Fordham Law Review

Volume 81 | Issue 1

Article 5

2012

Crying Over the Cache: Why Technology Has Compromised the Uniform Application of Child Pornography Laws

Katie Gant
Fordham University School of Law

CRYING OVER THE CACHE: WHY TECHNOLOGY HAS COMPROMISED THE UNIFORM APPLICATION OF CHILD PORNOGRAPHY LAWS

*Katie Gant**

As thousands of individuals surf the internet daily, every image on every web page is saved automatically to their computer's cache, absent user direction. Sections 2252(a)(2) and 2252(a)(4)(B) of Title 18 of the U.S. Code criminalize knowing possession and knowing receipt of child pornography images. For the defendant who intentionally saves illicit images to his computer, the cache simply verifies already-proven knowing possession or receipt. However, for the defendant who only views child pornography online, the presence of images in the cache may not be enough to prove knowledge beyond a reasonable doubt. How can the prosecution prove a defendant knowingly received an image he has potentially never seen? How can a prosecutor prove a defendant knowingly possessed an image that may have been a pop-up? Questions like these have split circuit courts over the application of § 2252(a)(2).

Several circuit courts have confronted cases with defendants who undoubtedly viewed child pornography images online, but who only left one clue as to their "knowing" receipt—the presence of images in the cache. The Tenth Circuit found that absent direct proof that a defendant viewed the image, the presence of a file in the cache is not enough to meet the "knowing receipt" standard. The Eleventh and Fifth Circuits disagreed, holding that a pattern of seeking out images satisfies the knowledge requirement. This Note analyzes the split and concludes that the presence of images in the cache proves a defendant's knowing receipt. The Tenth Circuit's demand of "direct proof of viewership of the image in question" imposes impossible evidentiary requirements. Defendants who view child pornography online have satisfied § 2252(a)(2)'s mens rea requirement even without direct proof of viewership of the image in question.

TABLE OF CONTENTS

* J.D. Candidate, 2013, Fordham University School of Law; B.A., 2009, University of Oklahoma. I would like to thank my advisor, Professor Ian Weinstein, for his insight and guidance.

INTRODUCTION

Terry Dobbs was sentenced to eleven years imprisonment after investigators found two images of child pornography in his computer's cache.[1] Milton Pruitt was sentenced to eight years when investigators discovered illicit images of minors in the cache of his computer.[2] David Winkler was sentenced to six years because five child pornography video files resided in his computer's temporary storage.[3]

Child pornography is a highly stigmatized crime that Congress is determined to punish severely.[4] Dobbs, Pruitt, and Winkler were all convicted under 18 U.S.C. § 2252(a)(2),[5] which criminalizes knowing receipt of child pornography.[6] However, Dobbs is not spending the next eleven years of his life behind bars. The Tenth Circuit reversed his conviction after the court found that there was insufficient evidence to prove that Dobbs *knowingly* received the two cached images he was prosecuted for having on his computer.[7] Winkler and Pruitt were not so lucky.[8] All three men were caught searching for prohibited images over the internet, but one walked free. This inconsistent standard for the same conduct is alarming.

Congress' attempt to tailor the law to uniformly prosecute child pornography defendants has been compromised by an entity greater and more influential than Congress itself—internet technology. "As a user browses the internet, the computer stores images . . . in its temporary memory the way a ship passing through the ocean collects barnacles that cling to its hull."[9] While online, *every* image on *every* web page is saved to a user's hard drive in the internet cache.[10] This caching occurs even if the user does not view an image.[11] Thus, the ocean of illegal images available online and the capacity of the cache have changed the face of child pornography prosecutions, clouding statutory mens rea elements and resulting in conflicting decisions in the circuit courts.

[1] *See* United States v. Dobbs, 629 F.3d 1199, 1201–02 (10th Cir. 2011).

[2] *See* United States v. Pruitt, 638 F.3d 763, 765 (11th Cir. 2011).

[3] *See* United States v. Winkler, 639 F.3d 692, 695 (5th Cir. 2011).

[4] *See infra* notes 59–60 and accompanying text.

[5] 18 U.S.C. § 2252(a)(2) (2006).

[6] *Id.*; *Winkler*, 639 F.3d at 695; *Pruitt*, 638 F.3d at 765; *Dobbs*, 629 F.3d at 1201.

[7] *Dobbs*, 629 F.3d at 1209.

[8] The Eleventh Circuit affirmed Pruitt's conviction. *Pruitt*, 638 F.3d at 767. The Fifth Circuit affirmed Winkler's conviction. *Winkler*, 639 F.3d at 701.

[9] *Winkler*, 639 F.3d at 696.

[10] *See* United States v. Kuchinski, 469 F.3d 853, 862 (9th Cir. 2006).

[11] *See id.*

Circuit courts are split on the meaning of knowing receipt[12] and knowing possession[13] when child pornography images are found exclusively in the defendant's internet cache. Can a user knowingly possess an illegal image if he does not know that the image is saved to his computer? Can he knowingly receive an illegal image if he does not know that the cache exists? Can the prosecution prove "knowing[] access[] with intent to view"[14] if there is no way to prove that the user viewed the *specific* images? Different answers to these questions have divided federal circuit courts, and raise an even greater question: what does "knowingly" mean in a technologically advanced day and age?[15]

The 2008 amendments to § 2252 endeavored to give courts a clear idea on what constitutes criminal activity by criminalizing viewership.[16] However, the amendments have not solved the underlying problem: the cache saves almost everything.[17] The government may prove that a defendant has used search terms likely to return illegal results.[18] The government may prove that a pattern of activity indicates that a defendant viewed the images in question.[19] But some courts demand that the government prove that the defendant viewed the *images in question* beyond a reasonable doubt.[20] This statutory interpretation means that criminalizing viewership may ease prosecutions in cases in which there is direct proof, like a download or a browser history,[21] demonstrating that the defendant has viewed the images in question. But it will not ease prosecutions in which the images are found exclusively in the cache and there is no proof linking the cached image to the defendant's line of sight.

Part I of this Note explains the technology of internet caching, then addresses the statutory history of child pornography law and its application in the circuit courts. Part II explores the disagreement between the Tenth

[12] 18 U.S.C. § 2252(a)(2) (2006). *Compare Winkler*, 639 F.3d at 700, *and Pruitt*, 638 F.3d at 767, *with Dobbs*, 629 F.3d at 1201.

[13] 18 U.S.C. § 2252(a)(4)(B) (2006 & Supp. V 2011). *Compare Winkler*, 639 F.3d at 696, *and Pruitt*, 638 F.3d at 766, *with Dobbs*, 629 F.3d at 1201.

[14] 18 U.S.C. § 2252(a)(4)(A).

[15] "Judicial confusion over what exactly constitutes computer-based 'possession' and 'receipt' is evident from a brief perusal of . . . child pornography cases." United States v. Polizzi, 549 F. Supp. 2d 308, 351 (E.D.N.Y. 2008), *vacated and remanded on separate grounds*, United States v. Polouizzi, 564 F.3d 142 (2d Cir. 2009).

[16] *See* 18 U.S.C. § 2252(a)(4)(B).

[17] *See Deleting Web Browser Cookies & Cache*, N.Y.U. INFO. TECH. SERVICES, http://www.nyu.edu/its/faq/cache.html (last visited Sept. 21, 2012); *see also* United States v. Kuchinski, 469 F.3d 853, 862 (9th Cir. 2006).

[18] *See Dobbs*, 629 F.3d at 1211.

[19] *See id.* at 1204.

[20] 18 U.S.C. § 2252. The statute criminalizes knowing possession and receipt of "any visual depiction." *Id.*

[21] An example of such a browser history would be a URL that takes the user directly to *one* image. This occurs if the user has searched for images before, found one he liked, and then memorized the URL. This allows him to type the URL directly into his browser for repeat viewing. However, a browser history with a URL that takes the user to a website with multiple images might not be effective in proving that a defendant has viewed the image. The image could be at the bottom or side of the page, could be too small to view, or could have occurred due to a pop-up.

Circuit and the Fifth and Eleventh Circuits regarding the level of evidence required to prove a defendant knowingly received images found exclusively in his computer's cache. Finally, Part III of this Note argues that uniform application of the law can only be achieved by allowing the use of circumstantial evidence to demonstrate knowledge when prosecuting child pornography defendants.

I. Setting the Stage for the Split: The Cache, the Law, and How Circuit Courts Reconcile the Two

The intersection between the law and technology is a game of catch-up for Congress. Therefore, when possession and receipt of child pornography over the internet became a commonplace crime, Congress had to respond in order to criminalize the conduct it aimed to prevent. This part first introduces the technology of internet caching. Next, it provides an overview of the federal law criminalizing possession and receipt of child pornography. Finally, this part summarizes the four most influential circuit court cases concerning cached child pornography images.

A. What's the Cache?

A cache is a storage device in a computer's main memory meant to improve download speed.[22] When a computer user views a website online, the web browser automatically saves copies of the images on that page to the computer's internet cache.[23] The cached files improve browser performance by allowing the browser to quickly redisplay the same images if the user returns to the page.[24] Images located in the cache are called temporary internet files.[25] For the purposes of this Note, it is helpful to remember that the cache is a place on the computer, while temporary internet files are items, like images, located in the cache.

Normally an image is not copied into the cache without the user accessing a web site on which the image is contained.[26] However, unusual circumstances such as the "occurrence of a pop-up or the existence of malicious software" can copy an image into the cache absent user access.[27]

[22] *See Cache*, MERRIAM WEBSTER'S COLLEGIATE DICTIONARY 170 (11th ed. 2003); *see also Cache*, WEBOPEDIA COMPUTER DICTIONARY, http://www.webopedia.com/TERM/C/cache.html (last visited Sept. 21, 2012).

[23] *See* United States v. Kennedy, 643 F.3d 1251, 1253 n.2 (9th Cir. 2011).

[24] *See id.* (citing United States v. Romm, 455 F.3d 990, 993 nn.1, 3 (9th Cir. 2006)). The 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." United States v. Stulock, 308 F.3d 922, 925 (8th Cir. 2002).

[25] *See Temporary Internet File*, WEBOPEDIA COMPUTER DICTIONARY, http://www.webopedia.com/TERM/T/temporary_Internet_file.html (last visited Sept. 21, 2012).

[26] United States v. Dobbs, 629 F.3d 1199, 1210 (10th Cir. 2011).

[27] *Id.*

Files in a cache can be deleted in three ways.[28] First, on the default setting, the web browser automatically empties the cache when it reaches a given size.[29] Second, the user can instruct the browser to empty the cache.[30] Third, sophisticated users can go into the cache and manually delete the temporary internet files, "rather than effect the deletions automatically through the web browser's default setting."[31] Deleted cache files remain in the computer's unallocated space[32] until other material overwrites them.[33] While in this unallocated space, they may be recovered using specialized software.[34]

After seizing a computer, the government often employs computer forensic experts who use specialized software[35] to recover images that have not yet been overwritten by other material.[36] The images may be found in the cache, recycle bin, or other unallocated space in the computer.[37] The forensic experts are able to specify the number of images, their location on the hard drive, the content of the images, and the time of their arrival.[38]

B. What's the Law?

This section explores the federal statutes criminalizing knowing receipt and possession of child pornography. It traces the evolution of federal child pornography statutes and looks at 18 U.S.C. § 2252(a)(2), (a)(4)(B) to see how they stand today. Then, it analyzes the most recent amendment to the law, which now criminalizes knowing access of child pornography "with intent to view." Finally, it distinguishes knowing possession and knowing

[28] The ability to delete files in the cache demonstrates that those files are accessible. *See id.* But they are system protected, which blocks any user from accessing the cache except by means of system commands. *See id.* A user may execute a system command to open the cache notwithstanding a computer's warning. *See id.* From there, the user may manipulate the contents of the cache. *See id.*

[29] United States v. Romm, 455 F.3d 990, 995 (9th Cir. 2006).

[30] *See id.*

[31] *Id.*

[32] "Unallocated space is space on a hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software. Such space is available to be written over to store new information. Even if retrieved, all that can be known about a file in unallocated space (in addition to its contents) is that it once existed on the computer's hard drive." United States v. Flyer, 633 F.3d 911, 918 (9th Cir. 2011).

[33] *See id.* at 918.

[34] *See id.*

[35] Examples include EnCase and Snagit, which recovered 2,039 images of child pornography from a defendant's computer in *United States v. Bass*. *See* 411 F.3d 1198, 1200 (10th Cir. 2005). "With EnCase, it is possible to recover deleted files, as well as information showing when the files were created, accessed, or modified." *Romm*, 455 F.3d at 995.

[36] *See, e.g.*, *Bass*, 411 F.3d at 1200; United States v. Tucker, 305 F.3d 1193, 1197–98 (10th Cir. 2002).

[37] *See Tucker*, 305 F.3d at 1197–98 ("[A computer forensic detective] recovered files containing child pornography from different parts of the hard drive. Some were located in the Web browsers' cache files. Others were located in the computer's recycle bin and in 'unallocated' hard drive space.").

