) (citing Ferber, 458 U.S. at 765, to explain that statutes which criminalize possession of child pornography are not overbroad and do not violate First Amendment rights); see also Commonwealth v. Simone, No. 03-0986, 2003 WL 22994238, at *8 (Va. Cir. Oct. 10, 2003) (explaining that there are limited number of situations where speech is unprotected) (citing Chaplinsky v. New Hampshire, 315 U.S. 568, 571-72 (1942)). The Chaplinsky Court stated that:

There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or “fighting” words--those which by their very utterance inflict injury or tend to incite and immediate breach of the peace. It has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may
be derived from them is clearly outweighed by the social interest in order and morality.

Id. Further, federal and state governments have created child pornography laws, which although not considered to be part of the “obscene” category of prohibited speech, are so similar to obscenity, “from both a public policy, legislative, and judicial standpoint,” that it too is prohibited. See id. (explaining how Virginia developed child pornography laws).

40 See Simone, 2003 WL 22994238, at *8 (citing Ferber, 458 U.S. at 756-57) (determining that defendant bookstore owner was properly found guilty under New York’s version of CPPA, although defendant claimed that statute, like CPPA, was overbroad and therefore unconstitutional). Like the Ashcroft Court, the Simone court faced questions about the constitutionality of Virginia’s child pornography statute. See Simone, 2003 WL 22994238, at *2 (explaining defendant’s first point of contention regarding his conviction for possessing child pornography). The Simone court determined that Virginia’s Constitution, as does the U.S. Constitution, both protect individuals’ free speech rights equally. See id. (discussing how although Constitutions protect individuals’ freedom of speech, there are limitations to that freedom).

41 See Simone, 2003 WL 22994238, at *8 (citing Ferber, 458 U.S. at 756-57; Ashcroft, 535 U.S. at 250) (explaining in Ashcroft that Ferber court found “proximate link” between crime of child pornography and its continued accessibility in future).

42 See Simone, 2003 WL 22994238, at *8 (citing Ferber, 458 U.S. at 756-57; Ashcroft, 535 U.S. at 250) (discussing how criminalizing child pornography will aid in ending economic benefits associated with illegal materials’ sales).

43 See Simone, 2003 WL 22994238, at *8 (citing Ferber, 458 U.S. at 763) (stating that artistic value
regarding art and minors can be achieved by using young adults who look like minors).

44 See id. (citing Ferber, 458 U.S. at 764) (declaring that child pornography laws and acts deal with visual depictions of children engaged in sexual actions).

45 For a further discussion of the Trojan Horse Defense, see infra notes 92-124 and accompanying text.

46 See, e.g., United States v. Shaffer, 472 F.3d 1219, 1225-26 (10th Cir. 2007) (asserting that when defendant downloaded child pornography from peer-to-peer website, Kazaa, defendant knowingly possessed child pornography under CPPA); United States v. Romm, 455 F.3d 990, 1000-01 (9th Cir. 2006) (upholding United States v. Tucker, 305 F.3d 1193, 1205 (10th Cir. 2002) (concluding that defendant satisfied possession element of CPPA by viewing child pornography and having it stored in Internet Cache). Possession was established because the defendant was aware that when viewing websites and pornography, the computer hard drive automatically stored that information in Internet Cache. See id. (noting how possession was established at trial); United States v. Stulock, 308 F.3d 922, 924 (8th Cir. 2002) (stating that defendant did not possess child pornography because he did not download nor save illegal pornographic material); United States v. Tucker, 305 F.3d 1193, 1204-05 (10th Cir. 2002) (determining that although defendant never downloaded child pornography he was still guilty under CPPA). The defendant merely viewed child pornography and was aware that his web browser “saved the images against his will”; however, the court concluded that this still satisfied possession element and convicted the defendant. See id. (discussing court’s line of reasoning when trying defendant); United States v. Navrestad, 66 M.J. 262, 268 (C.A.A.F. 2008) (explaining that defendant could not be convicted for possessing child pornography because although public computer which was used to access internet and illegal pornographic material saved images in Temporary Internet File, defendant was unaware of this process and was not in control of child pornography); People v. Scolaro, 910 N.E.2d 126, 131-32 (Ill. App. Ct. 2009) (discussing similar state
statute, comparable to CPPA. The court determined that possession under child pornography laws was satisfied when the defendant controlled images -- unbeknownst to himself -- in computer’s Internet Cache).

47 See Romm, 455 F.3d at 999 (discussing that Court must interpret “possession” by its plain meaning and attempt to determine Congress’ intentions when using “possession” in CPPA); Scolaro, 910 N.E.2d at 133 (stating that, “Illinois’s child-pornography statute does not define ‘possess.’ However, as both parties note in their briefs, where a term is not defined by the legislature, the ‘undefined terms in a statute shall be given their ordinary and popularly understood meanings.’” (quoting People v. Ward, 830 N.E.2d 556, 559 (Ill. 2005)).


