UIC John Marshall Journal of Information Technology & Privacy Law

Volume 33 | Issue 2 Article 1

2017

Ignorance of Technology a Pass for Violating Child Pornography Laws? – What's the Cache?, 33 J. Marshall J. Info. Tech. & Privacy L. 47 (2017)

Angela Lewosz

COMMENTS

IGNORANCE OF TECHNOLOGY A PASS FOR VIOLATING CHILD PORNOGRAPHY LAWS? – WHAT'S THE CACHE?

ANGELA LEWOSZ *

INTRODUCTION

In *United States v. Tucker,* the court found the defendant, Tucker, guilty of possessing child pornography after Tucker viewed child pornography on his computer, knowing that these images were stored on his hard drive by his internet cache (an internet file that automatically saves images appearing on a user's webpage).[1] After each internet session, Tucker would go into his internet cache and delete the images.[2] Since, legally, Tucker exercised control over the images in the cache files, the court determined that he possessed the images.[3]

---

* Angela Lewosz is from Des Plaines, Illinois, and received a BS in Finance from DePaul University in 2015. Angela is a JD candidate at the John Marshall Law School, expecting to graduate in June 2018. She is the 2017-2018 Editor-in-Chief of the John Marshall Journal of Information Technology & Privacy Law. She would like to thank the members of the Journal for their assistance in editing this Comment.

1. *United States v. Tucker*, 305 F.3d 1193, 1198 (10th Cir. 2002); *The Fundamentals of Cache,* SL CENTRAL (Oct. 17, 2000), http://www.slcentral.com/articles/00/10/cache/print.php.

2. *Id*.

3. *Id*. (holding that Tucker's control over the images in the cache were established by his "habit of manually deleting images from the cache files."). A forensic examination revealed that Tucker went into his cache files and dragged images from the cache files into his computer's recycle bin. *Id*. Tucker said that he would delete the images from his cache files after each one of his Internet sessions. *Id*. Tucker argued that he did not have control over the images in the cache because his web browser automatically saved images into his cache files without any action on his part. *Id*. at 1199. However, Tucker still admitted that he knew the web browser would save the images. *United States v. Tucker*, 305 F.3d 1193, 1204 (10th Cir. 2002). The district court dismissed this argument, reasoning that Tucker specifically visited these websites to look at child pornography and the images would not have been saved into the cache, had he not intentionally searched for them. *Id*. at 1199 The Court of Appeals agreed with this reasoning and added that Tucker had the ability to control the images in the cache by attaching it in an email, posting it on a web-

In *United States v. Kuchinski*, the court found the defendant, Kuchinski, not guilty of possessing child pornography after he viewed child pornography on his computer, not knowing the images were stored on his hard drive by his internet cache.[4] The court ruled that since Kuchinski did not know that the cache files stored these images, he did not possess them.[5]

Both of these men simply searched the internet for child pornography and viewed it.[6] They did not save the images, nor did they distribute the images.[7] Essentially, they used the internet for the same purpose.[8] Yet, because one man knew that the cache stored images and took action to make sure the images were deleted, the court found him guilty of possessing child pornography.[9] On the other hand, the man who was ignorant of technology got a free pass.[10] Ignorance of the law is no excuse, so why should ignorance of technology be an excuse?[11]

18 U.S. Code § 2252(a)(4)(B) states that it is illegal to knowingly possess child pornography.[12] The two examples mentioned above all

---

site, renaming it, and modifying it. *Id*. at 1204 Because Tucker could treat the images inside of his cache like any other image saved on his computer, he was found in possession of the image. *Id*.

4. *United States v. Kuchinski,* 469 F.3d 853, 862 (9th Cir. 2006).

5. *Id*. at 863 (holding that a defendant should not be charged with possession and control of child pornography when he does not know about the existence of cache files, unless there is some other evidence that the defendant had control and dominion over the images in the cache files). Kuchinski admitted that he knowingly possessed 110 images that he downloaded. *Id*. at 861 However, an additional 13,904 to 17,784 images were found in his Deleted Temporary Internet Files. *Id*. at 856 These additional images would make a substantial difference in calculating his guidelines sentencing range. *Id*. at 862 The base offense level with the 110 images that he had downloaded was at 19. *Id*. However, 5 levels would be added to the base offense if there were over 600 images present. *United States v. Kuchinski,* 469 F.3d 853, 862 (9th Cir. 2006). This difference in the sentencing guidelines are impacted directly by the images that are found within the cache. *Id*. Since the court held that Kuchinski should not be charged with possession and control of the images in his cache, since he did not know about the existence of the cache, the images found in the cache files should not have been taken into account for sentencing purposes. *Id*. at 863

6. *Tucker*, 305 F.3d at 1198; *Kuchinski,* 469 F.3d at 862.

7. *Tucker*, 305 F.3d at 1198; *Kuchinski,* 469 F.3d at 862.

8. *Tucker*, 305 F.3d at 1198; *Kuchinski,* 469 F.3d at 862 (9th Cir. 2006).

9. *Tucker*, 305 F.3d at 1195.

10. *Kuchinski,* 469 F.3d at 863.

11. *Check v. United States,* 498 U.S. 192, 199 (1991) (explaining that "ignorance of the law or a mistake of law is no defense to criminal prosecution" and it is presumed that everyone knows the law).

12. 18 U.S.C. § 2252(a)(4)(B) (2016) (providing in part: "(a) Any person who … (4) either … (B) knowingly sells or possesses with the intent to sell any **child pornography** that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; shall be punished as provided in subsection (b).")[emphasis added].

center around the question of what does "possession" actually mean.[13] That question is fairly easy to answer when thinking about tangible items that people own. For example, someone can say that one possesses a painting that is hanging on a wall in his/her home. On the contrary, one would say that someone does not own a painting that he/she is standing in front of in an art gallery; he/she is just viewing the painting.[14] Surely, one does not possess this painting if he/she is just viewing it.[15] How can this question be answered when thinking about digital images? Does someone possess child pornography simply because he/she viewed the image on his/her computer screen? Does it matter how many images the individual viewed or if the individual viewed one image multiple times? Is there a difference of possession if the images are saved onto the computer by the user or are saved automatically by the browser into the cache? Courts have not given clear answers to these questions and have come up with different rulings on what constitutes as possession.[16]

It is difficult for the courts to answer these questions because of continuing advances in technology.[17] In 2008, Congress added amendments to 18 U.S. Code § 2252, which criminalize viewership of child pornography.[18] However, these amendments do not address the fact that the cache saves virtually everything that a user views.[19] When a user visits a website, the browser automatically downloads the images

13. *Tucker*, 305 F.3d at 1198 (holding that Tucker's control over the images in the cache were established by his "habit of manually deleting images from the cache files."); *Kuchinski,* 469 F.3d at 863 (holding that a defendant should not be charged with possession and control of child pornography when he does not know about the existence of cache files, unless there is some other evidence that the defendant had control and dominion over the images in the cache files).

14. *United States v. Romm,* 455 F.3d 990, 1001 (9th Cir. 2006).

15. *Id*.

16. See, e.g., Priscilla M. Grantham, *"But Your Honor, I Didn't Possess Those Pictures; My Computer Did." Temporary Interest Files, Web Browser Cache Files, and Child Pornography.* NAT'L CENTER FOR JUSTICE AND THE RULE OF LAW (2009) (noting that *Tucker* and *Kuchinski* are two of the leading cases that show the discrepancy between courts when images found inside of an internet cache are at issue).

17. *Id*. (explaining that two people do not need to exchange child pornography in dark alleys anymore; child pornography can be produced with digital video recorders, cameras, phones, and then exchanged via the internet).

18. 18 U.S.C. § 2252(a)(4)(B)(Act Oct. 8, 2008, in subsec. (a), in para. (1), in the introductory matter, inserted "using any means or facility of interstate or foreign commerce or", in para. (2), in the introductory matter, inserted "using any means or facility of interstate or foreign commerce or" in two places, in para. (3)(B), in the introductory matter, inserted ", shipped, or transported using any means or facility of interstate or foreign commerce", inserted "using any means or facility of interstate or foreign commerce", and deleted "by any means," preceding "including by computer", and, in para. (4), in para. (A), inserted ", or knowingly accesses with intent to view,", in para. (B), in the introductory matter, inserted ", or knowingly accesses with intent to view,", inserted "using any means or facility of interstate or foreign commerce or"; and substituted "in or affecting interstate" for "in interstate" wherever appearing.)