[38] *See* United States v. Dobbs, 629 F.3d 1199, 1202 (10th Cir. 2011).

receipt—two separate crimes that courts oftentimes confuse due to the conceptually challenging technology of the cache.

1. History and Development of Child Pornography Laws

Congress first criminalized child pornography with the Protection of Children Against Sexual Exploitation Act[39] (PCA) in 1978.[40] The PCA forbade transactions involving child pornography that had moved in interstate commerce or was produced using interstate materials.[41] Congress passed the Act pursuant to its findings that "child pornography and prostitution had become highly organized, multi-million-dollar industries" that exploited thousands of children in the production of pornography.[42]

By 1982, the U.S. Supreme Court recognized what Congress had already noted: that the "exploitive use of children in the production of pornography has become a serious national problem."[43] To combat the developing industry, the Court found in *New York v. Ferber* that child pornography was not entitled to First Amendment protection.[44] The Court also found that "[t]he most expeditious if not the only practical method of law enforcement may be to dry up the market for this material by imposing severe criminal penalties on persons . . . promoting the product."[45]

In light of the decision in *Ferber* and the continued growth of the child pornography industry,[46] Congress passed the Child Protection Act of 1984[47] (CPA). Originally, to be prosecuted under the CPA, a defendant must have produced child pornography for sale, and such material must have violated *Miller v. California*'s[48] obscenity test.[49] But in the amended CPA, Congress eliminated both the production for sale requirement—as much of the activity associated with child pornography was not for profit[50]—and the obscenity test under *Miller*.[51]

[39] 18 U.S.C. § 2251 (2006).

[40] Lori J. Parker, Annotation, *Validity, Construction, and Application of Federal Enactments Proscribing Obscenity and Child Pornography or Access Thereto on the Internet*, 7 A.L.R. FED. 2D 1, 30 (2005).

[41] *Id.*

[42] New York v. Ferber, 458 U.S. 747, 749 n.1 (1982) (citing S. REP. NO. 95-438, at 5 (1977)).

[43] *Id.* at 749.

[44] *Id.* at 774.

[45] *Id.* at 760.

[46] *See* Debra D. Burke, *The Criminalization of Virtual Child Pornography: A Constitutional Question*, 34 HARV. J. ON LEGIS. 439, 450 (1997).

[47] Child Protection Act of 1984, Pub. L. No. 98-292, 98 Stat. 204.

[48] 413 U.S. 15 (1973).

[49] *See* Burke, *supra* note 44, at 450; *see also Miller*, 413 U.S. at 36–37. The test finds that the basic guidelines for the trier of fact must be:

> (a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest . . . (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Id. at 24.

[50] *See* Burke, *supra* note 44, at 450.

With the advent of internet technology, child pornography became a new monster: "The ability to rapidly communicate with large numbers of people and the perception of anonymity in cyberspace . . . made the internet a popular venue for both seekers and providers of obscenity and child pornography."[52] This spawned federal and state legislation directly aimed at preventing and punishing child pornography transmission, receipt, and possession over the internet.[53]

The first such law was the Child Protection and Obscenity Enforcement Act of 1988,[54] an amended version of the 1977 PCA.[55] The act made it unlawful to use a computer to transport, distribute, or receive child pornography.[56]

Then, the 1996 passage of the Child Pornography Protection Act[57] (CPPA) criminalized child pornography involving real children, virtual children, and adults portrayed as children in the images.[58] This represented a change in Congressional direction, defining the crime not in terms of "harm inflicted upon the child, but rather as an evil in and of itself."[59] With the CPPA, "Congress further expanded the statutory prohibitions against child pornography."[60] But in *Ashcroft v. Free Speech Coalition*,[61] the Supreme Court held that some of the definitions of child pornography in the CPPA were overbroad and impermissibly criminalized virtual child pornography.[62] The law after *Ashcroft* stood until the 2008 amendments. It was illegal to knowingly possess or knowingly receive child pornography images over the internet, but the law no longer criminalized possession or receipt of virtual child pornography.

2. Statutory Provisions

In line with Congress's view that child pornography is an evil in and of itself,[63] § 2252(a)(4)(B) criminalizes knowing possession of child pornography.[64] Section 2252(a)(4)(B) has several important requirements.

[51] *See Miller*, 413 U.S. at 24.

[52] Parker, *supra* note 38, at 1.

[53] *See id.*

[54] Pub. L. No. 100-690, 102 Stat. 4486 (1988) (codified as amended at 18 U.S.C. § 2251 (2006)).

[55] *See* Deborah F. Buckman, Annotation, *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).

[56] *Id.*

[57] 18 U.S.C. §§ 2252A, 2256(8)(B).

[58] *Id.*

[59] *See* Burke, *supra* note 44, at 452.

[60] *See* Buckman, *supra* note 55, at 544.

[61] 535 U.S. 234 (2002).

[62] *See* Parker, *supra* note 38, at 31.

[63] *See supra* note 59 and accompanying text.

[64] 18 U.S.C. § 2252(a)(4)(B) (2006 & Supp. V 2011) (providing in relevant part: "(a) Any person who . . . (4) either . . . (B) knowingly 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 in interstate or foreign commerce, or which was produced using materials which have been

First, it requires a mens rea of "knowingly."[65] Second, the "visual depiction" can be in any form.[66] Third, the depiction must have passed through interstate commerce.[67] Last, the depiction must be of a minor engaged in "sexually explicit conduct."[68]

Section 2252(a)(2) criminalizes knowing receipt or distribution of child pornography.[69] Section 2252(a)(2) contains similar requirements to § 2252(4)(B), demonstrating the interrelatedness of the two crimes.[70]

The Supreme Court addressed the application of scienter required by the term "knowingly" as used in the PCA.[71] The Court found that knowingly applied to the elements of the crime concerning minor performers and the sexually explicit nature of the material, despite the more natural grammatical reading of the PCA under which the scienter element would apply only to transport.[72] By including a broadly applicable scienter requirement despite the most natural grammatical reading,[73] the Court demonstrated a willingness to err on the side of overcriminalization in the highly controversial crime of child pornography.

The trend towards more criminalization is also demonstrated by the choice of the word "knowingly" to define the level of mens rea for the crime. Under the statutory provisions, possession and receipt do not require intent or willfulness, but rather the lesser standard of knowledge.[74] In *United States v. Polizzi*,[75] the Eastern District of New York struggled with this level of scienter, finding that "the provisions may be void for vagueness and overbreadth because they appear to potentially criminalize innocent conduct."[76] The court noted that when analyzing cases in which images are

mailed to so shipped or transported, by any means including by computer, if—(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct; shall be punished as provided in subsection (b) of this section.").

[65] *See id.*

[66] *See id.*

[67] *See id.*

[68] *See id.*

[69] 18 U.S.C. § 2252(a)(2) (2006) (providing in relevant part: "(a) Any person who . . . knowingly receives, or distributes, any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by a computer, or knowingly reproduces any visual depiction for distribution in interstate or foreign commerce through the mails, if—(A) the producing of such visual depictions involves the use of a minor engaged in sexually explicit conduct; and such visual depiction is of such conduct; . . . shall be punished as provided in subsection (b) of this section.").

[70] *See id.*; *see also infra* Part I.B.4 (discussing the subtle difference between knowing possession and knowing receipt).

[71] *See* United States v. X-Citement Video, Inc., 513 U.S. 64, 78 (1994).

[72] *Id.*; *see also* 18 U.S.C. § 2252(a)(1)–(2).

[73] *Id.* at 70.

[74] *See* 18 U.S.C. § 2252(a)(2), (a)(4)(B) (2006); *see also* United States v. Irving, 452 F.3d 110, 122 (2d Cir. 2006) ("[T]he government [is] only required to prove that [the defendant] knowingly—not willfully—received or possessed the images.").

[75] 549 F. Supp. 2d 308, 342 (E.D.N.Y. 2008), *vacated and remanded on separate grounds*, United States v. Polouizzi, 564 F.3d 142 (2d Cir. 2009).

[76] *Id*. This was because knowledge of the nature of the images may be acquired purposefully or accidentally and the statute did not account for this distinction. "A person

found exclusively in the cache, courts have "conflated knowledge with intent" or "implied an intent requirement where none exists in the words of the statute" in order to affirm guilty convictions.[77] This issue speaks to the heart of the conflict splitting the Tenth Circuit from the Fifth and Eleventh, and will be discussed in Part II of this Note.

3. The 2008 Amendments

In 2006, the Ninth Circuit noted that "to commit the crime" of possession "one has to do something more than look: he must ship, produce, or at least knowingly possess. . . . There is nothing . . . that criminalizes looking."[78] This standard changed in 2008 when Congress amended § 2252(4)(B) to include "knowing[] access[] with intent to view."[79] Now, a defendant may be guilty of a felony if he visits an internet website containing child pornography images intending to view the images found therein.[80] There is no element of possession or receipt required.[81] Rather, viewing even a single image of child pornography will suffice.[82] However, the defendant must know that the images are child pornography, as required by *United States v. X-Citement Video, Inc.*,[83] and must knowingly—not accidentally or purposefully—access the website.[84] By the terms of the statute, the defendant does not even have to view the images, but rather, simply has to intend to view the illegal images through knowing access.[85]

The 2008 amendments also incorporate an affirmative defense for knowing possession or "knowing[] access[] with intent to view" in § 2252(c).[86] This addition was designed to allow a defendant who accidentally possesses or views three or less images to escape conviction if

has not done anything 'morally wrong,' or had 'an evil intent,' . . . simply because he passively received and possessed depictions of child pornography he did not seek. Yet there is no requirement of moral culpability in the statute." *Id.* at 349 (quoting *X-Citement Video*, 513 U.S. at 73 n.3); *see also infra* Part III.A.2.

[77] *Polizzi*, 549 F. Supp. 2d at 354. For example, in *United States v. Tucker*, 305 F.3d 1193, 1205 (10th Cir. 2002), the "appellate court also emphasized that the defendant had *intentionally* sought out and viewed child pornography *knowing that the images would be saved on his computer, even if only temporarily*." *Polizzi*, 549 F. Supp. 2d at 356.

[78] United States v. Gourde, 440 F.3d 1065, 1079–81 (9th Cir. 2006) (Kleinfeld, J., dissenting).

[79] 18 U.S.C. § 2252(a)(4)(A) (2006 & Supp. V 2011).

[80] Note that the affirmative defense is not a defense to the receipt of child pornography defined by 18 U.S.C. § 2252(a)(2). *See Polizzi*, 549 F. Supp. 2d at 348.

[81] *See id.*

[82] *See id.*

[83] 513 U.S. 64, 78 (1994).

[84] 18 U.S.C. § 2252(a)(4)(A).

[85] *See id.*

[86] 18 U.S.C. § 2252(c) (providing in relevant part: "It shall be an affirmative defense to a charge of violating paragraph (4) of subsection (a) that the defendant—(1) possessed less than three matters containing any visual depiction proscribed by that paragraph; and (2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any visual depiction or copy thereof—(A) took reasonable steps to destroy each such visual depiction; or (B) reported the matter to a law enforcement agency and afforded that agency access to each such visual depiction.").

he takes the affirmative steps required under the statute.[87] Congress intended to provide some means of "separating levels of culpability,"[88] after recognizing that "the imprecision of § 2252's language and its potential mismatch with the activities that Congress actually meant to criminalize."[89]

4. Possession versus Receipt: What's the difference?

Separating possession and receipt is the first key to uniform prosecutions; however, doing so is easier said than done. This problem was illustrated in *United States v. Myers*,[90] where Myers argued that the distinction between receipt and possession of child pornography is meaningless because anyone in possession of child pornography must have received it at some point in time.[91] The defendant in *United States v. Kuchinski*[92] made the same argument.[93]

In *Polizzi*, the Eastern District of New York grappled with the "conceptually challenging" definition of receipt and possession in the computer context.[94] The court explained: "Once a computer receives an illicit image . . . the computer user possesses 'matter' containing child pornography, even before viewing the electronic screen."[95] Thus, it appears at first glance that the crimes subsume one another, as possession could not have occurred but for receipt. However, when a defendant "intentionally or unintentionally sees the child pornography pictures, the user 'knowingly possesses' them—even if the images were unsolicited, unwanted, or a complete surprise."[96] This makes the possession charge "purely passive."[97] Such is not the case with knowing receipt. Receipt implies affirmative action by the defendant. In order to knowingly receive an image, a defendant must have sought it out and known that the image he is receiving is of child pornography.[98] The same is not true of possession. A viewer

[87] Note that the affirmative defense is not a defense to the receipt of child pornography defined by 18 U.S.C. § 2252(a)(2). *See Polizzi*, 549 F. Supp. 2d at 348.

[88] *See* Note, *Child Pornography, the Internet, and the Challenge of Updating Statutory Terms*, 122 HARV. L. REV. 2206, 2219 (2009) (finding that "the defense alone is probably insufficient to achieve the intended level of filtering.").