[W]ith knowledge of the nature or content thereof, possesses any film, videotape, photograph or other similar visual reproduction or depiction by computer of any child or severely or profoundly mentally retarded person whom the person knows or reasonably should know to be under the age of 18 or to be a severely or profoundly mentally retarded person, engaged in any activity described in subparagraphs (i) through (vii) of paragraph (1) of this subsection . . .

49 See, e.g., Romm, 455 F.3d at 1000-01 (determining that defendant was guilty of possessing pornography when government found the illegal pornographic material in defendant’s Internet Cache); Tucker, 305 F.3d at 1204-05 (declaring that although defendant merely viewed child pornography, defendant was aware that his web browser “saved the images against his will”). Therefore, the court concluded that this still satisfied possession element and convicted the defendant. See id. (same); Scolaro, 910 N.E.2d at 131-32 (determining that possession under child pornography statute was satisfied when defendant controlled images, in computer hard drive’s Internet Cache). See also Stulock, 308 F.3d 922, 924 (8th Cir. 2002) (stating that defendant did not possess child pornography because he did not download or save illegal pornographic material); Navrestad, 66 M.J. at 268 (finding defendant could not be convicted of possessing child pornography although such illegal pornographic material was found on public computer that defendant used to access internet, saved child pornography images to its Temporary Internet File).

50 For a further discussion on how courts will seemingly continue to face issues associated with the possession element to the CPPA and the Trojan Horse Defense, see infra notes 82-90 and accompanying text.

51 See H.R. 3726, 109th Cong., § 2(2) (2005) (stating reasons for criminalizing possession of child pornography) These reasons include:

(A) The vast majority of child pornography prosecutions today involve images contained on computer hard drives, computer disks, and related media. (B) Child pornography is not entitled to protection under the First Amendment and thus may be prohibited. (C) 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. (D) Every instance of viewing images of child pornography
represents a renewed violation of the privacy of the victims and a repetition of their abuse. (E) Child pornography constitutes prima facie contraband, and as such should not be distributed to, or copied by, child pornography defendants or their attorneys. (F) It is imperative to prohibit the reproduction of child pornography in criminal cases so as to avoid repeated violation and abuse of victims, so long as the Government makes reasonable accommodations for the inspection, viewing, and examination of such material for the purposes of mounting a criminal defense.


54 For a further discussion about inconsistent prosecutions in child pornography cases due to the possession element, see supra note 46 and accompanying text.

55 For a further discussion concerning situations where defendants were acquitted because they did not “control” the child pornography through downloading, see infra note 103.
United States v. Stulock, 308 F.3d 922 (8th Cir. 2002).

57 See id. at 923-24 (summarizing court’s holding that defendant was guilty of receiving child pornography, yet simultaneously, innocent of possessing child pornography).

58 See id. (illustrating inconsistency in court’s prosecution of child pornography defendant).

59 See id. (asserting question that arose in Stulock). For a further discussion of this question through an analogy, see infra note 99.

60 See Stulock, 308 F.3d at 924 (discussing background of how defendant was located and charged with receiving child pornography).

61 See id. (providing fundamental information that led to defendant’s conviction).

62 See id. (explaining how defendant was charged with possession of child pornography).

63 See id. (discussing how defendant was set-up by law enforcement agents).

64 See id. (asserting that defendant was located through his purchase of illegal material). For a further discussion of websites Stulock visited, see supra note 46.

65 See id. (explaining that agents were capable of retrieving child pornography files that defendant had previously deleted). The court explained that:

More than 3,000 deleted files were recovered from the temp directory, including numerous examples of child pornography. Stulock’s computer was configured to use the temp directory as the location where downloaded files that had been packaged in the ZIP file format would be stored. These ZIP files have capability of storing hundreds of
photos, without requiring user to save each image individually.

66 See id. (asserting that courts can infer that defendants have either downloaded files or viewed them, when they are recovered in Temporary Internet File).

67 Zip File--Definition, http://encarta.msn.com/dictionary_/zip%2520file.html (last visited Oct. 10, 2009). Zip file is defined as “a computer file with the extension .zip containing data that has been compressed for storage or transmission. Id. (defining “zip file”).

68 See Stulock, 308 F.3d at at 926 (asserting that because the images were covered in the Internet Cache or Temporary Internet File, court was unwilling to convict Stulock).

69 See id. (determining that defendant could not be convicted of possessing child pornography under 18 U.S.C. § 2252A(a)(4)(B), without defendant “purposely sav[ing] or downloa[d]ing the image).

70 See id. at 926 (asserting argument that defendant attempted to use to prevent being convicted of possessing child pornography).