19. *Kuchinski,* 469 F.3d at 862.

on a webpage into a temporary folder, called the cache.[20] The purpose of this is so that when the user revisits the website at a later time, these already stored images will help the webpage load much quicker than if the user was visiting the website for the first time.[21] This whole process occurs without the knowledge of most average users.[22] Throughout this automatic process, an individual may not scroll to the bottom of a page, and yet all of the images on that page will be stored in the cache.[23] Therefore, courts cannot prove that a defendant actually viewed such an image just because it exists in the defendant's cache.[24]

This comment explains how the cache works, discusses computer forensic examinations, and provides a history of child pornography laws. It next explores how the courts have interpreted the changing pornography laws with advances in technology. It then specifically assesses the different approaches the courts take when reconciling the *mens rea* (the mental element) of knowledge in accordance with possession. Finally, this comment analyzes the strengths and flaws in the courts' arguments and suggests a proposal for how the courts should deal with the cache in relation to the criminalization of possession within the federal child pornography laws.

BACKGROUND

THE HISTORY OF CHILD PORNOGRAPHY LAWS

In 1977, with a surge of child pornography public awareness, Congress enacted the Protection of Children Against Sexual Exploitation Act ("PCA").[25] The PCA criminalized commercial producers, distributors, and receivers of obscene child pornography (child pornography is deemed to be obscene if it "appeal[s] to the prurient interest in sex, which portray[s] sexual conduct in a patently offensive way, and which, taken as a whole, do[es] not have serious literary, artistic, political, or scientific value".[26] Following this was the 1982 landmark decision in

---

20. *Id.*

21. *Id.*

22. *Id.*

23. *United States v. Dobbs,* 629 F.3d 1199, 1210 (10th Cir. 2011).

24. *Id.*

25. Audrey Rogers, *From Peer-to-Peer Networks to Cloud Computing: How Technology Is Redefining Child Pornography Laws*, 87 ST. JOHN'S L. REV. 1013, 1016 (2013), http://digitalcommons.pace.edu/lawfaculty/963/, *See* 18 U.S.C. § 2251 (2008). Child pornography is defined as "any visual depiction" of a "minor" taking part in "sexually explicit conduct." Child pornography is essentially a visual of a child "suffering real sexual abuse." A minor is defined as "a real child under eighteen years old." Sexually explicit conduct is defined as "actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal' intercourse; 'bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person." J. Elizabeth Mcbath, *THRASHING OUR SYSTEM OF JUSTICE? OVERTURNING JURY VERDICTS WHERE EVIDENCE IS FOUND IN THE COMPUTER'S CACHE,* 39 AM. CRIM. L. 381, 383-384 (2012).

26. Rogers, *supra* note 25 at 1017.

New York v. Ferber, where the Supreme Court held that the First Amendment does not protect child pornography.[27] Following the decision in *Ferber,* Congress passed the PCA Act of 1984.[28] In this act, Congress removed the obscenity and commercial production requirement

27. *New York v. Ferber,* 458 U.S. 747, 774 (1982) (holding that child pornography is not protected by the First Amendment and does not provide an exception for child pornography containing "serious literary, scientific, or educational value are"). The statute at issue in this case, §263.15 (a New York law which controls the dissemination of child pornography) prohibited anyone from "promoting a sexual performance by a child when, knowing the character and content thereof, he produces, directs or promotes any performance which includes sexual conduct by a child less that sixteen years of age." *Id*. at 751. Sexual performances are defined as "any performance or part thereof which includes sexual conduct by a child less than sixteen years of age." *Id*. Sexual conduct is defined as "actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sado-masochistic abuse, or lewd exhibition of the genitals. *Id.* A performance is defined as "any play, motion picture, photograph or dance" or "any visual representation exhibited before an audience." *Id*. Promote is defined as a "means to procure, manufacture, issue, sell, give, provide, lend, mail, deliver, transfer, transmute, publish, distribute, circulate, disseminate, present, exhibit or advertise, or to offer or agree to do the same." *Id*. Ferber, the defendant, was an owner of a sexually oriented bookstore in Manhattan. *New York v. Ferber,* 458 U.S. 747, 751-752 (1982). Ferber sold two films containing young boys masturbating to an undercover police officer. *New York v. Ferber,* 458 U.S. 747, 752 (1982). Ferber was found guilty under a jury trial for violating §263.15. The Appellate Division of the New York Supreme Court affirmed and the New York Court of Appeals reversed, stating that §263.15 violated the First Amendment. *Id*. at 751. The United States Supreme Court granted certiorari to rule on the question: "To prevent the abuse of children who are made to engage in sexual conduct for commercial purposes, could the New York State Legislature, consistent with the First Amendment, prohibit the dissemination of material which shows children engaged in sexual conduct, regardless of whether such material is obscene?" *Id*. at 753. The court ruled that States are able to regulate child pornography beyond an obscenity standard. *Id*. at 756. The court first explained that the state has a compelling interest in "safeguarding the physical and psychological well-being of a minor." *Id*. at 756-757. Second, the distribution of films showing child pornography is related to the abuse of a minor because the films display a permanent record of a child participating in sexual conduct and the distribution network for such films must be stopped to control the exploitation of children. *Id*. at 759 Ferber argued that instead of regulating child pornography under a state statute, it should be regulated under the *Miller* obscenity test. *New York v. Ferber,* 458 U.S. 747, 760 (1982). The *Miller* test asks whether a work "appeals to the prurient interest of the average person." *Id*. at 761 The court explained that this test does not help combat the issue of a child suffering abuse from the distribution of child pornography in which he or she is depicted in. *Id*. Furthermore, the *Miller* test does not prohibit work that is not necessarily offensive or which has "literary, artistic, political, or scientific value." *Id*. The fact that a depiction of child pornography is not obscene or has some kind of value is irrelevant to the fact that a child has been abused. *Id*. Third, the child pornography industry has an economic motive of an illegal activity. *Id*. Fourth, it is extremely unlikely that any kind of child pornography would provide significant literary value, as the means could be accomplished without using an actual child. *New York v. Ferber,* 458 U.S. 747, 762 (1982). Fifth, the First Amendment does not protect all speech; it only protects certain categories of speech. *Id*. Ultimately, the court held that the statue, §263.15, as written, pertains to a category that is not entitled to First Amendment protection. *Id*. at 765.

28. Rogers, *supra* note 25 at 1017.

from the 1977 act.[29]

As new technology began to emerge, Congress again amended the 1977 version of the PCA in 1988 to prohibit the use of a computer to move child pornography.[30] In 1996, Congress enacted the Child Pornography Prevention Act of 1996 ("CPPA").[31] This amendment prohibits the possession of computer disks with child pornography on it and adds "virtual" (computer-generated) material to the definition of child pornography.[32] Congress realized that as technology was becoming more advanced, people could manipulate children in sexually explicit images.[33] Not only was actual child pornography now criminalized, but pornography that appeared to include children was criminalized as well.[34] For example, people can manipulate adult pornography so that a child's head appears on an adult's body.[35] Thus, people do not use an actual child to produce the pornography, but a child still appears to be in the pornography.[36] In 2008, with the continued growth of technology, Con-

---

29. *Id.*; *See Miller v. California,* 413 U.S. 15, 20-23 (1973) (explaining that obscenity law protects sexually explicit work if it shows serious artistic value); *See also Ferber,* 458 U.S. at 774 (holding that child pornography is not protected by the First Amendment and does not provide an exception for child pornography containing "serious literary, scientific, or educational value are"). Congress found that child pornography circulated by gift or exchange, so by having a commercial requirement, the statute could not effectively reach most transactions. Rogers, *supra* note 25 at 1017; *See Miller,* 413 U.S. at20-23 . This issue became even worse with the emergence of technology, which is now primarily used to exchange child pornography. Rogers, *supra* note 25 at 1017. Congress also discovered that between 1978 and 1984, there was only one person who was convicted of producing child pornography. *Id.* at 1018. Therefore, Congress was more interested in stopping the exchange of child pornography, rather than the production of it. *Id.* It was hard for the law to reach producers of child pornography since most of it is produced in countries that do not have effective laws deterring the production of child pornography. *Id.*

30. Deborah F. Buckman, *Validity, Construction, and Application of 18 U.S.C.A. § 2252(a), Proscribing Certain Activities Relating to Material Constituting or Containing Child Pornography*, 2 A.L.R. Fed 2d 533, 544 (2005).