[89] *Id.*

[90] 355 F.3d 1040 (7th Cir. 2004).

[91] *Id.* at 1042.

[92] 469 F.3d 853 (9th Cir. 2006).

[93] *See id.* at 859. Kuchinski claimed that once he pled guilty to possession of child pornography, "he could not be tried for receipt of child pornography" because possession was a lesser included offense in receipt. *Id.*

[94] *Polizzi*, 549 F. Supp. 2d at 342 ("[D]efining Internet-facilitated computer 'possession' and 'receipt' as all-encompassing boundaries of criminality becomes conceptually challenging since the forbidden objects are bits of data in electromagnetic form that can be transferred instantaneously and automatically by wire or wirelessly, and stored automatically in a multitude of places and in various electronic forms.").

[95] *Id.* at 347.

[96] *Id.*

[97] *Id.*

[98] *See* United States v. X-Citement Video, Inc., 513 U.S. 64, 78 (1994). It is important to note that the court in *Polizzi* disagreed, finding that "receipt and possession may constitute the same act." *See Polizzi*, 549 F. Supp. 2d at 357. The court reached this conclusion

who solicits "only adult pornography, but without his knowledge is sent a mix of adult and child pornography" is not guilty of receipt, as he did not *knowingly* receive the image.[99] However, the same defendant may be guilty of knowing possession if he decides to retain the illegal material.[100] Thus, in the more complicated computer context, the distinction between the crimes could be meaningless but for the requirement of knowledge.

In *United States v. Romm*,[101] the Ninth Circuit found that because "Romm knowingly possessed the files in the internet cache, it followe[d] that he also knowingly received them."[102] The court reached this result because of its analysis of Romm's possession charge.[103] However, as explained above, there are situations in which a defendant may knowingly possess without having knowingly received images.[104] The *Romm* court concluded that possession naturally leads to receipt without analyzing Romm's affirmative action of receipt.[105] By contrast, Congress has identified its intent to punish receipt more severely than possession,[106] which suggests that it is important for courts to analyze the crimes separately.

Another helpful way to differentiate the two crimes is through the amount of evidence required to prove each. As stated in *United States v.*

because it found that knowing receipt can be passive as well. *See id.* at 348. For example, when a person is emailed an illegal image and his computer automatically opens his email, he receives the image without taking any action. *Id.* For the purposes of this Note, this example is distinguishable. First, it would be difficult for a court to find that receipt "knowing," as the email automatically opened the image without any action by the defendant. Second, the circuits split on the issue of knowing receipt and possession for images found exclusively in the cache does not focus on images automatically displayed on a user's computer screen through email.

[99] United States v. Myers, 355 F.3d 1040, 1042 (7th Cir. 2004).

[100] *Id.*

[101] 455 F.3d 990 (9th Cir. 2006).

[102] *Id.* at 1001.

[103] In *United States v. Mohrbacher*, 182 F.3d 1041, 1048 (9th Cir. 1999), the Ninth Circuit found that downloading child pornography constitutes both the act of possession and receipt. *See Romm*, 455 F.3d at 1001. Because the *Romm* court found that the cache files were analogous to downloading, taking possession of the files in the cache also constituted the "knowing receipt" of those files. *Romm*, 455 F.3d at 1000–01.

[104] *See supra* notes 99–100 and accompanying text.

[105] Romm admitted that he had gone online and used a search engine to find images that pleased him. *See Romm*, 455 F.3d at 995. He displayed these images on his screen for five minutes before deleting them from his cache. *Id.* This affirmative action of seeking out the image demonstrated "knowing receipt" under the Ninth Circuit's analysis in this case. *See id.* at 1001.

[106] "The 'PROTECT Act of 2003' amended Section 2252A to impose a prison sentence of 'not less than 5 years' for violations of Section 2252A(a)(2), which previously carried no statutory minimum." United States v. Miller, 527 F.3d 54, 59 n.4 (3d Cir. 2008) (citing H.R. REP. No. 108-66, at 50–51 (2003) (Conf. Rep.), *reprinted in* 2003 U.S.C.C.A.N. 683, 685). "Congress established a series of distinctly separate offenses respecting child pornography, with higher sentences for offenses involving conduct more likely to be, or more directly, harmful to minors than the mere possession offense." United States v. Grosenheider, 200 F.3d 321, 332–33 (5th Cir. 2000). "It is certainly not irrational to punish more severely the person who knowingly receives such material, because it is that person who is creating and/or perpetuating the market for such material." *Myers*, 355 F.3d at 1042.

Miller,[107] "the quantum of evidence required to prove knowing receipt of a downloaded file" may "be greater than that minimally required to prove knowing possession of the file."[108] When an image is found only in the cache, proving knowing possession only requires that the defendant knew that the image was in his possession—whether or not it got there through defendant's voluntary or accidental action.[109] However, when analyzing receipt of the same image, the prosecution must prove that the defendant knowingly and affirmatively acted, resulting in the image's presence in the cache.[110] The difference between passivity and activity necessarily requires more evidence. And, the fact that a defendant is guilty of possession if convicted under receipt, but a defendant guilty of possession may not be guilty of receipt, points to a higher evidentiary standard for proof of guilt under receipt.

C. Applying the Law: The Development of Internet Child Pornography Prosecutions in the 2000s

The following four cases[111] paved the way for possession and receipt analysis when child pornography images are found exclusively in the cache. Decided between 2002 and 2006 by the Ninth and Tenth Circuits,[112] they illustrate three approaches that circuit courts employ to determine a defendant's guilt in the complex circumstance of computer possession and receipt.

1. 2002: *United States v. Tucker*

After an anonymous tip informed law enforcement that Jeffrey Tucker[113] was viewing child pornography on his computer, the police searched his home.[114] Upon entering the house, an officer noticed that Tucker's computer was connected to the internet and that he "had been visiting a newsgroup labeled 'alt.sex.preteen.'"[115] Further forensic investigation of the computer revealed that many files had recently been deleted from

[107] 527 F.3d 54 (3d Cir. 2008).

[108] *Id.* at 64.

[109] *See supra* notes 96–97 and accompanying text.

[110] *See supra* note 98 and accompanying text.

[111] *See* United States v. Kuchinski, 469 F.3d 853 (9th Cir. 2006); *Romm*, 455 F.3d 990; United States v. Bass, 411 F.3d 1198 (10th Cir. 2005); United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002).

[112] Other circuit courts have analyzed the issue as well. *See e.g.*, *Miller*, 527 F.3d 54; United States v. Wilder, 526 F.3d 1 (1st Cir. 2008); United States v. Stulock, 308 F.3d 922 (8th Cir. 2002). However, the following four cases demonstrate a progression in the analysis. They are also the cases most cited by the Tenth, Fifth, and Eleventh Circuits in the split analyzed in this Note. *See infra* Part II.

[113] Tucker had been "convicted in 1990 in Utah state court for sexually abusing a child." *Tucker*, 305 F.3d at 1195. He was paroled in 1996, and as part of his agreement, he agreed to permit searches of his residence without a warrant to ensure his compliance with his parole. *See id.* at 1195–96. He also agreed not to view child pornography. *See id.* at 1196.

[114] *Id.*

[115] *See id.*

Tucker's hard drive.[116] The web browser history showed that Tucker had visited other newsgroups likely to contain child pornography.[117] Around 27,000 images were found on Tucker's computer—some of which were located in the cache.[118] The forensic evidence suggested that Tucker had knowledge of the cache, had accessed it, and had then manually deleted temporary internet files by dragging the images to the computer's recycle bin.[119] During interrogation, Tucker told investigators that his computer contained over 5,000 images of child pornography.[120]

Tucker was convicted of one count of possession of child pornography.[121] In his appeal, Tucker contended that he never possessed images of child pornography, rather he "merely viewed it on his Web browser."[122] Then, to prevent possession, he deleted the images from the cache after viewing.[123] Finally, he argued that he did not affirmatively save or download the images, so he lacked control over the images.[124]

In analyzing Tucker's claims, the Tenth Circuit looked to the ordinary, everyday meaning of possession as "the holding or having something . . . as one's own, or in one's control."[125] The court found that Tucker demonstrated voluntary possession by continuing to view child pornography when he knew that the images were "being saved, if only temporarily, on his computer."[126] Because Tucker had control over the images stored in his cache, as demonstrated by his manual deletions, Tucker possessed the images in question.[127] Thus, the court determined that "each time [Tucker] intentionally sought out and viewed" images of child pornography over the internet, he "knowingly acquired and possessed the images."[128]

2. 2005: *United States v. Bass*

The Tenth Circuit tackled the issue of possession of internet images again in *United States v. Bass*,[129] coming to the same result through a similar analysis. Through an ongoing investigation, police learned that Brian Bass "was a member of an e-group entitled Candyman."[130] Based on this membership, police came to Bass's home and interviewed Bass, who

[116] *See id.*
[117] *See id.* at 1197.
[118] *See id.*
[119] *See id.* at 1198.
[120] *See id.* at 1197.
[121] *See* United States v. Tucker, 150 F. Supp. 2d 1263, 1269–70 (D. Utah 2001).
[122] *See Tucker*, 305 F.3d at 1204.
[123] *See id.*
[124] *See id.*
[125] *Id.* (citing OXFORD ENGLISH DICTIONARY (2d ed. 1989)).
[126] *Id.* at 1205.
[127] *Id.*
[128] *Id.*
[129] 411 F.3d 1198 (10th Cir. 2005).
[130] *Id.* at 1198. The FBI investigation of this Candyman group, coined "Operation Candyman," resulted in many child pornography prosecutions. *See* United States v. Fantauzzi, 260 F. Supp. 2d 561, 562–63 (E.D.N.Y. 2003).

admitted to viewing child pornography.[131] After seizing his computer, police recovered more than 2,000 images of child pornography from Bass's cache.[132] They also recovered a file referencing how to remove information from a computer, as well as software entitled "Window Washer" and "History Kill."[133] In interviews, Bass admitted that he was intentionally viewing child pornography and that he used Window Washer and History Kill to remove the images from his computer.[134]

Bass was convicted of five counts of knowing possession of child pornography.[135] In his appeal to the Tenth Circuit, Bass argued that there was insufficient evidence to support the convictions because did not *knowingly* possess the images.[136] He claimed he was ignorant of the fact that the images were automatically stored on his computer, thus differentiating *United States v. Tucker*[137] from his own case.[138]

The Tenth Circuit found that a jury could reasonably infer that Bass knew the images were automatically saved from the fact that he used file-removing software to wipe images form his hard drive.[139] Finding the case similar to *Tucker* despite Bass's claims to the contrary,[140] the circuit court affirmed Bass's conviction.[141]

However, Judge Paul J. Kelly found this reasoning unpersuasive, writing in his dissent that "[t]he court's decision effectively rewrites the statute to criminalize viewing child pornography via computer."[142] Although Bass intentionally sought out and viewed child pornography "[t]he issue is . . . whether he *knowingly possessed* child pornography."[143] Judge Kelly contended that there was no evidence that Bass intentionally downloaded child pornography, saved any images, attached photographs to an email, knew his computer automatically saved images viewed on the internet, or that he reaccessed cached images.[144] To support a conviction of possession, "something more than viewing must be proven, and the

[131] *See Bass*, 411 F.3d at 1200.

[132] *See id.*

[133] *See id.*

[134] *See id.* at 1201.

[135] *See id.* at 1200.

[136] *See id.* at 1201–02.

[137] 150 F. Supp. 2d 1263 (D. Utah 2001).

[138] *See Bass*, 411 F.3d at 1201–02.

[139] *Id.* at 1202.

[140] The court defined possession as it had in *Tucker*, but did not analyze Bass's dominion and control of the images found in his cache. *See id.* at 1202. Rather, it stated that because Bass knew the images were being automatically saved to his computer in the cache, he was guilty of possession just as Tucker, aware of the automatic caching function of his computer, was guilty of possession. *See id.*

[141] *See id.* at 1206.

[142] *Id.* at 1206 (Kelly, J., dissenting).