71 See id. (stating court’s conclusion in finding defendant guilty of receiving child pornography).

72 See id. at 925 (deciding that defendant not guilty of possessing child pornography).

73 For a further discussion about downloading as a requirement to convict child pornography defendants, see supra notes 55-63 and accompanying text.

74 For a further discussion on how future courts should handle technologically involved child pornography cases, see infra notes 78-86 and accompanying text.
For a further discussion regarding the discrepancies between American courts and whether to convict defendants only when downloading occurs rather than when child pornography is discovered in cache files, see supra note 22 and accompanying text. See also United States v. Scolaro, 910 N.E.2d 126, 127 (Ill. App. Ct. 2009) (affirming defendant’s conviction of possessing child pornography in violation of Illinois’ child pornography statute). The defendant was named as a child pornography customer when Department of Homeland Security (DHS), located the customer information from various child pornography websites. See id. at 127 (providing explanation regarding defendant’s original arrest). After searching the defendant’s computer, law enforcement agents uncovered only legal pornography. See id. at 128 (providing background information on case prior to it being taken to trial). Scolaro admitted to officers that although he viewed child pornography images, he never saved them to his computer’s hard drive. Id. (noting discussion between defendant and officers). Further, the defendant also admitted to subscribing to number of child pornography websites which featured minors ranging from eight to sixteen years old. See id. (asserting that defendant subscribed to child pornography websites, such as, “Virgin X Boys, Sunrise Boys, Boys-Are-Us, and Charming Boys,” using his credit card). DHS agents utilized computer forensic software and ultimately discovered 689 additional child pornography images that the defendant had deleted. See id. at 129 (explaining process by which officers uncovered images that defendant viewed and later deleted; however, these images still remained in the “unallocated section of defendant’s hard drive”). The unallocated section of a hard drive is known as a computers’ free space, and is the location where a computer receives data and images from websites visited by users. Id. (explaining technical computer jargon). The defendant appealed his conviction, because he claimed that because he did not download or save child pornography images, he did not knowingly possess illegal material. See id. at 129 (stating reasons defendant appealed his conviction of possessing child pornography). The defendant argued that to be convicted of possessing child pornography, he must be found to have printed, saved, downloaded,
or in some other way have exercised control over those illegal images. See id. at 130 (declaring ultimate issue on appeal and discussing applicable state statute). The Scolaro Court discusses the decision of Tucker to regarding a similar situation involving the federal child pornography statute. See id. (noting that in Tucker, court faced a similar problem, where although defendant did not save or download child pornography, he admitted that he was aware that computer automatically sent and saved images in Internet Cache). The Scolaro Court used the Tucker decision and determined that whether or not the defendant knew that his computer automatically saved website information and images to the Internet Cache, he was still guilty of possessing child pornography because he exercised control over the images. See id. at 131 (determining that when images are located in Internet Cache, they can be viewed, modified, printed, e-mailed, copied or posted to newsgroup; therefore, because defendant sought out images, he exercised control over them). Having the mere ability to view, modify, print, e-mail, copy or post these images, convinced the court that Scolaro possessed child pornography under applicable Illinois child pornography statute. See id. at 133 (expressing ultimate conclusion of Scolaro Court). For a further discussion about courts and cases that require the defendant to download child pornography in order to find the defendant guilty, see supra notes 55-65 and infra notes 67-69 and accompanying text.

76 See United States v. Romm, 455 F.3d 990, 998 (9th Cir. 2006) (discussing that where defendant viewed child pornography and was aware that those images were saved to defendant’s hard drive, defendant could be prosecuted for possession of that child pornography); see also United States v. Tucker, 305 F.3d 1193, 1198-99 (10th Cir. 2002) (explaining that when defendant purposely searches internet for child pornography, views it, and knows computers save such images, defendant is in control of illegal pornography and can be prosecuted for possession of child pornography). For a further discussion about Temporary Internet Files and the Internet Cache, see supra note 16 and accompanying text.
See id. (adding “intent to view” into CPPA, illustrated Congress’s intent to criminalize accessing and even mere viewing of child pornography and its desire to end dissemination of child pornography); see also H.R. 4120, 110th Cong. §203 (as enrolled by both House and Senate, January 3, 2008) (explaining Congress’s intention of enhancing, effectively, prosecution of child pornography cases through insertion of “intent to view”).

United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002).

See Tucker, 305 F.3d at 1195 (introducing that defendant appeals his conviction of possessing child pornography under CPPA and provides background facts that led to defendant’s arrest).

See id. at 1196 (establishing how Tucker’s friend learned of child pornography on his computer and informed law enforcement agents).

See id. at 1196-97 (asserting that although child pornography may not always be saved or downloaded onto computers, prosecution for possession of child pornography may still be applicable).