31. *Id.* Congress explained that it has "a compelling governmental interest in criminalizing the production, distribution, possession, sale, or viewing of visual depictions of children engaging in sexually explicit conduct." *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. *Ashcroft v. Free Speech Coalition,* 535 U.S. 234, 242 (2002).

36. Rogers, *supra* note 25 at 1020. The Supreme Court challenged the CPPA and held that the prohibitions in regard to virtual images were "overbroad and unconstitutional" because it prohibited images that were not obscene and that did not contain actual children in them. *Ashcroft,* 535 U.S. at 258. The Court explained that the statute essentially prohibited images that contained adults who looked like children or by using computer imaging. *Id.* The Supreme Court disagreed with the amendment and struck it down because virtual pornography did not contain actual children that were being abused. Rogers, *supra* note 25, at 1020. The Court explained that the penalties under the CPPA were extremely severe. *Ashcroft,* 535 U.S. at 244. A first offense could put someone in prison for 15 years and a repeat offender would have a sentence between 5 and 30 years in prison. *Id.* The Court went on to explain that film makers or book publishers would not be inclined to create art as freely, in fear of being punished by this law. *Id.*. Some of the greatest literary works, such as *Romeo and*

gress expanded the definition of possession of child pornography to "accessing with intent to view."[37]

THE CACHE

Cache is derived from the word "*Cacher,"* which means "to hide" in French.[38] When a user is browsing the internet, images that appear on his/her screen are automatically stored into a Temporary Internet Cache folder.[39] The user has no control over this process, unlike when a user intentionally saves an image onto his/her computer.[40] The purpose of caching is for the internet browser to be able to load images quicker.[41] When many internet users access the same webpage, this can put a burden on the workload of servers.[42] When a user visits the page a second time, the information that is stored through caching is accessed, and by using those images, the page loads much more quickly.[43] This slows down the amount of time it takes for the entire webpage to load.[44] This makes the user's internet experience and the overall network performance much more efficient.[45]

However, given the fact that caching saves every image that comes across the screen, images that the user did not intend to come across are also saved into the cache.[46] For example, caching also saves images

---

Juliet, have themes of child abuse and teenage sexual activity. *Id*. at 247. The Court notes that the CPPA is so broad that is prohibits any material that would "convey the impression" that minors are involved in the work. *Id*. at 257. Therefore, a film could contain no instances of minors engaged in sexually explicit scenes, but the title could "convey the impression" that child pornography is involved. *Id*. The analysis the courts would have to follow under the statute depend on "how the speech is presented, not on what is depicted." *Ashcroft v. Free Speech Coalition,* 535 U.S. 234, 257 (2002). Ultimately, the Court explained that the CPPA is in fact targeting speech that is protected by the First Amendment. *Id*. Congress disagreed with the Supreme Court, nothing that virtual pornography is "'indistinguishable' from a real depiction." Rogers, *supra* note 25, at 1020. Congress then enacted the 2003 PROTECT Act which "created a five-year minimum sentence for transporting, distributing, or receiving child pornography." *Id*. The PROTECT Act essentially contained the same sentencing rules for a possession of child pornography offense. *Id*.

37. Rogers, *supra* note 25, at 1020; 18 U.S.C. § 2252A(a)(5)(B).

38. *Andrew S. Tanenbaum, MODERN OPERATING SYSTEMS* 178, 305 (1992).

39. *United States v. Parish,* 308 F.3d 1027 (9th Cir. 2002). The type of cache being referenced to in this comment is a web browser cache. The word cache (or "system cache,) in general, may refer to a storage area on a computer, separate from the web browser cache. *See* Paul Mazzuco, *The Fundamentals of Cache,* SL CENTRAL (Oct. 17, 2000), http://www.slcentral.com/articles/00/10/cache/print.php.

40. *See Parish,* 308 F.3d 1027 (9th Cir. 2002).

41. Cache, WEBOPEDIA COMPUTER DICTIONARY, http://www.webopedia.com/TERM/C/ cache.html (last visited Sept. 11, 2016).

42. Richard S. Vermut, *File Catching on the Internet: Technical Infringement or Safeguard for Efficient Network Operation?,* 4 J. INTELL. PROP. L. 273, 337 (1997).

43. *Id*. at 336.

44. *Id*.

45. *Id*.

46. *Dobbs,* 629 F.3d at 1210 (explaining that the cache saves images even when

that show up on the screen through pop-up ads or through malicious software.[47] In these examples, the user is not intentionally accessing the website where these images are saved from.[48]

Though the cache automatically stores information without any action on behalf of the internet user, there are three ways in which images can be deleted from the cache.[49] The web browser automatically deletes images out of the internet cache when the images hit a certain amount.[50] The user can also command the browser to empty the cache at any time.[51] Finally, the user can manually delete individual files out of the cache.[52] When a user knows how to access the cache, he/she can open up the image to view, print, rename, or move it to another folder.[53] The user can essentially treat this file like any other file he has on his computer.[54] However, when the user deletes images from the cache, the images are moved into the computer's unallocated space on the hard drive.[55] The images remain in this unallocated space until other files overwrite them.[56] Images located in this unallocated space can only be accessed by forensic software.[57]

COMPUTER FORENSIC EXAMINATIONS

Computer forensic examinations start with acquisition, proceed with authentication, and end with recovery.[58] The forensic examiner can acquire evidence from a computer on-site by searching the computer and printing hard copies of certain images or by making electronic copies of the images.[59] The forensic examiner can also duplicate an electronic copy of everything that is stored on the computer or take the whole computer hardware to examine the images stored off-site.[60] Police officers all concur that taking the whole computer off-site is the best

---

a user has not scrolled and therefore actually seen an image that is displayed on the webpage).

47. *Id*.

48. *Id*.

49. *Romm,* 455 F.3d at 995.

50. *Id*.

51. *Id*.

52. *Id*.

53. *Id*.

54. *Id*.

55. *United States v. Flyer,* 633 F.3d 911, 918 (9th Cir. 2011).

56. *Id*.

57. *Id*. An example of a forensic program used by law enforcement is called EnCase. *EnCase Forensic,* GUIDANCE SOFTWARE, INC. https://www.guidancesoftware.com/encase-forensic (last visited Nov. 18, 2016). This program is sold by Guidance Software, Inc. *Id*. The program is designed to be used for the whole forensic investigation, beginning when a case is opened to the end of the investigation. *Id*.

58. Wayne Jekot, *COMPUTER FORENSICS, SEARCH STRATEGIES, AND THE PARTICULARITY REQUIREMENT,* 7 PGH. J. TECH. L. & POL'Y 5, 15 (2007).

59. *Id*. at 17.

60. *Id*..

method to ensure that all stored data on the computer can be properly examined.[61] Once officers take the computer off-site, forensic examiners make a copy of all of the images stored on the hardware.[62]

After copying the data, forensic examiners authenticate it by comparing the data on the computer to the copy.[63] Forensic software accomplishes this by a hashing algorithm, which takes the data stored on a computer as an input and produces hash values, which are a unique set of numbers, as an output.[64] Hash values are like fingerprints, in that the probability of having two different sets of data with the same value is almost impossible (even if the sets of data have minor differences, both of them will have different hash values).[65] Forensic examiners then compare the values of the original data (found on the computer's hard drive) and the copied data (the data that forensic examiners copied from the hard drive).[66] If both values are the same, then forensic examiners successfully authenticated the copy and can properly analyze the data.[67]

The final step of a computer forensic examination is the analysis of the data.[68] Forensic examiners can view files from the computer's cache, as well as files that a user deleted from the cache and moved into unallocated folders.[69] Forensic examiners can also analyze information such as a user's browsing history, how many times the user visited a certain website, downloaded files, as well as whether a user manipulated certain files.[70] This manipulation can involve things such as moving images to different folders, enlarging, cutting, or pasting images.[71] After this analysis, prosecutors must determine whether a user violated any law.[72]

---

61. *Id*. at 29; Usually, authorities can only obtain the original computer through a traditional search warrant. *See* Computer Crime & Intel. Prop. Section, U.S. DEP'T OF JUSTICE, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009), *available at* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf. (last visited Nov. 19, 2016). There have been a number of issues that have arisen in the courts, regarding Fourth Amendment issues in relation to computer-based child pornography. *See* Amy E. Wells, *COMMENT:* Criminal Procedure: *The Fourth Amendment Collides with the Problem of Child Pornography and the Internet,* 53 OKLA. L. REV. 99 (2000).

62. Jekot, *supra* note 58, at 29.

63. *Id*. at 30.