[143] *Id.*

[144] "[T]he record is devoid of any evidence showing Mr. Bass re-accessed any of the images in his computer, or that he knew how to do so. The most that can be said is that he exercised general control over all the files in his computer by relying on software to clean up the hard drive. This cannot be equated with manually retrieving files and deleting them" as the defendant in *Tucker* did. *Id.* at 1207.

something more is 'knowingly holding the power and ability to exercise dominion and control.'"[145] In a heated conclusion, Judge Kelly noted that "the court's leap from viewing child pornography to knowingly possessing it based solely on a computer default operation, without any proof the defendant knew about such operation, establishes a precedent that mere negligence suffices for criminal liability, and casts the net of criminality far wider than Congress provided."[146]

3. 2006: *United States v. Romm*

Unlike Tucker and Bass, Stuart Romm was convicted of both possession and receipt.[147] Despite this distinction however, the Ninth Circuit demonstrated a similar analysis to that of the Tenth Circuit in *Tucker*.[148] A forensic examination of Romm's computer after his arrest revealed that all the child pornography on the computer had been deleted, mostly from the cache.[149] A forensic detective opined at trial that Romm had purposefully deleted the images from the cache, either by commanding his browser to do so or by manually deleting the temporary internet files.[150] During the course of the investigation, Romm told agents that he knew they were going to find illegal content on his computer, described how he used Google to search for child pornography websites, and admitted to viewing images on his screen for five minutes before deleting them from his cache.[151]

The court first analyzed possession, finding that receipt of the images turned upon whether Romm possessed them.[152] To establish possession, the court found 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.'"[153] Looking to the Tenth Circuit's *Tucker* analysis for guidance, the Ninth Circuit went further than its sister circuit and found that, to possess images in the cache, the defendant must not only exercise control over the images but also "know that the unlawful images are stored on a disk."[154] Because Romm admitted that he repeatedly sought child pornography, exercised control over the images in his cache when he deleted the folder's contents, and conceded knowledge that the images were saved to his cache (a disk), the court held

[145] *Id.* (quoting United States v. Simpson, 94 F.3d 1373, 1380 (10th Cir. 1996)). Judge Kelly reasoned that the government had to prove dominion and control *and* subjective knowledge to find Bass guilty of possession. *Id.* at 1207–08.

[146] *Id.* at 1208.

[147] *See* United States v. Romm, 455 F.3d 990, 993 (9th Cir. 2006).

[148] *See id.* at 999–1000.

[149] *Id.* at 995.

[150] *Id.*

[151] *Id.*

[152] *See id.* at 998.

[153] *Id.* at 999 (quoting United States v. Carrasco, 257 F.3d 1045, 1049 (9th Cir. 2001)).

[154] *Id.* at 1000.

that there was "sufficient evidence for the jury to find that Romm committed the act of knowing possession."[155]

In reviewing receipt, the Ninth Circuit turned to its decision in *United States v. Mohrbacher*,[156] which held that downloading child pornography constitutes both possession and receipt.[157] The court found caching analogous to downloading.[158] Therefore, because Romm possessed the images in the cache, it necessarily followed that he received them.[159]

4. 2006: *United States v. Kuchinski*

Although reaching a different result than in *Romm*, the Ninth Circuit in *Kuchinski* used the same reasoning[160] to find that the images found in John Kuchinski's cache should not be considered when determining his offense level for sentencing guideline purposes.[161] After executing a search warrant, the FBI discovered "between 15,120 and 19,000 separate images of child pornography" on Kuchinski's computer.[162] Of those, between 15,010 and 18,890 were recovered from the cache.[163] The district court found him guilty of both possession and receipt.[164]

The Ninth Circuit found that "there was no evidence that Kuchinski was sophisticated, that he tried to get access to the cache files, or that he even knew of the existence of the cache files."[165] The court's determination that the thousands of images should not be used in determining Kuchinski's sentence turned on his knowledge of his computer's caching function, and therefore, his lack of control over the images found there.[166] The court noted:

> Where a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with the possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images. To do so turns abysmal ignorance into

[155] *Id.* at 1001. Interestingly, the Ninth Circuit also based its finding on the fact that Romm could "copy the images, print them or email them to others." *Id.* Although Romm did not in fact exercise that type of control over the images, the court found possession because he had the ability to do so. *Id.*; *see also infra* Part III.A.1.a.

[156] 182 F.3d 1041 (9th Cir. 1999).

[157] *See Romm*, 455 F.3d at 1002.

[158] *Id.*

[159] *Id.*

[160] The Ninth Circuit noted that it had "made it plain" in *Romm* "that a person does knowingly receive and possess child pornography images when he seeks them out over the internet and then downloads them to his computer." United States v. Kuchinski, 469 F.3d 853, 861 (9th Cir. 2006).

[161] *Id.* at 863.

[162] *Id.* at 856.

[163] *See id.*

[164] *See id.* at 855–56.

[165] *Id.* at 862.

[166] *See id.*

> knowledge and a less than valetudinarian grasp into dominion and control.[167]

D. Three Approaches to Possession

As demonstrated by the previous four cases, courts employ various analyses when determining whether a defendant has possessed images found exclusively in their cache. The following section will categorize these three approaches in order to provide a clear understanding of the factors circuit courts consider and the inferences they make in deciding to affirm or reverse a defendant's conviction.

1. "Sought the Images + Knowledge" Inference Approach

One method of analyzing whether a defendant has possessed images found exclusively in the cache is the "sought the images + knowledge" inference approach, which was employed by the Tenth Circuit in *Tucker*.[168] It is an inference approach because it requires a few logical deductions: By seeking out the images, the defendant initiated a process on his computer whereby the images were automatically saved.[169] Because the defendant knew about the automatic saving function, he had the requisite "knowledge" required to be found guilty of knowing possession.

Upon first examination the court's reasoning might appear to be a "control and knowledge" approach.[170] However, the *Tucker* court detailed several events in the facts that had little do with control, including the illicit images on the screen when investigators came knocking on Tucker's door, his web browser history, and his admissions during interviews that he had viewed illegal images.[171]

This interpretation could be analogized to drug possession. X decides he wants to purchase drugs. He calls Y, his dealer, and picks up the drugs from Y's house. X does not want to get arrested for possession of drugs and believes the police cannot arrest him if the drugs are not on his person. So X uses a small quantity, then throws the drugs away in the dumpster behind his house.

Tucker sought out child pornography because he wanted to look at the illegal images just as X intentionally sought out drugs from Y. But, because he did not want to get caught, Tucker went into his cache and manually deleted images just as X threw away the drugs he no longer

[167] *Id.* at 863.

[168] *See supra* notes 126–28 and accompanying text.

[169] *See supra* note 126 and accompanying text.

[170] This is because the court defines possession as "the holding or having something (material or immaterial) as one's own, or in one's control," and reasons that "Tucker had control over images stored in his cache and thus possessed them." United States v. Tucker, 305 F.3d 1193, 1204–05 (10th Cir. 2002). Therefore, while the analysis has hints of "control," it is best to categorize it separately, as the Tenth Circuit held that because the defendant "intentionally sought out and viewed child pornography knowing that the images would be saved on his computer," he knowingly acquired and possessed the images in violation of former 18 U.S.C. § 2252A(a)(5)(B). *Id.* at 1205.

[171] *See id.* at 1196–97.

needed. X sought out the drugs and knew that he would be guilty if they were found on his person; thus, he was guilty of possession. Tucker sought out the images and knew that they were being saved; thus, he was guilty of possession.[172]

2. "Remove the Images to Infer Knowledge" Approach

Another approach to knowing possession was demonstrated in *Bass*. It is similar to *Tucker*, however, it differs from the Tenth Circuit's earlier analysis because it requires another inference. Because Bass used software to remove illicit images from his computer, the Tenth Circuit inferred that he knew about his computer's automatic caching function: because he knew about the automatic caching function, he knew the images were saved.[173] Therefore, he possessed the images just as the defendant in *Tucker* possessed the images.[174]

This approach could be analogized to possession of hard-copy child pornography images. X wishes to view child pornography. He goes to Y and borrows several images of child pornography. On his way home, he does not want to get caught possessing child pornography, so he purchases a paper shredder. He brings the shredder home and proceeds to shred the images. When the police discover that he borrowed the images from Y, they search X's house and find the image remnants and the shredder. Under *Bass*'s standard, the remnants coupled with the shredder demonstrate X's possession. Although X attempted to get rid of the images, the shredder manifested his guilt because it showed that he had knowledge of the illegality of his conduct and was attempting to rid himself of liability through use of the shredder.

Bass wished to view child pornography.[175] He went to a web site and looked at several child pornography images.[176] Fearful that his mom would find the images, he bought History Kill software and deleted the images.[177] But, because of the police's sophisticated computer analysis techniques, they were able to recover illegal images and the History Kill software from his computer.[178] The court reasoned that because knowledge of the cache is sufficient for a conviction,[179] it could infer Bass's knowledge of the cache from his software purchase.[180]

[172] *See id.* at 1205.

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

[174] The Tenth Circuit considers knowledge sufficient for possession. *See supra* Part I.D.1. In *Tucker*, the court came to this conclusion because Tucker sought out the images knowing that they would be saved. *See supra* notes 126–28 and accompanying text. In *Bass*, the court presupposed that knowledge was sufficient for possession, instead using an inference to get from the manner of deletion to possession. *See supra* notes 126–28.

[175] *See Bass*, 411 F.3d at 1200–01.

[176] *See id.*

[177] *See id.*

[178] *See id.*

[179] *Id.* at 1201–02.

[180] *Id.* at 1202.

3. "Knowledge and Control" Approach

This is the approach of the Ninth Circuit, as demonstrated in *Romm* and *Kuchinski*. The Ninth Circuit uniformly applied the approach in both cases, but came to a different result because of the factual differences in the two cases.[181] Under this approach, knowledge gives way to control, which in turn gives way to possession. If a defendant knows that the images are in his cache, he can control them.[182] If he can control them, he possesses them.[183] Thus, in *Romm*, because the defendant knew about his cache, he had an ability to control the images; therefore, he possessed them.[184] Although the court found that Romm exercised actual control over some of the images,[185] the ability to control is all that is needed.[186] In *Kuchinski*, because the defendant did not know about his cache, he could not control the images and therefore did not possess them.[187]

II. THE SPLIT: WHY THE TENTH CIRCUIT REACHED A DIFFERENT KNOWING RECEIPT RESULT THAN THE ELEVENTH AND FIFTH CIRCUITS

This part sets forth the circuit split regarding the proper interpretation of knowing receipt. Specifically, the courts disagree over whether circumstantial evidence that a defendant was actively seeking out child pornography can prove knowing receipt of images found only in the cache, absent the defendant's knowledge of the cache. In 2011, the Tenth Circuit reversed a receipt conviction in *United States v. Dobbs*,[188] while the Eleventh Circuit in *United States v. Pruitt*[189] and the Fifth Circuit in *United States v. Winkler*[190] affirmed such convictions. Presented with factually similar cases, the circuit courts reached different results based on their interpretation of "knowingly" in the challenging context of computers.

A. Knowing Receipt Requires Proof of Knowledge of the Images in Question: United States v. Dobbs

In April 2006, U.S. Postal Inspectors seized Terry Brian Dobbs's computer, pursuant to a search warrant issued in a fraud investigation.[191] Upon preliminary examination, agents discovered child pornography on Dobbs's computer, leading to a second search warrant and a more thorough investigation of the computer.[192] Computer forensic specialists found over

[181] *Compare* United States v. Kuchinski, 469 F.3d 853, 862–63 (9th Cir. 2006), *with* United States v. Romm, 455 F.3d 990, 1001 (9th Cir. 2006).

[182] *See Kuchinski*, 469 F.3d at 863; *Romm*, 455 F.3d at 998.

[183] *See Kuchinski*, 469 F.3d at 863; *Romm*, 455 F.3d at 998.

[184] *Romm*, 455 F.3d at 1001.

[185] He enlarged several thumbnail images for better viewing. *See id.* at 1001.

[186] *Id.* at 1001.

[187] *Kuchinski*, 469 F.3d at 862–63.

[188] 629 F.3d 1199, 1200–01 (10th Cir. 2011).

[189] 638 F.3d 763, 767 (11th Cir. 2011).

[190] 639 F.3d 692, 701 (5th Cir. 2011).

[191] *See Dobbs*, 629 F.3d at 1201.

[192] *See id.*

150 images of child pornography in Dobbs's cache.[193] Dobbs was indicted for receipt, attempted receipt, and possession of child pornography in violation of § 2252(a)(2) and § 2252(a)(4)(B).[194]

During trial, the government's forensic specialist, Jonathon Bridbord,[195] testified as to several findings that he made during his investigation of Dobbs's computer.[196] First, Dobbs typed multiple search terms reflecting the pursuit of child pornography into his internet browser.[197] Second, after entering the search terms, Dobbs continued on to additional pages to recover more results.[198] This page advancement occurred up to thirty-six times during each search session.[199] This evidence led Bridbord to testify that the computer activity suggested someone who was "methodically seeking out child pornography."[200]

However, Bridbord also testified that the specific images at issue were found exclusively in the cache.[201] Therefore, there was no evidence that Dobbs actually viewed those images.[202] There was also no evidence that he clicked on the images, manipulated them, or exercised any control over them.[203] And, there was no evidence that Dobbs accessed his cache or even knew that it existed.[204]

During trial, the Northern District of Oklahoma initially admitted seventeen images, but "[t]hat number was winnowed down to two when the government failed to provide adequate evidence that fifteen of the images had traveled in interstate commerce."[205] The two remaining images, captured on March 15, 2006, at 9:29 p.m. and 9:31 p.m., "were banner images comprised of multiple smaller images."[206]

The government's strategy at trial was to create a "time line of activity . . . establishing a pattern indicative of the hunt for child pornography."[207] Bridbord testified that the arrival of questionable images on Dobbs's computer was immediately preceded by searches using terms likely to return illegal child pornography.[208] However, this pattern existed for

[193] *See id.*

[194] *See id.*

[195] Bridbord was an employee of the U.S. Department of Justice's Child Exploitation and Obscenity Section. *See id.* at 1210 (Briscoe, C.J., dissenting).