See id. at 1198 n.3 (defining “newsgroup” as “a location on the Internet which . . . ‘is analogous to a bulletin board where people post messages and they’re able to reply, and they’re also able to exchange date, exchange documents and images.’”)

See id. at 1198-99 (explaining process by which court ultimately concluded that defendant was guilty of knowingly possessing child pornography). Nearly 5,000 child pornography images were discovered on his computer in various locations. See id. (noting number of pornographic images in controversy). Due to Tucker consistently deleting child pornography located in the Internet Cache, the court concluded that he was in control of the pornographic images and therefore possessed them. See id. (explaining court’s reasoning for finding that defendant controlled illegal material).
See id. (determining that court had to consider that defendant intentionally sought out and viewed child pornography; therefore he not only viewed child pornography, but also “reached out for” and possessed illegal pornographic material).

See id. at 1204 (discussing how court came to conclusion that defendant was aware that child pornography images and information from websites he frequented would actually be automatically saved onto defendant’s hard drive).

See id. (finding defendant controlled child pornography). See also Ty E. Howard, supra note 14, at 1242 (explaining why 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).

United States v. Romm, 455 F.3d 990 (9th Circ. 2006).

See id. (concurring with Tucker court that defendant can be convicted by merely viewing illegal material and it being automatically stored in his Internet Cache, without proving defendant downloaded material); see also Tucker, 305 F.3d at 1205 (determining defendant did not have to manually download child pornography to be convicted under CPPA).

See Romm, 455 F.3d at 995 (discussing how computer forensic expert discovered that Defendant clicked on thumbnails of images in order to make the illegal material display larger on his screen). A “thumbnail”
refers to “a small image of a graphics file displayed in order to help you identify it.” See id. at 995 n.9 (citing Douglas Downing, et al., Dictionary of Computer and Internet Terms, 149 (Barron’s 8th ed. 2003)) (defining what thumbnail means in computer terms).

90 See Romm, 455 F.3d at 995 (asserting that defendant accessed his hard drive’s Internet Cache with intention of deleting illegal material he searched for and viewed).

91 See Tucker, 305 F.3d at 1198-99 (determining that defendant knowingly possessed child pornography, although he did not download material and it was automatically saved in computer’s Internet Cache). For a further discussion of why Tucker Court determined that Tucker knowingly possessed child pornography, see supra notes 76-80 and infra notes 82-84 and accompanying text. See also Romm, 455 F.3d at 1000 (concluding that, like in Tucker, where the defendant has “unfettered access to the [I]nternet [C]ache”, he searches for and views child pornography, and knows that images are saved to Internet Cache, knowing possession is satisfied).

92 See id. (explaining various ways that defendant could have utilized illegal materials and determining that defendant controlled child pornography). Although the defendant referred to his actions as “saving” and “downloading,” he actually did not download any child pornography images. See id. (explaining how defendant described his activities). His description of his activities as “saving” and “downloading” did not affect Romm Court’s decision. See id. at 1000-01 (noting Romm’s explanation of his actions did not change outcome of case).

93 See id. (inferring that because the defendant accessed and deleted child pornography he previously viewed, in Internet Cache, he knew that copies of illegal material would automatically be saved in Internet Cache). See id. at 1001 (deciding that defendant was able to control illegal material which he purposely sought out and viewed, and knew that the images would be copied into the Internet Cache).
For a further discussion of why the Tucker Court determined that Tucker knowingly possessed child pornography, see supra notes 76-83 and accompanying text. For a further discussion of Romm, see infra notes 87-95 and accompanying text. For a further discussion of Stulock, see supra 57-69 and accompanying text. For a further discussion of Kuchinski, see supra note 22. For a further discussion of Kuchinski, see supra note 22. For a further discussion of Kuchinski, see supra note 22.


[K]nowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer . . . .

Id. (stating current version of CPPA) (emphasis added).

See Black’s Law Dictionary 825 (8th ed. 2004) (defining “intent”). “While motive is the inducement to do some act, intent is the mental resolution or determination to do it.” See id. (same) (emphasis added).

For a further discussion of Tucker, see supra notes 76-84 and accompanying text; for a further discussion of Romm, see supra notes 87-90 and infra notes 92-95 and accompanying text. For a further discussion of the social impact of child pornography, see infra notes 134-149 and accompanying text.

For a further discussion of the social impact of child pornography, see infra notes 134-149 and accompanying text.
See United States v. Bass, 411 F.3d 1198, 1207 (10th Cir. 2005) (Kelly, J., dissenting) (disagreeing with majority opinion and discussing CPPA). The dissenting judge explains that, “[a]lthough reprehensible, viewing child pornography is not a crime.” See id. (citing United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002)) (explaining charges associated with defendant in child pornography trial). The court stated that, “[t]he district court explained that one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically stored to the browser’s cache, without having purposely saved or downloaded the image.” Id. For a further discussion of Stulock, see supra notes 57-69 and accompanying text. 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, “[i]n this context, viewing alone does not constitute ‘control’”).