64. *Id*. at 31.

65. *Id*.

66. *Id*. at 37.

67. *Id*.

68. Wayne Jekot, *COMPUTER FORENSICS, SEARCH STRATEGIES, AND THE PARTICULARITY REQUIREMENT,* 7 PGH. J. TECH. L. & POL'Y 5, 41 (2007).

69. Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Files,* 19 BERKELEY TECH. L.J. 1227, 1234-1235 (2004).

70. *Id*. at 1236.

71. *Id*.

72. *Id*.

ANALYSIS

18 U.S. Code § 2252, the federal child pornography statute, does not actually define what possession means.[73] The standard legal meaning of the term "possess" can be defined as "[t]he fact of having or holding property in one's power; the exercise of dominion over property."[74] Courts have expanded on this definition and have said that "[t]he government must prove a sufficient connection between the defendant and the contraband to support the inference that the defendant exercised dominion and control over [it]."[75] Since there is no one definition that applies to the possession of digital images, the courts have struggled to apply the legal definition in cases that involve finding images stored in a computer's cache.[76]

Assistant District Attorney Ty E. Howard explained the difficulty that courts have with images found in a computer's cache by analyzing the typical factors that various courts use in determining whether someone possesses contraband.[77] The factors include: "knowledge of the contraband," "destruction of the contraband," "manipulation and control over the contraband," seeking and obtaining the contraband, "the amount of contraband," and any other evidence that may be relevant.[78] Normally, the courts would find someone in possession of tangible contraband if they meet the above factors.[79] However, this becomes tricky when courts analyze these factors to determine possession of digital images, which are not tangible.[80] Digital images that are found in the cache are copies of images that have existed on the computer screen at some point in time.[81] The court must determine which version of the image the court will analyze under these factors: digital images that once appeared on the computer screen or copies of digital images in the cache.[82]

Ty E. Howard also first recognized that the courts implicitly use two different approaches to determine if an individual possesses images that are in his computer cache.[83] The first approach is called the "Pre-

---

73. *18 U.S.C. §§2252*, 2252A (2006).

74. BLACK'S LAW DICTIONARY 1183 (7th Ed. 1999).

75. *United States v. Carrasco,* 257 F.3d 1045, 1049 (9th Cir. 2001) (quoting *United States v. Gutierrez,* 995 F.2d 169, 171 (9th Cir. 1993).

76. Howard, *supra* note 69, at 1253.

77. *Id*. Howard is an Assistant District Attorney at the Chester County District Attorney's Office, West Chester, Pennsylvania. *Id*. He received his B.A. from Pennsylvania State University in 1994, his M.G.A. from the University of Pennsylvania in 1997, and his J.D. in 200 from Georgetown University. *Id*. Howard was the first to analyze the fact that courts who do not understand how the cache works can make incorrect rulings based on images that are found in the cache, versus images that once appeared on a computer screen. Mcbath, *supra* note 25, at 383-384.

78. Howard, *supra* note 69, at 1253.

79. *Id*.

80. *Id*.

81. *Id*.

82. *Id*.

83. *Id*. at 1254.

sent Possession" approach, where the courts have ruled that images found inside of the cache render "actual knowing possession at the time the images are found."[84] The second approach that courts use in child pornography cases involving the cache is called the Evidence Of Approach.[85] Under this approach, courts have ruled that images found inside of the cache indicate prior knowing possession.[86] The number of child pornography images found in an individual's cache does not have a significant bearing under either approaches.[87] Extraneous evidence is also not a significant factor that the courts analyze under either approaches.[88] The reason that courts do not rely on such evidence is because the evidence does not show knowing possession of the images that are at question.[89] The evidence simply shows that the individual has an interest in child pornography.[90]

PRESENT POSSESSION APPROACH

The Law

Under the Present Possession Approach, possession begins when an individual searches for an image that is automatically saved in the computer's cache.[91] Possession ends when the user manually deletes the file or when the cache automatically overwrites the file.[92] The analogy to best describe this approach is one of a file cabinet- where the cache is a file drawer automatically "filing" the downloaded images, as if they were files, into its file drawer.[93]

When analyzing the factors under the Present Possession approach, knowledge of images within the cache is significant because this ap-

---

84. 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, 1254 (2004); Federal cases that use the Present Possession Approach include: *Dobbs,* 629 F.3d at 1199; *United States v. Flyer,* 633 F.3d 911 (9th Cir. 2011); *Kuchinski,* 469 F.3d at 853; *Romm,* 455 F.3d at 990; *Tucker* 305 F.3d at 1193.

85. Howard, *supra* note 69, at 1254; Federal cases that use the Evidence Of Approach include: *United States v. Kain,* 589 F.3d 945 (8th Cir. 2009); *United States v. Pruitt,* 638 F.3d 763 (11th Cir. 2011); *United States v. Zarn*, 365 F. App'x 838 (9th Cir. 2010).

86. Howard, *supra* note 69, at 1255.

87. *Id*. at 1263.

88. *Id*. Some examples of extraneous evidence are: witness testimony, past behavior, hard copies of child pornography inside of the individual's home, and stories mentioning child pornography. *Id*.

89. *Id*.

90. *Id*.

91. 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, 1254 (2004).

92. *Id*. at 1255.

93. *Id*. at 1254.

proach focuses on the actual images inside of the cache.[94] If an individual is not aware of the cache, he/she cannot knowingly possess the images found inside of it.[95] Even if an individual claims he/she had no knowledge of the cache, courts have established knowledge by analyzing the user's general familiarity with the computer.[96]

Next, under the Present Possession approach, destruction of images that are in the cache may lead the court to determine that the individual knowingly possessed the image.[97] For example, in *United States v. Tucker,* the court found the defendant, Tucker, guilty of possessing child pornography because of his regular habit of manually deleting images stored inside of his computer's cache.[98] The court explained that because he was able to access the images to delete them, this showed that he had dominion and control over them.[99] On appeal, Tucker argued that he searched for child pornography only for the purpose of viewing the images, not to possess the images.[100] He further argued that he had no control over the saved images, as the web browser automatically saved these images into the cache.[101] The Court disagreed, and explained that he knowingly possessed the images since he purposely sought out these images and the court also noted that "the images would not have been saved to his cache file had Tucker not volitionally reached out for them."[102] Even though Tucker admitted that he knew the internet cache saved the images, he argued he did not want them to be saved on there; which is why he deleted them after each internet session.[103] The Court did not find this argument convincing, reasoning that when an individual has access to an image in a cache file, he/she can "attach it to an email, post it to a newsgroup, place it on a Web site, or print a hard copy."[104] Basically, an individual can do to a cached image whatever he/she can do to an image that he/she saves on his/her computer, thus exercising control over the image.[105]

The Court seems to base its whole argument on what Tucker *could* have done with the images, and not his actual actions.[106] It did not matter that all Tucker did was delete the images, as opposed to modifying, sending, or printing them.[107] Therefore, under the Present Possession

---

94. *Id*. at 1256.
95. *Id*.
96. *Id*. at 1257.
97. 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, 1258 (2004).
98. *Tucker,* 305 F.3d at 1198.
99. *Id*.
100. *Id*. at 1199.
101. *Id*.
102. *Id*.
103. *Id*. at 1204.
104. *United States v. Tucker,* 305 F.3d 1193, 1204 (10th Cir. 2002).
105. *Id*.
106. *Id*.
107. *Id*.

approach, the court can find someone guilty of possession simply because he/she had the *ability* to control the images in question.[108]

The manipulation and control that the user exercises over the images in question presents issues because courts suggest that when the individual is just actively looking for images, he/she is intending to manipulate the actual image that shows up on his/her computer screen.[109] An image an individual manipulates is not the same image that appears in the cache, which is simply a copy of the image.[110] Therefore, analyzing the image that is located in the cache is not exemplary of an image that a user might have once copied, enlarged, printed, transferred, or saved.[111] The Present Possession approach does make a distinction between both sets of images, as exemplified in *Tucker*.[112] However, the court did not have a hard time finding that Tucker displayed control over the images in the cache.[113] The court found that knowledge of the second set of images in the cache is enough to demonstrate control over the images.[114]

The next factor in the analysis under the Present Possession Approach is the actions the user took to obtain the images.[115] This factor again provides difficulties with establishing knowing possession.[116] Courts generally analyze whether a user subscribed to a certain pornography website and what specific terms the individual used to search for pornography.[117] If a user has subscribed to a certain website, this shows that the user was aware of the content of the images on there, but this does not prove knowledge of the images in the cache for possession.[118] With this same analysis, search terms can show that a user intended on reaching out for child pornography, but this only applies to the images that come across his/her computer screen and not images found in the cache, which are a copy of those images that once appeared on the screen.[119]