[196] *Id.*

[197] *See id.* at 1201 n.2. Examples included "very young sex," "erotic preteen," "youngest porn," "pedo pics," and "preteen Lolita."

[198] *See id.* at 1201.

[199] *Id.*

[200] *Id.*

[201] *See id.*

[202] *See id.* at 1202.

[203] *See id.*

[204] *See id.*

[205] *See id.* As 18 U.S.C. § 2252(a)(2) reads, "[a]ny person who . . . knowingly receives . . . any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported." 18 U.S.C. § 2252(a)(2) (2006).

[206] *Dobbs*, 629 F.3d at 1202.

[207] *Id.*

[208] *See id.*

images outside of the two images charged.[209] For the two charged images, there was no "temporally proximate search indicating the pursuit of child pornography."[210] Dobbs was found guilty of knowingly receiving and attempting to receive child pornography.[211] The district court "sentenced him to 132 months imprisonment and nine years of supervised release."[212]

1. The Tenth Circuit's Analysis

On appeal, Dobbs argued that there was "insufficient evidence to prove that his receipt of child pornography was 'knowing.'"[213] As an example, he pointed to the lack of evidence regarding his knowledge of the cache.[214] He argued that "'a man who doesn't know he has certain images inside his computer [cannot] be said to have knowingly accepted those images . . . [or] to have knowingly exercised control over them.'"[215]

On appeal, the government again pointed to Dobbs's "'pattern of methodically seeking out child pornography.'"[216] They tendered that this pattern, coupled with Dobbs' ability to control the images in the cache, was sufficient to prove that he knowingly received child pornography.[217]

a. Knowing Receipt

The Tenth Circuit was guided by the ordinary meaning of "receives" as the court in *Tucker* was guided by the ordinary meaning of "possesses."[218] The Tenth Circuit accepted the district court's definition of receive as "to accept an object and to have the ability to control it."[219] It also accepted the district court's definition of knowingly[220] as "an act was done, or visual depictions were received, voluntarily and intentionally, and not because of mistake or accident."[221]

The Tenth Circuit first reasoned that "[t]here is little doubt that Mr. Dobbs—or at least his computer—'received' child pornography."[222]

[209] *Id.*

[210] *Id.*

[211] *Id.*

[212] *Id.*

[213] *Id.* at 1202.

[214] *See id.*

[215] *Id.* (quoting Reply Brief of Petitioner-Appellant at 5, *Dobbs*, 629 F.3d 1199 (10th Cir. 2011) (No. 09-5025)).

[216] *See id.* at 1203 (quoting Brief of Respondent-Appellee at 15–16, *Dobbs*, 629 F.3d 1199 (10th Cir. 2011) (No. 09-5025)).

[217] *See* Brief of Respondent-Appellee at 15–16, *Dobbs*, 629 F.3d 1199 (10th Cir. 2011) (No. 09-5025).

[218] *See id.* at 1203; *see also* United States v. Tucker, 305 F.3d 1193, 1204 (10th Cir. 2002).

[219] *See Dobbs*, 629 F.3d at 1203.

[220] At the beginning of its analysis, the Tenth Circuit noted that after Dobbs was charged, the statute had been amended to criminalize "knowing[] access[] with intent to view," but explained that it had to review Dobbs's conviction under the law at the time of the charged offense. *Id.* at 1203 n.5.

[221] *Id.* at 1204.

[222] *Id.*

However, the question before the court was if Dobbs received the "*the two images that were sent to the jury*" with the requisite knowledge required by the statute.[223] Pointing to the lack of evidence surrounding the two images at issue, the court emphasized again that there was no evidence presented to the jury that Dobbs ever saw the two images, exercised control over them, or "even knew about his computer's automatic caching function."[224]

The court discounted the government's methodical pattern of seeking out child pornography strategy. In its brief, the government noted that the temporary internet files found in Dobbs's cache provided "circumstantial evidence" that he received images of child pornography by downloading the websites on which the images appeared.[225] The court found this pattern and the contention of circumstantial evidence inapplicable to the two images at hand.[226] The pattern of "search-and-creation" was based upon evidence related to the fifteen excluded images and was therefore irrelevant to the question of Dobbs's knowing receipt of the two charged images.[227]

The Tenth Circuit also discounted the government's argument that the presence of child pornography images in Dobbs's cache provided circumstantial evidence of knowing receipt.[228] "The mere presence of the files in the cache is certainly proof that the files were *received*," but in order to prove knowing receipt, "the government needed to present proof that Mr. Dobbs at least knew of the automatic-caching process."[229]

The Tenth Circuit distinguished its decision in *Bass*, in which it affirmed Bass's guilt despite his claimed lack of knowledge of the cache:[230] "In contrast to *Bass*, the government presented absolutely no evidence here from which a reasonable jury could infer that Mr. Dobbs knew of his computer's automatic-caching function . . . ."[231] Citing *Kuchinski*,[232] the court reasoned that if circumstantial evidence were enough to stand for a conviction under knowing receipt, the court would transform unsubstantiated knowledge into knowledge itself.[233]

The government's argument—that *Bass* was about *possession* of child pornography, thus creating different proof requirements than the case at

[223] *Id.*

[224] *Id.*

[225] Brief for Appellee at 16, *Dobbs*, 629 F.3d 1199 (10th Cir. 2011) (No. 09-5025).

[226] *Dobbs*, 629 F.3d at 1204.

[227] *See id.*

[228] *See id.* at 1205.

[229] *Id.*

[230] *See id*; *see also* United States v. Bass, 411 F.3d 1198, 1202 (10th Cir. 2005); *supra* Part I.C.2.

[231] *Dobbs*, 629 F.3d at 1205.

[232] The Tenth Circuit summarized the facts and court findings in *Kuchinski*, a case where many more images were found in the defendant's cache, to support its holding. *See id.* at 1205 n.7. The court noted that *Kuchinski* relied heavily on the Ninth Circuit's decision in *Romm*, which in turn relied upon that court's holding in *Tucker*—that the defendant's knowledge of the cache and the control over the images found there are the standard for determining a defendant's guilt. *See id.*

[233] *See id.* at 1206.

bar[234]—was unsuccessful. The government argued that in a pure receipt case, "'evidence that the defendant intentionally sought out child pornography establishes that his receipt was knowing.'"[235] The court found otherwise. According to the court, the government "posit[ed] that defendants need not know that they actually have received child pornography . . . to be convicted of *knowing* receipt of child pornography, so long as they intentionally were seeking it out."[236] The court found this contention "logically untenable and unpersuasive on its face."[237]

The government also argued that it did not need to establish Dobbs's actual control over the images, but merely his ability to control the images.[238] However, the court quickly dismissed this contention.[239] In order to have the ability to control an image, the defendant must know that the image exists.[240] Otherwise, the "defendant's conduct with respect to the images could not be deemed to be *knowing*."[241] Thus, because the government had not proven that Dobbs knew about the cache, they had not proven that Dobbs had the ability to control the images.[242] The court concluded that "the lack of a search-and-creation pattern as it relates to the two images before the jury, when combined with the absence of any evidence establishing that Mr. Dobbs ever saw the images, forfends any view that *knowing* receipt could have been found by a rational jury."[243]

b. Attempted Receipt

Dobbs was also charged with attempted receipt.[244] Once again, the Tenth Circuit found the government's arguments unavailing.[245] The government contended that the lack of direct evidence that Dobbs viewed the two images was not fatal to the attempt charge because "there was 'substantial evidence establishing Dobbs's intent to receive.'"[246] The court found that in order for Dobbs to be guilty attempted receipt, he needed to have intended to carry out the knowing receipt of child pornography and

[234] The government argued that possession has a more stringent standard than receipt. *See id.* at 1206 n.8. The Tenth Circuit noted that this was "open to serious question," citing United States v. Davenport, 519 F.3d 940, 943 (9th Cir. 2008), and United States v. Miller, 527 F.3d 54, 71 (3d Cir. 2008), for the proposition that possession is a lesser included offense of receipt. *Dobbs*, 629 F.3d at 1206 n.8.

[235] *Dobbs*, 629 F.3d at 1206 (quoting Brief for Appellee at 29, *Dobbs*, 629 F.3d 1199 (10th Cir. 2011) (No. 09-5025)).

[236] *Id.*

[237] *Id.*

[238] *Id.* at 1207 (referencing United States v. Romm, 455 F.3d 990 (9th Cir. 2006), where the Ninth Circuit found that Romm's ability to control the images was sufficient to prove knowing receipt).

[239] *Id.*

[240] *See id.*

[241] *Id.*

[242] *See id.*

[243] *Id.*

[244] *Id.*

[245] *Id.* at 1208.

[246] *Id.* (quoting Brief for Appellee at 32, *Dobbs*, 629 F.3d 1199 (10th Cir. 2011) (No. 09-5025)).

have taken a substantial step toward the commission of the crime.[247] Emphasizing again the government's lack of proof for the two images charged,[248] the court could not find the intent or substantial step[249] necessary to find Dobbs guilty.[250] Instead, finding that the government provided insufficient proof to establish the knowledge required for conviction under § 2252(a)(2), the Tenth Circuit reversed the Northern District of Oklahoma with instructions to vacate the conviction and sentence.[251]

2. Chief Judge Briscoe's Dissent

Chief Judge Mary Briscoe dissented from the majority's holding, finding that the "evidence presented by the government at trial was sufficient to allow the jury to find that Dobbs knowingly received or attempted to receive the two images at issue."[252]

a. Analysis

Reemphasizing the standard of review,[253] Chief Judge Briscoe dove into her findings by summarizing Jonathon Bridbord's description of caching on a Windows computer like Dobbs's.[254] Due to the nature of the cache, Chief Judge Briscoe posited that "absent the presence of unusual circumstances, such as the occurrence of a pop-up or the existence of malicious software, an image cannot be simultaneously displayed on the computer monitor and copied into the cache without the user accessing a web site on which the image is contained."[255]

At trial, Bridbord testified that Dobbs first used his computer on November 15, 2005.[256] Dobbs began conducting Google searches for child pornography on December 15, 2005.[257] Dobbs continued to conduct searches for child pornography in late December 2005,[258] February 2006,[259]

[247] *Id.* (citing Tenth Circuit decisions that upheld the circuit's attempt standard).

[248] "As noted, the pattern of child-pornography-related searches immediately preceding the creation of illegal images in the cache does not apply to the two images submitted to the jury." *Id.* at 1207.

[249] "In some instances, '[d]efining conduct which constitutes a 'substantial step' toward commission of the crime has proven a thorny task.' However, on this record, it is not." *Id.* at 1208 (quoting United States v. Savaiano, 843 F.2d 1280, 1296 (10th Cir. 1988)).

[250] *Id.* at 1209.

[251] *Id.*

[252] *Id.* (Briscoe, C.J., dissenting).

[253] "'In reviewing sufficiency challenges, we ask whether, *viewing the evidence in the light most favorable to the government as the prevailing party*, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" *Id.* (quoting United States v. Hutchinson, 573 F.3d 1011, 1033 (10th Cir. 2009)).

[254] *Id.* at 1210–11.

[255] *Id.* at 1210.

[256] *Id.* at 1211.

[257] On that date, Dobbs used search terms associated with websites known to contain images of child pornography. *See id.*

[258] During that time period, Dobbs used the search phrase "very young sex." *Id.*

early to mid-March 2006,[260] and early April 2006.[261] Bridbord also pinpointed the websites Dobbs visited from December 2005 to April 2006.[262] But the visits to the pinpointed sites were not always associated with "Dobbs' Google searches for child pornography images."[263] This demonstrates that on some occasions, Dobbs directly visited potential child pornography websites "without first employing a search engine or any child pornography-related search terms."[264]

Bridbord could not identify the websites from which the charged images were derived because that data was either never written onto the hard drive or was overwritten by other data.[265] But Bridbord found that immediately following the creation of the two charged images Dobbs visited four websites associated with child pornography.[266] As a result, eight additional images of child pornography were copied into the cache of Dobbs's computer.[267] Bridbord ruled out the possibility that the two images at issue arrived in the cache of Dobbs's computer by way of a pop-up or malicious software.[268]

From Bridbord's testimony and evidence, Chief Judge Briscoe believed that the jury had enough evidence to conclude that Dobbs knowingly received child pornography.[269] Citing *Romm* for the proposition that a person can receive child pornography by seeking it, but not downloading it,[270] Briscoe contended that Dobbs's methodical use of Google searches coupled with the images found in Dobbs's cache were enough to prove knowing receipt.[271]

b. Why Dobbs's Arguments Fail

Chief Judge Briscoe addressed Dobbs's two arguments on appeal. She found that Dobbs "correctly note[d] that the government offered no direct proof that either of the two images actually appeared on his computer

[259] During that time period, Dobbs used the search terms "Lolita top," and "lolita new." *Id.*

[260] During that time period, Dobbs used the search terms "pedo," "erotic preteen," "pretty teen sex," "top preteen models," "lolita models," and "pedo pics." *Id.*

[261] During that time period, Dobbs used the search terms "pedo sex," "preteen models," "preteen lolita," "preteen newsgroups," "lola," "nymphet," and "nymphet pics." *Id.*

[262] *Id.*

[263] *Id.*

[264] *Id.*

[265] *Id.* at 1212.