See H.R. 4120, 110th Cong. §203 (as enrolled by both House and Senate, January 3, 2008) (explaining Congress’s intent of enhancing, effectively, prosecution of child pornography cases). Congress inserted the phrase, “or knowingly accesses with intent to view,” throughout the CPPA in order to aid in the prosecution of child pornography defendants. Id. (discussing Congress’s 2008 CPPA amendments). Further, 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. (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.

See id. at § 102 (listing Congress’s findings associated with why it must enhance prosecution of child pornography cases).


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.

See id. (same). See also, Ty E. Howard, supra note 14, 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 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. (continuing to analogize person viewing—without purchasing—child pornography—magazine in bookstore, to merely viewing child pornography on internet).

See Ty E. Howard, supra note 14, at 1266 (discussing process of viewing child pornography via analogy).

See id. (explaining that it takes effort to view child pornography, including searching for, accessing, and enlarging material).
See id. (discussing that child pornography viewers do not merely stumble across illegal material).

Compare United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002) (determining that defendants in child pornography cases cannot be found guilty 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 CPPA, military members cannot be found guilty of possessing child pornography for merely viewing illegal material), with H.R. 4120, 110th Cong., § 203 (including "intent to view" in CPPA to enhance prosecution of child pornography defendants).

See H.R. 4120, 110th Cong., § 203 (2008) (explaining Congress’s intention to produce more effective and enhanced convictions of child pornography defendants under CPPA).

See Susan W. Brenner, et al., The Trojan Horse Defense In Cybercrimes, 21 Santa Clara Computer & High Tech. L.J. 1, 11 (2004) (defining term, Trojan Horse Defense). The Trojan Horse Defense is “any defense based on the alleged effects of malware, whether a Trojan horse, virus, worm or other program.” See, e.g., 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 claims that a computer virus was cause of depositing of child pornography in defendant–computer’s operating system); United States v. Miller, 527 F.3d 54, 63 & n.8 (3d Cir. 2008) (providing conflicting testimony between two forensic experts at trial, which were used to aid in defendant’s conviction); United States v. Shiver, 305 F. App’x 640,643 (11th Cir. 2008) (disproving defendant’s theory that virus placed child pornography on defendant’s computer); United States v. O’Keefe, 461 F.3d 1338, 1341 (11th Cir. 2006) (determining that although computer forensics expert discovered multiple viruses on defendant’s computer, they were determined to be incapable of downloading child pornography and defendant was convicted under CPPA); United States v.
Bass, 411 F.3d 1198, 1200 (10th Cir. 2005) (finding that although defendant’s computer allegedly suffered from virus which caused it to automatically save illegal child pornography, defendant was still guilty of possessing material); United States v. Vaughn, Cr. No. F. 05-00482 OWW, 2008 WL 4104241, at *22 (E.D. 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).

See Susan W. Brenner, et al., supra note 103, 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.” See id. at 12 (discussing what prosecution must substantiate to defeat Trojan Horse Defense). See also Black’s Law Dictionary 1425 (8th ed. 2004) (defining “SODDI Defense”). The Some-Other-Dude-Did-It Defense is “a claim that somebody else committed a crime.” Id.

See Susan W. Brenner, et al., supra note 103, at 9-10 (explaining defendant’s reasoning in attempting to establish Trojan Horse Defense). One commentator explains that:

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.


110 See Susan W. Brenner, et al., supra note 103, at 12-14 (describing how courts must be aware of potential problems associated with defendants’ ability to invoke Trojan Horse Defense). Brenner explains:

In a criminal prosecution, at least in the United States, the 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.

Id. (explaining issues surrounding Trojan Horse Defense).

111 See Susan W. Brenner, et al., supra note 103, at 8 (discussing defendant, Karl Schofield, who was acquitted of possessing child pornography by raising Trojan Horse Defense); see id. (citing John Schwartz, supra note 17, at C1)) (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 (UK), April 18, 2003, § News, available at 2003 WLNR 13123469 (explaining first recorded successful invocation of Trojan Horse Defense).

112 See Susan W. Brenner, et al., supra note 103, at 8 (asserting early arguments raised by child pornography defendants who raised Trojan Horse Defense).

113 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 to attacking other computers.” See id. (quoting Ed Skoudis with Lenny Zeltser, Malware: Fighting Malicious Code 251 (Mary Franz ed., Prentice Hall Professional Technical Reference 2004) (2003)) (defining Trojan virus).