The key to the Present Possession approach is whether the individual knew that the internet cache stores the images.[120] Since this approach focuses exclusively on what is found within the cache, if an individual knows about the images inside of the cache, the court can easily establish a line of reasoning that suggests the user exercised control

---

108. *Id*.
109. Howard, *supra* note 69, at 1260.
110. *Id*.
111. *Id*.
112. *Tucker,* 305 F.3d at 1204.
113. *Id*.
114. *Id*.
115. Howard, *supra* note 69, at 1260.
116. *Id*.
117. *Id*.
118. *Id*.
119. *Id*.
120. *Id*. at 1256.

over these images.[121]

Present Possession in the Courts

The court used the Present Possession approach in *United States v. Romm*, finding that Romm knowingly possessed child pornography found within the internet's cache.[122] Romm accessed child pornography images online and enlarged these images on his screen.[123] Romm said that he would keep images that he liked on his screen for five minutes and then would "delete" them (exit the page).[124] Romm used the words "save" and "download" when he explained this process.[125] Romm argued that he "knowingly" sought out these images, but he only viewed the images, and therefore was not guilty of possession.[126] The Court ruled that Romm showed he had dominion and control over the images when he enlarged them on his screen and "saved" them for five minutes before he "deleted" them.[127] The Court emphasized that since Romm knew images were automatically saved into the cache, this shows that Romm could have copied, printed, or emailed the images to others as exemplary of his degree of control over the images.[128]

Again, like in *Tucker,* the Court did not pay any attention to the fact that even though Romm did have the ability to take these actions, he actually did not go through with any of them.[129] To distinguish possession from mere viewing, the court used an analogy of an individual going to a museum to view the Mona Lisa.[130] When someone walks around a museum, he/she is just looking at paintings. An individual cannot copy, print, or email the Mona Lisa to another person.[131] However, the Court did not mention the fact that in the case at hand, there are two sets of images. One image exists in its original location on the in-

---

121. 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, 1256 (2004).

122. *Romm,* 455 F.3d at 993 (holding that Romm knowingly possessed child pornography based on 40 images that he deleted from his computer's cache, as well as 2 other images that were deleted from another area of his hard drive).

123. *Id*.

124. *Id*. at 995.

125. *Id*. Romm explained that he would search for child pornography on websites and when he found a photograph that he liked, he would "keep [it] on his screen for five minutes and then delete [it]." *Id*.

126. *Id*. at 997.

127. *United States v. Romm,* 455 F.3d 990, 998 (9th Cir. 2006).

128. *Id*. at 1001. The forensic analysis also showed that "Romm has enlarged a few smaller 'thumbnail' images in the internet cache." *Id*. at 995. The forensic examiner also gave an opinion that the files were deleted from the cache either manually or by instruction from Romm to delete the images. *Id*. There was no evidence that showed that Romm actually did anything with the individual images found inside of the cache. *Id*. at 996.

129. *Id*. at 1001; *Tucker,* 305 F.3d at 1204.

130. *Romm,* 455 F.3d at 1001.

131. *Id*.

ternet, while the other image exists in the individual's computer cache. The problem that the Present Possession approach illustrates, here, is that the court interprets the factors under this approach interchangeably with the images found on a user's computer screen and with the images found in the cache.

The court states that Romm "knowingly" sought out the images, viewed them on his computer screen, and then "deleted" them.[132] Romm never saved or deleted the images from his actual computer; the court is merely describing how he opened and exited web pages containing child pornography.[133] However, this analysis applies only to the images that appeared on his screen during that time. The analysis the Court used here cannot apply to the copy of the images found in the cache. The Court did not distinguish this action from the action of a user going into the cache, viewing the images from that location, and then deleting them. Romm did not do this, but the Court said he *could have.*[134] The Court basically said that whatever an individual can do with images that appear on his screen, he can also do it to the images that are saved in the cache, and that is enough to establish possession of such images.[135]

Another decision following the Present Possession approach is *United States v. Kuchinski,* where the defendant, Kuchinski, admitted to knowingly receiving and possessing 110 child pornography images that he actually physically downloaded onto his computer.[136] However, he was also charged for an extra 13,904 to 17,984 images which were found in his cache, which he did not admit to knowingly possessing.[137] These extra images make a substantial impact on the advisory sentencing guidelines range.[138] According to these guidelines, for 110 images, the base level (the starting point that courts use to determine a defendant's sentencing range) for the offense would be 19 (there are a total of 43 levels of offense- the more serious that the crime is, the higher the offense level).[139] However, with the additional images found in the cache, the offense base level would increase to 24.[140] This key difference in the offense levels relates to all of the images found in the cache.[141]

The court found that Kuchinski had no idea of the existence of the cache files and certainly did not know how to access the images within

---

132. *Id*. at 993.

133. *Id*. at 995.

134. *Id*. at 998.

135. *Id*.

136. *Kuchinski* 469, F.3d at 862.

137. *Id*.

138. *Id*.

139. *Id*.; *An Overview of the Federal Sentencing Guidelines.* United States Sentencing Commission. (March 30, 2017) http://www.ussc.gov/sites/default/files/pdf/about/overview/Overview_Federal_Sentencing_Guidelines.pdf.

140. *Kuchinski* 469, F.3d at 862.

141. *Id*.

them.[142] Using the Present Possession approach, the court made it clear that it makes a significant difference whether Kuchinski knew about the cache or not.[143] Since he did not know the cache saved the images, the court found him not guilty, because he did not possess those images.[144] Thus, the court did not take those images into account when calculating his guideline range.[145] This is in direct contrast to *Romm*, where "the defendant knew about the cache files and had actually taken steps to access and delete them."[146] Should the court let Kuchinski off the hook because he did not know about the cache files? That is what the court essentially determined in its holding.[147]

Kuchinski is a 9th Circuit case, just like *Romm*.[148] However, the court reached a different conclusion simply because Kuchinski did not know about the cache files.[149] Even though Romm knew about the cache files, he never actually went into the cache to manipulate the files.[150] The court based its reasoning on the fact that Romm *could have* gone into the cache and *could have* manipulated the files because he *knew* about the existence of the cache.[151] Here in *Kuchinski*, the defendant did not *know* about the existence of the cache.[152] When following the reasoning in *Romm,* Kuchinski *could not* exercise control over the cache, since he did not *know* about it.[153] It did not matter whether Romm took additional action to manipulate the images found in his cache files, it only mattered that he *knew* of their existence.[154] This analysis is troubling because both men sought out child pornography on the internet.[155] Both men also did not access their cache files.[156] However, the court found one of the men guilty of possession of images in the cache file, while the court found the other man not guilty.[157] This is simply because of how knowledgeable each man is of technology.[158]

---

142. *Id*.
143. *Id*.
144. *Id*. at 863.
145. *Id*.
146. *United States v. Kuchinski* 469, F.3d 853, 862 (9th Cir. 2006).
147. *Id*. at 863.
148. *Id*. at 853; *Romm,* 455 F.3d at 990.
149. *Kuchinski* 469, F.3d at 862.
150. *Romm,* 455 F.3d at 998.
151. *Id*. at 1000-1001.
152. *Kuchinski* 469, F.3d at 862.
153. *Romm,* 455 F.3d at 998.
154. *Id*.
155. *Kuchinski* 469, F.3d at 856; *Romm,* 455 F.3d at 993.
156. *Kuchinski* 469, F.3d at 862; *Romm,* 455 F.3d at 996.
157. *Kuchinski* 469, F.3d at 853; *Romm,* 455 F.3d at 990.
158. *Kuchinski* 469, F.3d at 853; *Romm,* 455 F.3d at 990.