[266] *See id.*

[267] *See id.*

[268] *See id.* Dobbs conceded on appeal that he received the child pornography. He admitted that at various times he used his web browser to search for images of child pornography, that he visited websites known to contain child pornography, that his visits to child pornography websites were followed closely by his Google searches of child pornography, and that images depicting child pornography were discovered on his computer. *Id.* at 1212 n.4.

[269] *Id.* at 1212.

[270] *See* United States v. Romm, 455 F.3d 990, 998 (9th Cir. 2006).

[271] *See Dobbs*, 629 F.3d at 1212.

monitor."[272] However, Chief Judge Briscoe was unconvinced "that such direct proof, which would be nearly impossible for the government to muster given the obviously secretive nature of the charged crime and the limitations of computer forensic science," was necessary in order to support a conviction for receipt.[273]

Dobbs's second argument contended that the government offered no evidence that he knew about his computer's cache or the caching process.[274] Again, Briscoe found this assertion to be true.[275] But she was not convinced that "such proof was required in order for the jury to convict Dobbs of knowing receipt of the images."[276] Chief Judge Briscoe pointed out that the government proved that Dobbs intended to seek out and view images of child pornography.[277] Bridbord proved that this "afforded Dobbs temporary dominion and control over the images."[278] Since the Ninth Circuit found that Romm "exercised control over the cached images while they were contemporaneously saved to his cache and displayed on his screen" because he had the ability to control them,[279] it followed that Dobbs also received the images displayed on his computer screen when he sought the images, resulting in their display on his screen.[280] Therefore, Chief Judge Briscoe determined that whether Dobbs was aware of the caching process was immaterial, as "the existence of copies of the images in the cache of his computer was, like fingerprints left at the scene of a crime, merely evidence of his actual criminal activity."[281]

c. Flaws in the Majority's Reasoning

Chief Judge Briscoe found several flaws in the majority's reasoning. First, the majority purported that the government's case exclusively relied on the search-and-creation pattern.[282] Judge Briscoe noted that Bridbord's evidence established that fact, but also that "Dobbs frequently visited child pornography web sites directly, i.e., without any preceding searches."[283] Thus, the absence of evidence of Google searches before Dobbs's receipt of the two charged images was not "fatal to the government's case," because the totality of evidence presented would have allowed a reasonable jury to determine that Dobbs directly visited websites to obtain the two images of child pornography at issue.[284]

[272] *Id.* at 1213.
[273] *Id.*
[274] *Id.*
[275] *See id.*
[276] *Id.*
[277] Dobbs admitted this fact. *Id.* at 1212 n.4.
[278] *See id.*
[279] United States v. Romm, 455 F.3d 990, 1000 (9th Cir. 2006).
[280] *See Dobbs*, 629 F.3d at 1213.
[281] *Id.*
[282] *See id.* at 1204 (majority opinion).
[283] *See id.* at 1214 (Briscoe, C.J., dissenting).
[284] *Id.*

Second, although the majority found that the search-and-creation pattern was extraneous to the question of receipt,[285] Judge Briscoe found the evidence highly relevant, as it proved "both absence of mistake and knowledge."[286] It was the "pattern of methodical activity that would have allowed a jury to reasonably infer" that Dobbs looked at every image on the websites he visited in his search of child pornography.[287]

The majority also found that the presence of images in Dobbs's cache taken alone did not demonstrate his knowledge of receipt.[288] Although Chief Judge Briscoe did not assert that this evidence alone was enough to affirm Dobbs's conviction, she found such evidence relevant to the receipt question.[289]

Chief Judge Briscoe took particular issue with the majority's requirement that Dobbs have knowledge of the cache. Judge Briscoe found that the focus on Dobbs's internet activity was to find and view images of child pornography, not to create copies of those images in his cache.[290] The copies of the images in the cache were merely proof of Dobbs's intentional pattern of activity.[291] Thus, "Dobbs's awareness of the cache or the automatic-caching process was unnecessary to his conviction."[292] Further, this awareness was also unnecessary to establish that Dobbs had the ability to control the images displayed on his screen.[293]

In closing,[294] Chief Judge Briscoe stated that "it was entirely permissible for the jury to infer that Dobbs directly visited, with the intent of finding and viewing images of child pornography, web sites containing the two images at issue."[295]

B. Circumstantial Evidence Is Sufficient to Prove Knowing Receipt

In the following two cases, the Eleventh and Fifth Circuits took a different approach than the Tenth Circuit in *Dobbs*. In short, concise opinions, the circuit courts affirmed Milton Pruitt and David Winkler's guilt for the same conduct that Terry Dobbs walked free for.

[285] *Id.* at 1204. (majority opinion).

[286] *Id.* at 1214. (Briscoe, C.J., dissenting).

[287] *Id.*

[288] *Id.* at 1215.

[289] For example, "this evidence would have supported a finding that the two images at issue arrived in the cache as a result of intentional activity" as opposed to "forces beyond his control and unbeknownst to him." *Id.* at 1215.

[290] *Id.*

[291] *Id.*

[292] *Id.*

[293] This is because Bridbord explained at trial that the images displayed on Dobbs's screen could have been manipulated. *See id.*

[294] Chief Judge Briscoe also analyzed the attempted receipt charge and found that a "substantial step" was taken toward the commission of receipt due to the plethora of evidence presented by Bridbord at trial. *See id.*

[295] *Id.*

1. The Eleventh Circuit: *United States v. Pruitt*

Milton Scott Pruitt utilized his position as a deputy sheriff in Forsyth County to view and access child pornography images.[296] By remotely accessing child pornography images stored electronically on the County's network server, Pruitt was able to view illicit images without directly downloading them to his personal computer.[297] The images remained on the County's server.[298]

His actions were discovered when a technology network manager for the County "noticed an unusual amount of internet activity on the County's network."[299] The manager was able to trace the activity to the person who had accessed the images through his account—Pruitt.[300] When confronted, Pruitt "admitted to opening and viewing the images."[301] Pruitt then gave a Georgia Bureau of Investigation special agent permission to search his home computer.[302] The special agent found approximately seventy images of child pornography in the cache of Pruitt's home computer.[303] The agent also determined that Pruitt had, on several different days, employed child pornography-related search terms and visited child pornography web sites.[304]

A jury convicted Pruitt on two counts of receipt.[305] The first was for receipt on his work computer, the second for receipt on his home computer.[306] He was also charged with knowing possession on his home computer, but the jury acquitted him on this count.[307]

Pruitt's argument on appeal was "that the evidence was insufficient to prove that he 'knowingly receive[d]' child pornography on his work and home computers."[308] The Eleventh Circuit found that Pruitt "seemingly took no affirmative steps to save images onto his computers' hard drives."[309] For example, when Pruitt accessed images at his office or at

[296] *See* United States v. Pruitt, 638 F.3d 763, 764 (11th Cir. 2011) (noting that the "[d]efendant had no work-related purpose for accessing the images").

[297] *See id.*

[298] *See id.* The County had child pornography images because they had a computer crimes unit in charge of investigating child pornography cases. *See id.*

[299] *See id.* at 764–65.

[300] *Id.* at 765.

[301] *Id.*

[302] *Id.*

[303] Over 200 additional images were found in Pruitt's unallocated space. *Id*. Unallocated space contains data emptied from the computer's hard drive. *Id*. at 765 n.2 (citing *United States v. Flyer*, 633 F.3d 911, 918 (9th Cir. 2011)). Unallocated space data is often overwritten to store new information. *Id.* Thus, all that could be known of the 200 images found in Pruitt's unallocated space is that they once existed on his hard drive. *Id*. Most likely, they existed in his cache. *Id.*

[304] *See id.* at 765. The special agent was able to trace the searches to the "HP Administrator" account. *Id.* The evidence presented at trial demonstrated that this was Pruitt's account. *See id.*

[305] *See id.*; *see also* 18 U.S.C. § 2252(a)(2)(A) (2006).

[306] *See Pruitt*, 638 F.3d at 765.

[307] *See id.*; *see also* 18 U.S.C. § 2252A(a)(4)(B).

[308] *See Pruitt*, 638 F.3d at 765.

[309] *Id.* at 766.

home, he did not actively save the images to the computer's hard drive, as demonstrated by the fact that the images were found solely in his cache and unallocated space.[310]

Concluding that the "ordinary meaning" of "receive" was to "knowingly accept" or "to take possession or delivery of,"[311] the Eleventh Circuit held that a person knowingly receives child pornography when he "intentionally views, acquires, or accepts child pornography on a computer from an outside source."[312] Citing *Romm*, the Eleventh Circuit found that an intentional viewer may be convicted whether or not he saves the images to his hard drive, edits the images, or exerts some sort of control over the images: "Evidence that a person has sought out—searched for—child pornography on the internet and has a computer containing child-pornography images—whether in the hard drive, cache, or unallocated spaces—can count as circumstantial evidence that a person has 'knowingly receive[d]' child pornography."[313] The court then refocused on the potentiality for inadvertent acceptance of images, stating that the "specter of spam, viruses, and hackers must not prevent the conviction of the truly guilty."[314]

As to the count of receiving images on his work computer, the evidence[315] was sufficient for a reasonable jury to have concluded that Pruitt knowingly received the images he viewed on his personal computer via the work computer.[316]

Finally, regarding the count of receiving images on his home computer, the Eleventh Circuit found the "totality of other evidence" was sufficient for Pruitt's conviction.[317] His internet searches performed on several different occasions, the lack of substantiation for a Trojan virus theory,[318] and Pruitt's confession to viewing child pornography on his work computer were enough.[319] Pruitt's conviction was affirmed in a concise four-page opinion.[320]

[310] *See id.*

[311] *See id.* (citing 13 OXFORD ENGLISH DICTIONARY 314 (2d ed. 1989); WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY: UNABRIDGED 1894 (1993)).

[312] *Id.*

[313] *Id.*

[314] *Id.* at 767. Because of the stigma associated with a child pornography conviction, the Eleventh Circuit noted the particular difficulty of prosecuting child pornography defendants in a technologically advanced day and age. *See id.*

[315] Although the Eleventh Circuit did not directly identify the evidence, it is reasonable to assume that it considered Pruitt's confessions coupled with his increased internet activity to be sufficient to affirm the conviction.

[316] *Id.*

[317] *Id.*

[318] At trial, Pruitt's computer forensics expert suggested that a Trojan virus was responsible for the images found in the cache and unallocated space of Pruitt's home computer. *See id.*

[319] *See id.*

[320] *Id.*

2. The Fifth Circuit: *United States v. Winkler*

Twelve days after the Eleventh Circuit ruled on *Pruitt*, the Fifth Circuit made a similar ruling in *Winkler*. However, in *Winkler*, the court relied on direct proof to affirm Winkler's conviction because the files found in his cache were video files.[321] Nevertheless, it is still an important case because the Fifth Circuit accepted a pattern of child pornography searches to evidence the defendant's knowing receipt.[322] Thus, the analysis in this case is in direct conflict with *Dobbs*.

The Immigration and Customs Enforcement (ICE) began a national investigation targeting child pornography offenders,[323] which led to "the discovery of a child pornography web site."[324] To access child pornography via the website, a user visited a welcome page that offered "samples of child pornography" and unlimited memberships in exchange for paid subscription.[325] Once subscribed, a user would receive an email containing a link to the content.[326] The link led users to a sign-in screen requiring a user name and password.[327] The sign-in screen "warned that its contents were illegal in all countries."[328] The website contained approximately 1,000 images of child pornography.[329]

ICE executed a search warrant of the server hosting the website.[330] There, agents came across David Winkler's email address and physical address.[331] They also found that Winkler's credit card "was used to make purchases of child pornography on two dates."[332] In a separate investigation, ICE came across several commercial child pornography websites.[333] An agent found that someone using a PayPal account associated with the name David Winkler had purchased access to one of these websites.[334]

In February 2007, Winkler's name was referred to local ICE agents.[335] The agents obtained Winkler's credit card records, which verified the purchases that the ICE had discovered in both of its investigations.[336] A

[321] *See* United States v. Winkler, 639 F.3d 692, 695 (5th Cir. 2011); *see also infra* Part II.B.2.a, b (discussing the difference between video files and image files and why video files provide direct proof of child pornography receipt).

[322] *See id.* at 699.

[323] *See Winkler*, 639 F.3d at 693.

[324] *See id.*

[325] *Id.* The website charged $79.95 for a twenty-day membership and $90.00 for a one-month membership. *Id.*

[326] *Id.*

[327] *Id.*

[328] *Id.*

[329] *Id.* at 694.