114 See Susan W. Brenner, et al., supra note 3, at 8 (discussing how computer forensics was utilized in prosecution of Karl Schofield). For a further discussion on more cases that utilized computer forensic testimony to discuss the Trojan Horse Defense, see supra note 92.

115 See Can a virus put porn on your PC?, Ir. Times (Ir), January 19, 2005, § Features, available at 2005 WLNR 718976 (discussing how Irish legislators are calling for changes in statutes concerning Trojan Horse Defense).

116 For a further discussion on the social impact of child pornography, see infra notes 134-149 and accompanying text.

117 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 that defendant’s invocation of Trojan
Horse Defense lacked adequacy); United States v. Miller, 527 F.3d 54, 63 & n.8 (3d Cir. 2008) (asserting that defendant’s use of Trojan Horse Defense could not stand); United States v. Shiver, 305 F. App’x 640, 643 (11th Cir. 2008) (determining that defendant’s utilization of Trojan Horse Defense did not succeed in acquitting him of possessing child pornography); United States v. O’Keefe, 461 F.3d 1338, 1341 (11th Cir. 2006) (finding defendant guilty of possessing child pornography under CPPA, regardless of defendant’s attempted raising of Trojan Horse Defense); United States v. Bass, 411 F.3d 1198, 1200 (10th Cir. 2005) (disregarding the finding that defendant’s computer was infected with viruses and still found defendant guilty); United States v. Vaughn, Cr. No. F. 05-00482 OWW, 2008 WL 4104241, at *22 (E.D.Cal. Sept. 03, 2008) (determining that Trojan Horse Defense did not lead to a reversal of lower court’s decision to convict defendant of possessing child pornography under CPPA).

See Susan W. Brenner, supra, 21 Santa Clara Computer & High Tech. L.J. at 8 (citing Patricia Dedrick, Auditor: Virus Caused Errors, Birmingham News (AL), August 26, 2003, § News, at 142, available at 2003 WLNR 15960131 (explaining rare case where defendant successfully raised Trojan Horse Defense--regarding tax fraud)). In the successful tax fraud case, the defendant blamed a virus for underreporting over $630,000 in income, over a few years. See id. (discussing non-child pornography case where Trojan Horse Defense was successfully invoked). After hearing defendant-testimony regarding the presence of a virus, the jury acquitted the defendant. See id. (illustrating case where Trojan Horse Defense led to defendant’s acquittal).

See O’Keefe, 461 F.3d at 1340 (explaining convictions defendant is appealing). At District Court, O’Keefe was convicted for receiving, advertising, and possessing child pornography under the CPPA. See id. (discussing convictions from lower court). O’Keefe was a high school math teacher and created two child pornography websites, “hctweens” and “modelquest.” See id. (describing events that led to defendant’s arrest and subsequent conviction).
O’Keefe’s website, “hctweens” — was an abbreviation for “hardcore” and “tweens” — which are children under the age of thirteen. See id. (explaining how defendant’s website’s title suggested child pornography on its face). Homeland Security eventually discovered and shutdown O’Keefe’s websites, but child pornography was already disseminated. See id. (explaining how defendant was located). At trial, the defendant asserted that he was an anti-child pornography vigilante who created the websites in question, because he wanted to capture child pornography viewers. See id. at 1341 (asserting defendant’s claims that he was benefiting society by creating the child pornography websites, rather than doing wrong). O’Keefe continued to explain that his website-traps were hacked by evildoers who changed his computer and placed child pornography on the websites through viruses. See id. (continuing defendant’s explanation of why child pornography was located on his websites). One of the government’s witnesses, James Fottrell, testified that upon inspecting the defendant’s computer, two viruses were discovered. See id. (discussing prosecution’s expert witness who scanned computer for viruses). Although Fottrell discovered multiple viruses on the defendant’s computer, he further testified that the viruses could only alter the default homepage of O’Keefe’s browser. See id. (explaining that although defendant’s computer was infected with viruses, prosecution’s expert witness was not automatically persuaded that viruses downloaded child pornography onto defendant’s computer). Ultimately, Fottrell determined that the viruses infecting the defendant’s computer were incapable of ‘downloading and uploading child pornography and sending out advertisements.’ See id. (asserting prosecution’s expert witness’ conclusion that viruses were not cause of child pornography on defendant’s computer). During closing arguments, the prosecution explained that, “[w]hen both the facts and the law are against you, as a defense attorney, you make something up. . . . You make up the Trojan horse virus.” See id. at 1344 (discussing prosecution’s implication that defense created the Trojan Horse Defense because they were unable to prove defendant’s case). The Eleventh Circuit concluded that a jury could find O’Keefe guilty regardless of the Trojan
Horse Defense argument, because the defendant admitted that the child pornography presented at trial was found on his computer, that he created a website to lure child predators, and that he “solicited” child pornography. See id. at 1350 (discussing reasons why appellate court affirmed district court’s conviction of O’Keefe). For a further discussion of cases that have raised the Trojan Horse Defense, see supra note 92. For a further discussion of the social impact of child pornography, see infra notes 134-149 and accompanying text.