EVIDENCE OF APPROACH

The Law

Under the Evidence Of approach, possession begins when an individual searches for an image and ends when the individual leaves the webpage containing the image.[159] The analogy to best describe this approach is one of a video camera- the cache represents a recording of activity that the user has engaged in.[160] Under this approach, the court does not rely too much on the images found inside of the cache, but focuses its analysis on the original images that appeared on the user's computer screen.[161]

When analyzing the factors under the Evidence Of approach, knowledge of the cache is irrelevant because criminal liability stems from the actual images that the individual "originally searched for, selected, and placed on his computer scene."[162] When the court analyzes images found within the cache under this approach, it must connect these images to the original images that appeared on the user's computer screen at some point in time.[163] Under this approach, the internet cache is simply a record of the action the individual took to view these images and does not relate to the possession of the original images.[164] Under the Evidence Of approach, destruction of images in the cache, is also irrelevant because again, criminal liability for the images does not extend to the images stored within the cache, but only to the original images.[165]

However, under the Evidence Of approach, analyzing manipulation and control of images does not have the same issues as explained in the Present Possession approach.[166] With this approach, the court analyzes the original image that a user intended to control with actions such as copying, enlarging, printing, transferring, or saving.[167] The court also analyzes the actions that a user took to obtain certain images.[168] A subscription to a website and definite search terms are solid indications that a user knew and intended to access the images in question.[169] Since the court is analyzing the actual image that the user is seeking out under this approach, knowledge of copies of this image in the cache is ir-

159. Howard, *supra* note 69, at 1255.
160. *Id*.
161. *Id*.
162. *Id*.
163. *Id*.
164. *Id*.
165. 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, 1257 (2004).
166. *Id*. at 1260.
167. *Id*.
168. *Id*.
169. *Id*.

relevant.[170]

Evidence Of in the Courts

United States v. Kain exemplifies the Evidence Of Approach, where the court charged the defendant, Kain, with possession of child pornography images located inside of his computer's cache.[171] Kain stated that the images were located in "user inaccessible space," so he could not exercise dominion and control over them.[172] Using the Evidence Of approach, the court explained that Kain had intentionally sought out the images, and therefore gained control of them.[173] The court compared this to a person who intentionally looks at a magazine containing child pornography.[174] By browsing through the magazine, the individual "knowingly possesses" the images, even if he does not own the magazine

---

170. *Id*.

171. *Kain,* 589 F.3d at 950.

172. *Id*. at 949.

173. *Id*. at 950. Police had a search warrant for Kain's home relating to evidence of marijuana trafficking. *Id*. at 947. The police got another warrant to search his computer, where they allegedly found twenty-seven images of child pornography. *Id*. at 947-948. The district court determined that Kain was guilty of possessing child pornography in a bench trial. *Id*. at 948. In the appellate court, Kain argued that the government did not prove "(i) that he knowingly possessed images of child pornography found on his computer; (ii) that the images depicted actual children under the age of eighteen, and that he knew those facts; and (iii) that twenty-two of the twenty-seven images depicted lascivious exhibition of the genitals, and that Kain knew that any of the images were child pornography." *United States v. Kain,* 589 F.3d 945, 948 (8th Cir. 2009). The standard of review was whether a reasonable fact finder could uphold the verdict, viewing the evidence in favor of the original verdict. *Id*. In proving the knowing possession element, the court said that Kain called in investigator after his computer was received and stated that he wanted to "clean it out." *Id*. Investigators found a folder named "Y," which contained twenty-one images of child pornography (party of the twenty-seven images that he was charged with) on Kain's computer. *Id*. The other six images that he was charged with were found in the computer's "temporary internet" and "orphan" files. *Id*. Temporary internet files contain web pages that a user viewed "so they can be viewed on the computer itself." *Id*. Orphan files, on the other hand, are filed that were saved on the computer at one point, but were later deleted. *United States v. Kain,* 589 F.3d 945, 948 (8th Cir. 2009). These files cannot be traced to their original locations. *Id*. The investigator found Trojan programs and testified that the existence of such programs suggested that the images on Kain's hard drive were "not placed on the hard drive by a Trojan." *Id*. at 949. The investigator also testified that Kain had visited the same child pornography websites more than once. *Id*. The combination of this evidence suggested that Kain knew he was looking at child pornography and that the images saved by his computer were traced to the images he once viewed. *Id*. The court explained that analyzing possession in this way is an issue of fact, not of law. *Id*. Furthermore, an FBI agent testified that Kain admitted to downloading images on his computer. *United States v. Kain,* 589 F.3d 945, 950 (8th Cir. 2009). The agent then told Kain that investigators found a total of four-hundred and five images on his computer. *Id*. Kain replied with, "[i]f they found [four-hundred and five] images, then there were [four-hundred and five] images on the computer." Given the totality of the facts, Kain possessed the child pornography images on his computer. *Id*.

174. *Id*.

or does not purchase it.[175] Under the Evidence Of approach, the court convicted the defendant of possessing child pornography based on images found inside of the cache, even though he did not actually know about the cache.[176]

Another case that used the Evidence Of approach is *United States v. Zarn,* where Zarn, the defendant, said that he searched and viewed child pornography on his computer, but he did not download the images, and he did not know that the computer automatically downloaded the images into the computer's cache.[177] Using the Evidence Of approach, the court ruled that it did not matter whether Zarn knew about the cache.[178] It also did not matter that he did not download the images himself.[179] The court ruled that the actual searching and viewing the images was enough for him to exercise dominion and control over them.[180] The court noted that Zarn used specific search terms in order to acquire the images.[181] Zarn exercised dominion and control over the images by "displaying them, closing the sites, and moving from one to another."[182] The court also mentioned that Zarn had the ability of "printing, saving, or copying them," even though he did not take any of these actions.[183]

WHICH APPROACH IS BETTER?

Zarn illustrates the fact that under the Evidence Of approach, knowledge of the cache is irrelevant.[184] Using the Present Possession approach, the court let Kuchinski off the hook because he did not know about the cache files, but in this case, using the Evidence Of approach, the court did not let Zarn off the hook.[185] The court focused its analysis on the original images that Zarn had searched for on the internet.[186] The court referenced *Romm* in its analysis, reasoning that Zarn exercised dominion and control over the images that he searched for and displayed.[187] The court also mentioned that Zarn had the *ability* to copy, print, or save these images.[188] However, in *Romm,* where the court used the Present Possession approach, the court reasoned that since Romm

175. *Id*. The court explained that by punishing the possession of child pornography, victims of child exploitation can be protected and the market will eventually become obsolete. *Id*. at 947.

176. *United States v. Kain,* 589 F.3d 945, 950 (8th Cir. 2009).

177. *United States v. Zarn,* 365 Fed. Appx. 838 (9th Cir. 2010).

178. *Id*.

179. *Id*.

180. *Id*.

181. *Id*.

182. *Id*.

183. *United States v. Zarn,* 365 Fed. Appx. 838 (9th Cir. 2010).

184. *Id*.

185. *Kuchinski* 469, F.3d at 853; *Zarn,* 365 Fed. Appx. at 838.

186. *Zarn,* 365 Fed. Appx. at 838.

187. *Id*.

188. *Id*.

knew that the cache automatically downloaded the images, he had the ability to manipulate the images.[189] This then led to dominion and control over the images, which subsequently proved knowing possession of the images in the cache.[190] Here, Zarn did not know about the existence of the cache and the court found that this was irrelevant.[191] The court ruled that Zarn still knowingly possessed the images because he had dominion and control over them.[192] Here, the court did not distinguish between the original images that were on the computer screen at one point and the copies of the images inside of the cache. The court only focused on the original images.[193]

In both of these 9th circuit cases, the court determined that the defendant was guilty of possessing the images found inside of the cache.[194] The court used the Present Possession approach in one case and the Evidence Of approach in another case; but it ended up with the same result in both cases.[195] In comparing these two cases under two different approaches, it does not matter whether one of the defendants was knowledgeable about technology.[196] The court found both of them guilty.[197] This analysis shows that courts can use two different approaches to get different results, but can also use different approaches to get the same result.[198] This seems to suggest that if a judge determines that he wants a defendant to be found guilty of possession, he can manipulate the ruling based on which approach he chooses.