[330] *Id.*

[331] *Id.* Agents found that Winkler's information "was transmitted to the website as part of a membership sign-up procedure." *Id.*

[332] *Id.*

[333] *Id.*

[334] *Id.*

[335] *Id.*

[336] *Id.*

search of Winkler's home resulted in the seizure of three hard drives.[337] One, a Maxtor hard drive,[338] contained two accounts: "user" and "staff."[339] Winkler admitted that the "user" account was his own.[340] On the "user" account, forensic specialists recovered twenty-six video files of child pornography.[341] Five of those video files were located in the cache.[342]

Agent James Beard, the government's computer forensic specialist, testified at trial that "a video file is copied to a temporary internet cache when the user takes an affirmative action such as clicking on the video in order to play it."[343] This means that a video is fundamentally different from an image because it does not save in the cache automatically.[344]

Winkler was charged with receiving[345] and possessing[346] child pornography.[347] After a jury trial, Winkler was found guilty and sentenced to seventy-three months imprisonment.[348]

On appeal, Winkler contested count one, which charged him with knowing receipt of two video files.[349] Winkler alleged that there was insufficient evidence to support the conviction because the prosecuted video files were found only in his cache.[350] Winkler contended that "the most the evidence shows is that he viewed those two videos over the internet, and that he was unaware that the files would be automatically downloaded into the temporary cache."[351] The Fifth Circuit disagreed. Noting that the "exact contours of the crime of 'knowingly receiving' electronic child pornography in a constantly shifting technological background are murky,"[352] the Fifth Circuit summarized how its sister circuits had addressed the issue.[353]

[337] *See id.* The three hard drives were the Quantum Fireball, Segate, and Maxtor. *Id.* On the Quantum Fireball, 261 images of child pornography were found in the CD-ROM toolkit extras folder—an unusual location for a user to save a file. *See id.* Computer forensic agent James Beard testified that, to save a file in there, "an individual would have to browse his hard drive's contents and specifically choose that obscure directory." *Id.* On the Seagate hard drive, Agent Beard found 261 images and eighteen videos of child pornography saved in another nondefault location. *Id.*

[338] The Fifth Circuit was only concerned with the Maxtor hard drive because it contained all the images at issue on appeal. *Id.*

[339] No child pornography was found in the "staff" account. *See id.* at 695.

[340] *See id.* at 694.

[341] *See id.*

[342] *See id.* at 695.

[343] *Id.*

[344] *See id.* Beard also testified at trial that there were no viruses or malware on the Maxtor hard drive. *See id.* He also found no evidence of a Trojan virus. *See id.*

[345] 18 U.S.C. § 2252(a)(2) (2006).

[346] *Id.* § 2252A(a)(5).

[347] *See Winkler*, 639 F.3d at 695.

[348] *See id.*

[349] *See id.* at 695–96.

[350] *See id.*

[351] *Id.* at 696.

[352] *Id.*

[353] *Id.* at 696–99. "Understandably, our sister circuits have struggled with whether to impute knowledge from the presence of illicit files found in such temporary storage." *Id.* at 696.

First, the Fifth Circuit addressed the Tenth Circuit's approach. Comparing Winkler's crime with that of the defendant in *Dobbs*,[354] the Fifth Circuit noted that there "was no evidence that the defendant in *Dobbs* was a member of any pay-per-view child pornography web site, or, indeed, that the defendant had *even seen* the two images that were the basis of his conviction."[355] Then, looking to the decisions in which the Tenth Circuit did affirm, the Fifth Circuit found *Bass* and *Tucker* to be cases "where a review of the evidence showed that the evidence did point convincingly towards the defendant's intent."[356]

Moving to the Eleventh Circuit's decision in *Pruitt*, the Fifth Circuit found that Pruitt's conviction was affirmed because "the evidence showed that the defendant sought out and viewed child pornography, searched for child pornography on the internet, and had downloaded child pornography on an entirely different computer at the same time."[357]

The Ninth Circuit came next. Looking first at *Kuchinski*, then *Romm*, the court noted that the Ninth Circuit's analysis turned on knowledge and control of the cache.[358] The Fifth Circuit reasoned that, in *Kuchinski*, the Ninth Circuit did not find the evidence sufficient to impute knowledge, while in *Romm*, it came to the opposite result because Romm admitted that he destroyed the images in the cache.[359]

Lastly, the Fifth Circuit addressed its own cache case, *United States v. Calderon*.[360] There, the Fifth Circuit had been faced with the issue of whether temporary internet files found in the cache may be counted for the purpose of sentencing.[361] The Fifth Circuit found substantial evidence in the record, including Calderon's "history with child pornography," his "activity procuring child pornography," and the "lack of alternate explanations for the presence of images found on his computer," to affirm his conviction for knowing possession.[362]

The Fifth Circuit noted that these cases were united not by the cache itself, but by "the broader concern that an internet user may find himself ensnared in a child pornography case unwittingly, by virtue of files that were copied to temporary storage and never knowingly received."[363] After summarizing the various strategies used by circuit courts to determine

[354] *See id.* at 697; *see also* United States v. Dobbs, 629 F.3d 1199, 1201 (10th Cir. 2011).

[355] *Winkler*, 639 F.3d at 697.

[356] *Id.*

[357] *Id.* at 697–98.

[358] *Id.* at 698.

[359] *See id.*

[360] 318 F. App'x 277 (5th Cir. 2009).

[361] *Winkler*, 639 F.3d at 698 n.3 (citing *Calderon*, 318 F. App'x at 278).

[362] *Id.*

[363] *Id.* at 698.

knowing receipt,[364] the Fifth Circuit found none of these techniques "talismanic."[365]

Finding that "receipt" should be given its everyday meaning in order to prevent "savvy users of child pornography from using the technologically static nature of our opinions as a basis for engaging in precisely the behavior the anti-child pornography statutes were meant to forbid," the Fifth Circuit emphasized that its inquiry was highly fact specific and not tied to the presence of the files in the cache.[366] Thus the Fifth Circuit determined that the facts before it were distinguishable from those in *Dobbs* and *Kuchinski*, and were more like those in *Tucker*, *Bass*, *Romm*, and *Pruitt*.[367] While the evidence in *Dobbs* was "tenuous at best," the evidence was "overwhelming" that Winkler sought out, downloaded and viewed the images, and had the ability to manipulate the images.[368]

The Fifth Circuit explained the importance of this evidence. First, the jury could reasonably infer that the two video files came from the members-only section of a child pornography website.[369] Second, Winkler repeatedly paid for access to child pornography websites, even entering a user name and password to access the two videos at issue in count one.[370] Finally, the videos could not have been copied to the cache without Winkler's affirmative action of clicking play.[371] Winkler's conviction was affirmed because the Fifth Circuit found that "there was sufficient evidence to do so."[372]

Thus, the Fifth and Eleventh Circuit disagree with the Tenth Circuit regarding what constitutes sufficient proof to determine if a defendant has knowingly received child pornography. The Tenth Circuit in *Dobbs* found that, in order to affirm Dobbs's conviction, it needed direct proof that Dobbs had knowingly viewed the images in question. The government's case, which proved Dobbs's systematic search for child pornography, was not enough to demonstrate his *knowing* receipt of the two images. Unlike the Tenth Circuit, the Fifth Circuit in *Pruitt* and the Eleventh Circuit in *Winkler* did not require direct proof, and looked to the defendants' searches for child pornography to affirm the two defendants' convictions. This circuit split demonstrates the need for uniform interpretation, and thus uniform application, of § 2252(a)(2) and § 2252 (a)(4)(B) so that courts can access the proper evidence when determining if a user has knowingly received, possessed, or accessed with intent to view child pornography.

[364] These strategies included "the defendant's knowledge of the cache function, a search pattern for child pornography, evidence of deleting illicit files after the fact, or the use of cache cleaning software." *Id.* at 698–99.

[365] *Id.* at 699.

[366] *Id.*

[367] *Id.*

[368] *Id.*

[369] *See id.*

[370] *See id.*

[371] *See id.*

[372] *See id.* at 701.

III. TECHNOLOGY NEED NOT COMPROMISE THE UNIFORM APPLICATION OF THE LAW: A PROPOSED SOLUTION

This part evaluates the Ninth and Tenth Circuits' reasoning in *Tucker*, *Bass*, *Kuchinski*, and *Romm*, and finds that these analyses are not compelling. Next, this part assesses the circuit split opinions and finds those arguments unconvincing as well. Lastly, this part advocates that the best statutory interpretation would allow courts to uniformly apply the law when child pornography images are found exclusively in the cache. The best definition of "knowingly" lies between the Tenth Circuit and the Fifth and Eleventh Circuits' interpretations, and would allow courts to look at circumstantial evidence when determining a defendant's state of mind in relation to images found exclusively in the cache.

A. Why Circuit Courts Before the Split Got It Wrong

The Ninth and Tenth Circuits analyzed the statute incorrectly for two reasons. First, computer possession and receipt is not the same as tangible possession and receipt. Therefore, the "everyday" definition of possession is helpful, but not dispositive, of what constitutes the crime in the computer context. Second, intent is not a mens rea element of the crime. By inferring intent into the crime, circuit courts have strayed from statutory terms and complicated an analysis that could be more straightforward.

1. A User Can Hold a Computer but Not the Pixels on the Screen

The Ninth Circuit developed the "control and knowledge" approach after looking to the everyday definition of possession. Finding that possession was defined as "[t]he fact of having or holding property in one's power; the exercise of dominion over property,"[373] the Ninth Circuit reasoned that knowledge of the cache and the ability to control the images therein evidence a defendant's guilt.[374] Furthermore, knowledge of the cache is one factor that the Tenth Circuit relied on when determining Tucker's and Bass's guilt.[375]

However, it makes little sense to suggest that if a defendant has knowledge of the cache, he has the requisite knowledge to be found guilty of knowing receipt or knowing possession. "Knowledge" in the statute does not speak to knowledge of computer technology—it speaks to knowledge of the images.[376] Imputing knowledge of a computer storage device to infer control is not the correct path because it results in arbitrary

[373] United States v. Romm, 455 F.3d 990, 999 (9th Cir. 2006) (citing BLACK'S LAW DICTIONARY 1183 (7th ed. 1999)).

[374] *See id.* at 1000–01; *see also supra* Part I.D.1.

[375] *See, e.g.*, United States v. Bass, 411 F.3d 1198, 1202 (10th Cir. 2005) ("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."); United States v. Tucker, 305 F.3d 1193, 1205 (10th Cir. 2002) ("Tucker continued to view child pornography knowing that the pornography was being saved, if only temporarily, on his computer.").

[376] *See* 18 U.S.C. § 2252(a)(2), (4)(B) (2006).

decisions. Tucker knew his cache existed—thus he was guilty of knowing possession.[377] Romm knew his cache existed—thus he was guilty of knowing possession and receipt.[378] Kuchinski did not know his cache existed—thus he was not guilty of knowing possession.[379] All three defendants sought out child pornography images over the internet.[380] All three defendants viewed images of child pornography in their search.[381] However, two are guilty and one is not because Romm and Tucker were more sophisticated computer users.[382]

There are two concerns with this approach. First, the divergent results of *Romm* and *Tucker* compared with *Kuchinski*, based on the determination that Romm and Tucker exercised actual control over the images found in their cache, may appear arbitrary given the fact that all three men sought and viewed images of child pornography. Second, a "knowledge and control" approach that accepts control as the "ability to control" leads to inconsistent results even among cases where it is agreed that the defendant has knowledge of the cache.

a. Actual Control Over Images Found in the Cache Does Not Evidence Knowing Possession

In *Romm*, the defendant deleted the images in his cache after learning that agents were going to search his computer.[383] In *Tucker*, the defendant manually deleted the images found in his cache.[384] Using this type of user control to help demonstrate knowledge is logical when defining possession. But Romm and Tucker did not use their caches to reaccess images other than when they were trying to conceal their guilt.[385] There was no evidence in either case that the defendants used their cache to reaccess temporary internet files. If there had been evidence that Romm or Tucker had used the cache to store images for later viewing like they might use any other folder on their computer, their knowledge combined with their actual control of images found in the cache would be sufficient.

But images in a cache are not like normal contraband. When a defendant possesses images on a computer, he cannot hold them. He cannot touch them. Computer possession cannot be equated with typical notions of possession. Romm, Bass, and Kuchinski employed the same strategy to search for images online.[386] All three defendants viewed child pornography

[377] *See Tucker*, 305 F.3d at 1205.

[378] *See Romm*, 455 F.3d at 990.

[379] *See* United States v. Kuchinski, 469 F.3d 853, 862 (9th Cir. 2006).

[380] *See id.* at 861–62; *Romm*, 455 F.3d at 998; *Tucker*, 305 F.3d at 1204.

[381] *See Kuchinski*, 469 F.3d at 862; *Romm*, 455 F.3d at 1001; *Tucker*, 305 F.3d at 1205.

[382] Furthermore, the result in *Kuchinski* appears especially surprising because of the thousands of images found in his cache. *See Kuchinski*, 469 F.3d at 856.