120 United States v. Miller, 527 F.3d 54 (3d Cir. 2008).

121 See id. at 63 & n.8 (3d Cir. 2008) (utilizing computer forensic testimony to aid in conviction of child pornography defendant regardless of presence of computer virus on defendant’s computer).

122 See id. at 59 (depicting the events that eventually led to defendant’s conviction).

123 See id. at 64-65 (discussing events that occurred following search of Miller’s home, but before Miller was tried and convicted of possessing and receiving child pornography).

124 See id. (asserting first time in Miller case where Trojan Horse Defense and computer virus was discussed).

125 See id. at 65 (explaining that government’s expert witness and defendant’s expert witness had varying beliefs as to whether or not Miller, as opposed to a virus, downloaded child pornography).

126 See id. at 65-66 (asserting fundamental problem associated with dates created, written, and accessed, in that Agent Price cannot prove who or what accessed child pornography on defendant’s computer; however, because agent does not know of any computer virus capable of downloading child pornography, he still believes that Miller was guilty).
See id. at 67 (listing factors Miller court took into consideration in deciding that defendant was guilty of possessing and receiving child pornography under CPPA).

See id. (citing United States v. Irving, 452 F.3d 110, 122 (2d Cir. 2006)) (explaining how government proved defendant was guilty of willfully downloading child pornography).

See id. (discussing defendant’s conviction of possessing child pornography).

See id. (citing United States v. Payne, 341 F.3d 393, 403 (5th Cir. 2003)) (discussing how government proved that defendant knowingly receiving child pornography by using the number of images recovered, and titles of images suggestive of child pornography on defendant’s computer).

See id. (citing United States v. Romm, 455 F.3d 990, 997-1001 (9th Cir. 2006)) (asserting that defendant had ability to access child pornography files when they were automatically stored in Internet Cache).

See id. at 59 (explaining what transpired at lower court, and what was later determined to be violation of double jeopardy clause).

See id. at 63 n.8 (providing computer forensic expert testimony from trial for Miller). The prosecution’s FBI Agent declares that although he is aware of viruses which could download material onto an unsuspecting person’s hard drive, he was unaware of such a program that sought out and specifically downloaded child pornography. See id. (discussing computer forensic testimony).

See id. (explaining that Agent Price knew of no virus that downloaded child pornography).

See id. (continuing Agent Price’s testimony). 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. (providing information about Agent Price’s testimony).

136 See id. (concluding that Agent Price did not believe that virus downloaded child pornography onto computer in question).

137 For a further discussion of Miller, see supra notes 101-114 and accompanying text.

138 See, e.g., United States v. Bass, 411 F.3d 1198, 1202 (10th Cir. 2005) (considering that defendant had software on his computer that would delete images and browsing history from defendant’s computer); Susan W. Brenner, et al., supra note 103, at 22-26 (explaining ways for prosecution to rebut Trojan Horse Defense); Note, Child Pornography, the Internet, and the Challenge of Updating Statutory Terms, 122 Harv. L. Rev. 2206, 2224-26 (2009) (discussing repeat behavior model, that courts can utilize when presented with Trojan Horse Defense).

139 See Note, supra note 134, at 2224-26 (discussing how “repeat behavior model” can aid courts when Trojan Horse Defense is raised by defendant). The author explains:

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.

Id. (discussing repeat behavior model).
See id. (explaining tools courts use when deciding cases where viruses are present). See also United States v. Shiver, 305 F. App’x 640, 641 (11th Cir. 2008) (explaining what convictions defendant appeals). Shiver was convicted of knowingly possessing and transporting child pornography under the CPPA. See id. (discussing defendant’s convictions). On appeal, Shiver contends that he did not knowingly possess any child pornography. See id. (explaining defendant’s appellate arguments). Shiver asserts that a virus caused his computer to download child pornography without his knowledge. See id. at 643 (discussing one of defendant’s several contentions as to how trial court’s decision should be reversed). The court explains, “Shiver argues that the government failed to show that he was aware of the images or that he exercised any control over them. Instead, he maintains that they were placed on his computer without his knowledge by a virus or by ‘pop-up’ windows that appeared on his computer screen unbidden. [The court] is not persuaded.” See id. (asserting that defendant’s virus defense failed). When determining how to consider the Trojan Horse Defense, the court looked to a number of other factors. See id. (discussing inadequacy of defendant’s Trojan Horse Defense). The court reasoned that:

The government also produced substantial indirect evidence that Shiver knowingly possessed the images. For example, during an interview with authorities, Shiver referred to himself as a ‘pedophile.’ In addition, the government’s computer expert testified that Internet searches conducted on Shiver's computer used words and terms that were likely to return pornographic images of children, and that many of the illicit images on Shiver's computer had been accessed on multiple occasions, thus belying Shiver's contention that a virus had placed the images on his computer without his knowledge. The government's expert also opined that, as a technological matter, the images on Shiver's computer could not plausibly be accounted for by pop-up windows. Shiver insists that since all of
the images had been deleted and stored in his computer's unallocated files, and since he lacked the "forensic software" to access or retrieve the images from that location, he consequently lacked the ability to exercise dominion or control over the images. But even assuming that Shiver was in fact unable to retrieve the images from the unallocated files, he was able to exercise control over the images by deleting them from his computer's cache.

Id. (citing United States v. Romm, 455 F.3d 990, 1000-01) (asserting that when child pornography defendants personally delete illegal images, they exercise dominion and control over them; therefore, they satisfy possession element of CPPA).

141 See Susan W. Brenner, et al., supra note 103, at 22 (discussing how defendant’s knowledge about computers can aid prosecution in proving that virus did not download child pornography).

142 See id. (explaining how defendant’s knowledge of computers can aid in convicting defendant). Brenner explains that:

Based on [the authors’] experience with the defense to date, it 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.

143 See Bass, 411 F.3d at 1202 (discussing how jury utilized information that revealed defendant used programs to delete files and internet history).

144 See id. (explaining how presence of some programs can aid in convicting defendant). The appellate court explains that:

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 . . . .” Both programs were installed on the computer when it was searched. . . . [t]here was sufficient evidence of knowing possession of child pornography.

Id. (discussing reasons for Bass’ conviction).

145 For a further discussion of the Trojan Horse Defense and how it has affected child pornography cases, see supra notes 92-136 and accompanying text.

146 For a further discussion on how society is impacted by child pornography litigation, see infra notes 139-149 and accompanying text.

147 See Ashcroft v. Free Speech Coalition, 535 U.S. 234, 244-45 (2002) (explaining why child pornography is so despised). The Court explained that “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.” Id. (noting legislative history related to criminalizing possession of child pornography).

148 For a further discussion of how CPPA was utilized, defined, and confused through child pornography cases and Trojan Horse Defense, and government’s intention to prosecute child pornography defendants consistently, see supra notes 46-124 and accompanying text.


150 See id. (discussing illegality of child pornography and how courts have inconsistently applied CPPA).


152 See id. (discussing Congress’ long fight against child pornography); see also 18 U.S.C. § 2252A (1996) (criminalizing transportation, possession, receiving, and producing of child pornography).


154 See id. (explaining how Congress amended CPPA, but courts may still encounter questions regarding its application). For a further discussion of how the 2008 amendments to the CPPA have yet to be fully defined and tested, see supra notes 10-11 and accompanying text.
See id. (elaborating on how courts will face questions regarding CPPA, but they must remember Congress’ intent to enhance prosecution under 2008 amendments).


See id. (discussing that enacting CPPA is only way for Congress to execute ways of eliminating child pornography). Congress stated that:

(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 (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. (enumerating reasons why Congress amended CPPA).

158 See id. (explaining that Congress’ enactments to end child pornography, illustrate its intentions).

159 See id. (asserting government’s interest in ending child pornography in America).

160 For a further discussion on the legislative intent behind the enactment of the CPPA and the social impact of child pornography, see supra notes 134-146 and accompanying text.

161 For a further discussion of how the CPPA was utilized, defined, and confused through child pornography cases and the Trojan Horse Defense, and government’s intention to prosecute child pornography defendants consistently, see supra notes 46-124 and accompanying text.

162 For a further discussion on the legislative intent behind the enactment of the CPPA and the social impact of child pornography, see supra notes 134-146 and accompanying text.


164 Compare United States v. Stulock, 308 F.3d 922, 924 (8th Cir. 2002) (deciding that defendant was innocent of possessing child pornography because he did not download material), with United States v. Tucker, 305 F.3d 1193, 1205 (10th Cir. 2002) (concluding that defendant satisfied possession element of CPPA by merely viewing child pornography and having it stored in Internet Cache).

165 For a further discussion of how the CPPA is confused through the possession element and the Trojan Horse Defense, see supra notes 46-124 and accompanying text.

For a further discussion of the reasons Congress enacted the CPPA, see supra 35-41 notes and accompanying text.

For a further discussion of the reasons Congress enacted the CPPA, see supra 35-41 notes and accompanying text.

For a further discussion on the legislative intent behind the enactment of the CPPA and the social impact of child pornography, see supra notes 134-146 and accompanying text.