Many courts do implicitly follow the Present Possession approach.[199] However, in doing so, some courts provide reasons for decisions that can only make sense under the Evidence Of approach.[200] As explained above, many of the factors that the courts use when making a decision do not properly apply to the Present Possession approach, because the courts do not distinguish between images that are found in the cache and images that were originally present on the computer screen.[201] This inconsistency between analysis and results can be due to the fact that the courts lack knowledge about how technology actually works.[202]

The Evidence Of approach is clearly more favorable to prosecutors, as it provides a greater likelihood that the court will convict a defend-

---

189. *Romm,* 455 F.3d at 998.
190. *Id.*
191. *Zarn,* 365 Fed. Appx. at 838.
192. *Id.*
193. *Id.*
194. *Romm,* 455 F.3d at 993; *Zarn,* 365 Fed. Appx. at 838.
195. *Romm,* 455 F.3d at 990; *Zarn,* 365 Fed. Appx. at 838.
196. *Romm,* 455 F.3d at 990; *Zarn,* 365 Fed. Appx. at 838.
197. *Romm,* 455 F.3d at 990; *Zarn,* 365 Fed. Appx. at 838.
198. *Romm,* 455 F.3d at 990; *Zarn,* 365 Fed. Appx. at 838.
199. Howard, *supra* note 69, at 1264.
200. *Id.*
201. *Id.*
202. *Id.*

ant of knowingly possessing child pornography.[203] The analysis under the Evidence Of approach does not address whether the defendant has knowledge of how his/her computer works.[204] It strictly analyzes the actions that the user takes.[205] Someone who reaches out for child pornography but does not know much about technology should still be penalized equally in comparison to someone who knows about the cache and takes actions to clear child pornography out of his/her cache. The goal of the federal child pornography laws is to protect children and to deter the production of child pornography.[206] Therefore, the Evidence Of approach, as opposed to the Present Possession approach, seems to be the better choice of the two.

In 2007, Congress added the language, "or knowingly access with intent to view" to 18 U.S.C. 2252 A(a)(4)-(5).[207] This language suggests that viewing child pornography is not even necessary in order to find that someone knowingly possesses the images.[208] This language supports the Evidence Of approach, where knowledge of the cache is irrelevant.[209] The language suggests that it does not matter whether someone has the ability to modify images found in the cache. In addition to this, it does not matter whether the individual even knows about the cache. However, it is not clear whether this amendment will help bring uniformity into the courts regarding child pornography laws.

Since Congress has not provided an explicit definition for the language, or any framework, the courts interpret the meaning themselves. Courts have been reluctant to define the actual meaning of possession in the statute, possibly because of the sentencing guidelines that come with a conviction of possession child pornography. The statutory range of imprisonment for an individual who possesses child pornography with a minor that is twelve years or older, is 10 years in prison.[210] For child pornography depicting a minor that is under the age of twelve, the range of imprisonment is 0 to 20 years.[211] With a prior sex conviction, the range is 10 to 20 years.[212] If a judge believes that the sentencing guidelines are too harsh, he may choose the Present Possession approach, where the court can let a defendant off the hook for images lo-

---

203. *Id*. at 1255.

204. *Id*. at 1260.

205. 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, 1255 (2004).

206. *See Kain,* 589 F.3d at 947(quoting Pub. L. No. 104-208, Tit. I, § 121, subsec. 1(12), 110 Stat. 3009-27 (1996).

207. *Enhancing the Effective Prosecution of Child Pornography Act of 2007*, Pub. L. No. 110-358, § 203, 122 Stat. 4001 (2008), *available at* https://www.congress.gov/110/plaws/publ358/PLAW-110publ358.pdf (last visited Nov. 19, 2016).

208. *United States v. Shiver,* 305 Fed. Appx. 640, 642 (11th Cir. 2008).

209. Howard, *supra* note 69, at 1255.

210. 18 U.S.C. §§ 2252A(b)(2).

211. *Id*.

212. *Id*.

cated the cache because he does not know about them.[213] If a judge thinks the sentencing guidelines fit the crime, he may choose the Evidence Of approach, where the court does not need to analyze whether the defendant knew about the cache and can reach a conviction more easily.[214]

For example, Jack B. Weinstein, who has been a federal judge for 43 years, threw out a conviction that would put a man who collected child pornography behind bars for 5 years.[215] Another judge, in Ohio, went against the recommended sentencing guidelines and sentenced a 71-year-old man to home confinement for 3 years instead of jail time.[216] That judge explained that the man did not have a criminal record and was ill, so his sentence could have meant life in prison.[217] Judge Weinstein has suggested that judges should inform juries about the mandatory prison sentence that different charges bring so jurors are aware of the connection between the crime and the punishment, which at some times, may seem disproportional.[218]

Jury instructions are extremely important in child pornography cases, especially when images discovered in the cache are involved.[219]

---

213. Howard, *supra* note 69, at 1256 (explaining that if an individual does not know about the existence of the cache, then he cannot knowingly possess the images inside of it.) The court would have to go into a more in-depth analysis to convict someone of knowingly possessing child pornography under this approach. *Id*. The court may turn to the user's expertise with the computer and may analyze the actions the user took. *Id*. Ultimately though, this approach focuses on what is found within the cache and it is easiest to establish a conviction if there is clear evidence that the user had knowledge of the images within the cache. *Id*.

214. *Id*. at 1260 (explaining that knowledge of images inside of the cache is irrelevant.) Under this approach, the court analyzes actions the user took to obtain the image and analyzes the level of control the user exercised on the images. *Id*. For example, the court looks at whether the user copied, printed, enlarged, saved, or emailed the image. 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, 1260 (2004). Under this approach, the court does not need to analyze whether the user had knowledge of the technology he was using (aka the functions of the cache.) *Id*.

215. A. G. Sulzberger, *Defiant Judge Takes On Child Pornography Law,* THE NEW YORK TIMES (May 21, 2010) http://www.nytimes.com/2010/05/22/nyregion/22judge.html?_r=0.

216. *Judge Battles Child Pornography Mandatory Minimum Sentence He Considers Unjust,* THINKPROGRESS (Sept. 27, 2013) https://thinkprogress.org/judge-battles-child-pornography-mandatory-minimum-sentence-he-considers-unjust-b440b1428b48#.1x1m3zagb.

217. *Id*.; Paul Butler, *Article: When Judges Lie (and When They Should),* 91 Minn. L. Rev. 1785 (2007) (explaining that when a judge is faced with a law that he does not agree with, he can "1) apply the law even though he thinks it is immoral; 2) openly reject the law; 3) resign; or 4) subvert the law by pretending that it supports the outcome the judge desires.")

218. Sulzberger, *supra* note 215.

219. *See Kuchinski* 469, F.3d at 862. In this case, the defendant, Kuchinski admitted to knowingly downloaded 110 child pornography images onto his computer but was also charged with 13,904 to 17,984 images that were found exclusively in his cache. *Id*. The images found inside of the cache would have made a huge impact on the

The average user may not even know of the existence of the cache, so it is important for jurors to be as informed as possible. Jurors can determine the ultimate sentence for someone if the court finds him guilty of possession of child pornography; a guilty verdict can impact sentencing based on whether the individual is charged on one or more counts.[220] A federal judge in Cleveland surveyed jurors, asking them about the appropriate sentence for a man convicted of receiving, possessing, and distributing child pornography.[221] The jury had come up with a more justifiably appropriate sentence of 14 months versus the mandatory minimum, which is 5 years.[222] The prosecutors in the case recommended a sentence of 20 years and the federal sentencing guidelines suggested a sentence of 27 years.[223] This is one example that shows, generally, people think the appropriate punishment for possessing child pornography is much less than the sentences being imposed.[224] If the court informed the jury about the minimum sentences, would they have suggested a longer sentence?

The Supreme Court has stated that child pornography cases, "unless applied with great care, can lead to unreasonable sentences."[225] Some sentences imposed for possessing child pornography end up being longer than sentences imposed for actually sexually abusing a child.[226] A judge in Manhattan recommended that minimum sentences should be included in jury instructions and jurors should have "the option of refusing to convict if the punishment seem[s] disproportionate.[227] In a case where the court found a defendant guilty of possession of 11 counts of child pornography (hard copies), Judge Weinstein actually asked the jury if its members would have convicted the man, had they known

---

sentencing guideline range. *Id*. For the 110 images that Kuchinski was charged for downloading onto his computer, the base level for the offense was 19. *Id*. For the images that were found in his cache, the base level for the offense would have jumped to 24. *Id*.

220. *See Id*. If the jury in this case would have found that the defendant, Kuchinski, knew about the images found inside of his cache, he could have been convicted with a much longer sentence. *United States v. Kuchinski* 469, F.3d 853, 862 (9th Cir. 2006). Kuchinski was charged with downloading 110 child pornography images onto his computer. *Id*. Kuchinski was also charged for an additional 13,904 to 17,984 images that were found exclusively in his cache. *Id*. The court found that Kuchinski did not know about the existence of the cache, so he was found not guilty of possessing those images. *Id*. If the court found that Kuchinski knew about the images in the cache, he could have been charged with a base offense level of 24, versus the base offense level of 19 for the 110 images that he downloaded onto his computer. *Id*.

221. Jacob Sullum, *Judges Find Federal Child Porn Sentences Are Much Longer Than Jurors Consider Just: In one case, the term sought by prosecutors was 17 times longer than the jury recommended,* REASON[DOT]COM: FREE MINDS AND FREE MARKETS (Feb. 23, 2015), http://reason.com/blog/2015/02/23/judges-find-federal-child-porn-sentences.

222. *Id*.

223. *Id*.

224. *Id*.

225. Sulzberger, *supra* note 215.

226. *Id*.

227. *Id*.

about the minimum sentence that comes along with the crime.[228] Five members of the jury stated that they did not think the man should go to prison at all and two of them stated that they would have changed their votes, had they known about the sentencing guidelines.[229] This case involved actual hard copies of child pornography; how would the jury react if it was deliberating on digital images, specifically images automatically saved in the cache?

An issue that arose with the court's reasoning in *Romm* was the fact that the trial court had not given clear instructions to the jury.[230] The court failed to "require the jury to find whether Romm knew images of child pornography were present on his disk."[231] The jury asked for clarification, but the court did not give any further guidance.[232] The court explained that since there was overwhelming evidence of Romm's knowledge, that there was no reason to correct the error in jury instructions.[233] The fact that the trial court made the mistake in relation to the jury instructions raises the question: Why did the court make this error? Was it because it does not understand how technology works or because it wanted to get a sure conviction for Romm?

PROPOSAL

It is clear that the courts have a wide range of discretion when picking which analysis to use in child pornography cases.[234] When dealing with images found inside of a user's internet cache, the court can either decide that knowledge of the cache is relevant (under the Present Possession approach) or irrelevant (under the Evidence Of approach).[235] This can give the court *too* much discretion, as the court can punish the same actions of two men differently, simply because one of them knew

---

228. *Id*.

229. *Id*.

230. *Romm,* 455 F.3d at 1003-1004. The jury instructions were as follows: "Defendant Stuart Romm is charged in Count 2 of the Indictment with Knowing Possession of Child Pornography, in violation of Title 18, United States Code, Section 2252A(a)(5)(B). In order for Defendant Romm to be found guilty of that charge, the Government must prove each of the following elements beyond a reasonable doubt: *First*, That Defendant Stuart Romm knowingly possessed a laptop computer with a hard drive that contained three or more images of child pornography; *Second*, That *the images of child pornography knowingly possessed* by Defendant Stuart Romm, had been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer. A person has possession of something if the person knows of its presence and has physical control of it, or knows of its presence and has the power and intention to control it."[emphasis added] *Id*. Basically, the court told the jury that it only needed to determine that "the images that Romm 'knowingly possessed' had a nexus to interstate commerce" instead of finding that Romm knowingly possessed the actual images. *Id*.

231. *Id*. at 1004.

232. *Id*.

233. *Id*. at 1005.

234. Howard, *supra* note 69, at 1254.

235. *Id*.

more about technology than the other.[236] Courts should use the Evidence Of approach in order to focus more on the defendant's actions, instead of his knowledge of technology. By not focusing on the user's knowledge of images found inside of the cache, the courts can apply uniformity across all child pornography cases.

In addition to the type of analysis the court uses in child pornography cases, another issue that arises with the court's discretion is sentencing guidelines.[237] Many judges disagree with the sentencing guidelines imposed for possession of child pornography and juries are inclined to change their analysis after learning about such guidelines.[238] If a judge does not properly inform a jury about the sentencing guideline range, they could choose to rule one way versus ruling another, had the members been properly informed.[239] Taking these factors into account, it seems as though the courts cannot apply uniformity to child pornography cases unless a jury is informed about which particular analysis the judge is using, as well as the sentencing guidelines that come along with a certain offense.

The sentencing guidelines for possession of child pornography provide different sentences for defendants that have had prior convictions and ones that have had no prior convictions.[240] Under both the Present Possession and Evidence Of approaches, the courts are reluctant to focus on extraneous evidence.[241] However, given the fact that there are different sentencing guidelines for people who have had prior convictions, this may be a good way for courts to use their discretion.[242] Extraneous evidence can show how likely the individual will seek out child pornography again and can show how much of a threat the individual can be to society. Sentencing a 70-year-old man to prison who has no prior convictions and who has looked at 2 images of child pornography one time is not likely to repeat the offense and does not appear to be a danger to society.[243] On the contrary, a younger man who has had previous convictions, has looked at thousands of images of child pornogra-

---

236. *Kuchinski* 469, F.3d at 853; *Zarn,* 365 Fed. Appx. at 838. Kuchinski, the defendant, did not know about the existence of the cache and under the Present Possession approach, he was found not guilty of possession of child pornography images found in the cache. *Kuchinski* 469, F.3d at 863. Zarn, the defendant, also did not know about the existence of the cache, but was found guilty of possession of child pornography images found in the cache under the Evidence Of approach. *Zarn,* 365 Fed. Appx. at 839. Note that these two cases both come from the 9th circuit. *Kuchinski* 469, F.3d at 853; *Zarn,* 365 Fed. Appx. at 838.

237. Sullum, *supra* note 221.

238. Sulzberger, *supra* note 215; Sullum, *supra* note 221.

239. Sulzberger, *supra* note 215.

240. 18 U.S.C. §§ 2252A(b)(2).

241. Howard, *supra* note 69, at 1263. Some examples of extraneous evidence are: witness testimony, past behavior, hard copies of child pornography inside of the individual's home, and stories mentioning child pornography. *Id*.

242. 18 U.S.C. §§ 2252A(b)(2).

243. *Judge Battles Child Pornography Mandatory Minimum Sentence He Considers Unjust, supra* note 216.

phy, and has hard copies of child pornography inside of his home is more likely to repeat the offense and could be a bigger danger to society. By looking at the totality of the circumstances within each case, the court can use its discretion to make that determination. Under such an analysis, the court can look at the internet cache to back up its observations. By focusing more on what actions the individual actually took, the court can spend less time on proving whether the individual knew that his computer's cache recorded his actions.

Therefore, the best way to get rid of the market for child pornography is for the courts to use the discretion they have to analyze a user's actions, regardless of whether the user had knowledge of the cache. There is no reason that a court should let a possessor of child off the hook just because he/she does not know about the existence of a cache. Therefore, the Evidence Of approach would be most appropriate to use. Furthermore, judges must inform the jury about the approach that the court is using, as well as the sentencing guidelines that come with that approach. The Evidence Of approach will allow the courts to distribute child pornography laws more evenly, as juries will not have to debate over whether an individual knew about the existence of the cache, and can focus their analysis instead on what actions the user took.[244] By taking these actions, judges can help change the discrepancy across child pornography cases, can help make child pornography laws more evenly distributed, and can ultimately eliminate the child pornography market.

Conclusion:

In sum, advances in technology have spurred confusion in regards to child pornography laws because even though Congress has produced legislation to address these changes, it has not provided instruction on how to apply the laws.[245] The main source of this confusion is the cache, which automatically records a user's actions when accessing child pornography, without any action taken from the user.[246] Whether the user knows about the cache is a question some courts struggle to answer.[247]

Courts have not been able to distribute federal child pornography laws evenly due to the fact that courts have great discretion in how they analyze whether a defendant possesses child pornography in relation to the cache.[248] The courts can use either the Present Possession approach or the Evidence Of approach.[249] The Present Possession approach analyzes whether a user had knowledge of the cache's operations, whereas the Evidence Of approach does not.[250]

---

244. Howard, *supra* note 69, at 1255 (explaining that under the Evidence Of Approach, knowledge of the cache is irrelevant and criminal liability stems from the action that the internet user originally took with child pornography images).

245. Grantham, *supra* note 16.

246. *Romm,* 455 F.3d at 995.

247. Howard, *supra* note 69, at 1254.

248. *Id*.

249. *Id*.

250. *Id*.

Courts should use their discretion in picking the Evidence Of approach when dealing with child pornography cases, as it will allow the court to focus on the defendant's actions, as opposed to his knowledge of technology.[251] Courts should not give defendants a free pass, just because they are not aware of the functions of technology. In addition to this, courts must fully explain to the jury what method it is using, as well as the guidelines that come along with the method. This will ensure that the jury will make an informed decision when asked if a defendant is guilty of a crime. These actions will help apply uniformity to the distribution of child pornography laws and will start to put an end to the market for child pornography.

251. *Id*. at 1255 (explaining that under the Evidence Of approach, knowledge of the cache is irrelevant).