[383] *See Romm*, 455 F.3d at 994–95.

[384] *See Tucker*, 305 F.3d at 1198.

[385] *See Romm*, 455 F.3d at 995; *Tucker*, 305 F.3d at 1198.

[386] *See supra* notes 134, 151 and accompanying text; *see also Kuchinski*, 469 F.3d at 862.

during their search.[387] The only difference was that Romm and Tucker each knew that their computer would automatically save the images they viewed online—an action that was beyond their control.[388] Therefore, each defendant exercised control over the images by deleting them.

The knowledge that a computer saves everything should not determine their guilt. While a drug user may be able to get rid of his drugs to hide his guilt, Romm and Tucker would never have been able to clear their computers of all proof of child pornography. There must be a way to determine possession for defendants like Romm, Tucker, and Kuchinski without utilizing the notion of control because all three committed essentially the same acts. The standard should not require a defendant to have knowledge of his cache or control over the images therein to be found guilty of possession. Allowing a conviction to stand based on knowledge of the cache is unjust, and using the everyday definitions to determine Romm and Tucker's guilt simply makes them guilty by default.[389]

Judge Kelly would disagree. In his dissent in *Bass*, Judge Kelly stated, "[k]nowledge is inextricably bound up with the ability to exercise control, especially in the realm of computers and technology."[390] But, as these cases show, knowledge is inextricably bound up with the ability to exercise control in every arena *but* the realm of computers and technology. The type of control that a user employs in the computer context, especially by deleting images, is very different from normal ideas about control, because it can be manifested through a single click. In the computer context, this control is so minimal that it should not be the determining factor of guilt in the prosecution of a much broader crime. Thus, the control standard for determining possession of child pornography images in the computer context does not work and should not be employed by courts.

b. The Theoretical Ability to Lift an Elephant Is Not the Same As Lifting an Elephant

The Ninth Circuit does not require actual control, just the "ability to control";[391] this is problematic. In *Romm*, this concern can be dismissed because Romm did exercise *actual* control over the images in his cache by deleting his temporary internet files.[392] The same is true of Tucker.[393] It

[387] *See supra* notes 134, 151 and accompanying text; *see also Kuchinski*, 469 F.3d at 862.

[388] *See supra* notes 134, 151 and accompanying text; *see also Kuchinski*, 469 F.3d at 862.

[389] Their guilt was effectively automatic after they exercised control over the images found in their cache because computer forensic specialists were always going to be able to inspect their caches and determine that there had been manual deletions.

[390] United States v. Bass, 411 F.3d 1198, 1208 (10th Cir. 2005) (Kelly, J., dissenting).

[391] *See Romm*, 455 F.3d at 1001.

[392] Another problem with the Ninth Circuit's analysis is that it emphasized Romm's control over the images while they were on his screen, not while they were in his cache. *See id.* The court noted that Romm clicked on thumbnails to enlarge them. *See id.* This is not the type of control that should speak to knowledge of the cache, as he did this independently of any caching process.

becomes problematic in cases like *Bass* where an inference was made to determine Bass's knowledge of the cache.[394] Applying the Ninth Circuit's standard, it may be inaccurate to say that Bass really had the "ability to control" the images because he utilized a computer program that did the "controlling" for him. He had the ability to buy History Kill, which in turn had the ability to delete the images,[395] but he was not sophisticated enough to exercise direct control over the images.[396] If the analysis turns on sophistication, Bass surely falls on the side of Kuchinski rather than Romm and Tucker.

Thus, when courts focus on the ability to control, they link the idea of computer possession with tangible possession in a way that does not quite connect. Such an approach stretches the already tenuous knowledge inquiry. Moreover, it mischaracterizes possession in the computer context because computer possession is intangible. This approach would hold more weight in analysis if it treated all defendants similarly, but it does not. Further, it seems problematic for the Ninth Circuit to convict a defendant based on his theoretical, not actual, ability to do something.

2. Intentionally > Knowingly

The court in *Polizzi* recognized the problem presented by the hierarchical nature of statutory mens rea terms, finding that courts often confuse these terms when analyzing a defendant's guilt under § 2252.[397] This problem presented itself in the Tenth's Circuit's analysis in *Tucker*, where the court found that each time Tucker "intentionally sought out and viewed child pornography with his Web browser he knowingly acquired and possessed the images."[398]

Although the use of the word "intentionally" does not automatically mean the Tenth Circuit implied a higher-level mens rea term than the statute demands, their overall discussion demonstrates that their analysis was misdirected. Relying heavily on Tucker's continued search for child pornography despite the knowledge that his computer was caching the images, the court looked to his "intentional" searches to affirm his guilt.[399] This intentionality spoke to the nature of his search, which was purposeful. But just because his search was intentional does not mean that his possession was knowing. Although it may seem logical to affirm a higher level mens rea term in order to find guilt under a lower mens rea term, it

[393] *See Tucker*, 305 F.3d at 1198.

[394] It must be noted that the Tenth Circuit did not use an "ability to control" approach. Rather, it stated that Bass's attempt to remove images from his computer gave rise to an inference of his knowledge of the caching function. *See Bass*, 411 F.3d at 1202.

[395] *Id.* at 1201.

[396] *Id.* at 1200–01.

[397] *See* United States v. Polizzi, 549 F. Supp. 2d 308, 349–50 (E.D.N.Y. 2008), *vacated and remanded on separate grounds*, United States v. Polouizzi, 564 F.3d 142 (2d Cir. 2009); *see also supra* note 77.

[398] *Tucker*, 305 F.3d at 1205.

[399] *See id.*

does not work when they speak to two different acts: one of which is an element of the crime and one of which is not.

Congress chose the term of "knowingly" to capture more culpable conduct.[400] Thus, when the Tenth Circuit added an "intentional search" requirement, it created a new type of analysis: the "sought the images + knowledge" inference approach.[401] This complicates the analysis. It was understandable for the Tenth Circuit to use the search terms as evidence against the defendant, but the Tenth Circuit should have found a way to use the evidence without introducing a new requirement into the crime that raised the bar for guilt under the statute.

B. Why Circuit Courts in the Split Got it Wrong

The following sections critique the circuit courts' reasoning in *Dobbs*, *Pruitt*, and *Winkler*, finding that the courts' analyses fell short of providing a consistent guideline for future courts to use when confronted with a defendant charged with knowing possession and receipt of child pornography.

1. *United States v. Dobbs*

The Tenth Circuit in *Dobbs* engaged in a different § 2252 analysis than it had in *Tucker* and *Bass*.[402] The *Dobbs* court liked the aspects of the *Tucker* decision that emphasized the "control and knowledge" approach utilized in *Romm* and *Kuchinski*.[403] However, the requirement that the defendant must have sought out the particular images at issue was completely abandoned in favor of an analysis that would not consider any circumstantial evidence as to a defendant's behavior in seeking out the images.[404] As a result, the Tenth Circuit took a step too far in the opposite direction.

The government put forth a compelling case as to every non-prosecuted image.[405] But the Tenth Circuit was adamant that Dobbs could not be found guilty of receipt unless the government proved that he knowingly received *the two images in question*.[406]

Dobbs did not offer any alternative explanation for why the images of child pornography were found in the cache. Pure powers of deduction could lead a reasonable jury to the conclusion that even if Dobbs did not specifically view the two images in question, the fact that he viewed at least some child pornography satisfies his knowing receipt.

More importantly, Dobbs was a receipt case.[407] Does a defendant have to see every image on a website in order to receive any images found

[400] *See supra* note 101 and accompanying text.
[401] *See supra* Part I.D.1.
[402] *See supra* Part 2.A.1.
[403] *See supra* Part I.D.3.
[404] *See* United States v. Dobbs, 629 F.3d 1199, 1205 (10th Cir. 2011).
[405] *See supra* notes 225–28 and accompanying text.
[406] *See Dobbs*, 629 F.3d at 1208.
[407] *See id.* at 1201.l

therein? No. Knowing receipt can easily occur without exact details about which cached images are received.

The court's insistence that Dobbs view *the two images in question* created a standard that would make guilt under the statute impossible for defendants like Dobbs. As Chief Judge Briscoe noted in her dissent, the technology of computer caching combined with the secretive nature of the crime means it is nearly impossible for a computer forensic specialist to prove that Dobbs viewed the two images.[408] The reasons for this are two-fold. First, when looking at a website, every image is saved to the cache.[409] But it is rare that a user views *every* image on the page. It is impossible to distinguish which images were viewed and which images were not just from examining the cache. Thus, there is always the possibility that defendants like Dobbs did not view the actual images in question. Second, the computer forensic specialist was not able to connect a Google search to the images in question. But there was ample explanation for this: Dobbs typed web addresses directly into his browser.[410] Therefore, it would have been impossible to find a search immediately preceding the viewing of the images in question to implicate his guilt. Therefore, the Tenth Circuit's insistence created a burden of proof that the government could never meet.

Moreover, § 2252(a)(2) does not require knowing receipt of the *images in question*.[411] Although this was a reasonable reading of the statute, it is an interpretation other circuit courts have not taken because of the impossibility of proof. The Tenth Circuit may have read this unnecessary element into the statute to prevent a case of mistake from leading to guilt. But there is now an affirmative defense for mistaken possession that will protect against an inaccurate prosecution.[412] The Tenth Circuit did not need to confine the statute to protect Dobbs from being prosecuted for an accident or mistake, especially because it was clear that *Dobbs* was not a mistake case.[413]

Finally, when criticizing the government's case, the Tenth Circuit noted:

> The mere presence of the files in the cache is certainly proof that the files were *received* through the automatic-caching process; however, for this evidence to be probative of the question of *knowing* receipt, the government needed to present proof that Mr. Dobbs at least knew of the automatic-caching process."[414]

Nowhere does the statute read that to be guilty under knowing receipt, a defendant must have knowledge of the caching process. By taking this reading of the statute, the Tenth Circuit missed the mark, and once again, unnecessarily read the statute too narrowly.

[408] *See id.* at 1210–13 (Briscoe, C.J., dissenting).

[409] *See supra* Part I.A; *see also supra* note 23.

[410] *See Dobbs*, 629 F.3d at 1211.

[411] 18 U.S.C. § 2252(a)(2) (2006).

[412] *See id.* § 2252(c); *see also supra* note 86.

[413] *See Dobbs*, 629 F.3d at 1205.

[414] *See Dobbs*, 629 F.3d at 1205.

In *Dobbs*, the Tenth Circuit took a step away from circuit courts' tendency to affirm a defendant's guilt when images are found exclusively in the cache. Although the court was free to depart from *Tucker*, its approach was too narrow and allowed Dobbs to escape conviction for the same conduct that Tucker and Bass were found guilty for.

2. *United States v. Pruitt*

Pruitt held that knowing receipt occurs when one intentionally views, acquires, or accepts child pornography on a computer from an outside source.[415] But § 2252(a)(2) now separately criminalizes viewership. Thus, this standard for knowing receipt cannot stand as the best test because the Eleventh Circuit defined "knowing receipt" as Congress has defined "knowing[] access[] with intent to view."[416] While the amended statute was not applied to Pruitt's crime, the 2008 amendments were available to the Eleventh Circuit when deliberating.

But the analysis in *Pruitt* was headed in the right direction because the Eleventh Circuit declined to consider Pruitt's ability to control the images found in his cache.[417] Instead, the Eleventh Circuit found that evidence that a defendant has searched for child pornography on the internet and has a computer containing child pornography images is enough to convict the defendant of knowing receipt.[418] Considering the strong evidence demonstrating Pruitt's knowing search for child pornography,[419] it was clear that Pruitt had knowingly received child pornography.

Therefore, the *Pruitt* court almost got it right. The court's definition of knowing receipt could have captured the conduct of defendants like Tucker, Kuchinski, and Dobbs, but ultimately defined knowing receipt as Congress had already defined it when they criminalized knowing access with intent to view.3. *United States v. Winkler*

Winkler is distinguishable because it concerned video files, which are inherently different from image files: a video file is not automatically downloaded into the cache unless the user presses play.[420] Therefore, there is no doubt that a defendant has viewed an illicit file if a child pornography video file is found in his computer's cache. This does not have to do with control; rather, it has to do with what was impossible to prove in *Dobbs*: while no prosecutor could have proved that Dobbs viewed the images, if the same files had been videos, his viewership would have been easier to prove.

Winkler is still a helpful comparison, though, because of the court's analysis. After finding Winkler's case more like *Tucker*, *Bass*, *Romm*, and

[415] *See* United States v. Pruitt, 638 F.3d 763, 766 (11th Cir. 2011).

[416] *See id.*

[417] *See id.*

[418] *See id.*

[419] This evidence included his confession to police, illicit search history, and the lack of an affirmative defense to explain the presence of so many child pornography images in his cache. *See id.* at 766–67.

[420] *See* United States v. Winkler, 639 F.3d 692, 695 (5th Cir. 2011).

Pruitt, and less like *Dobbs* and *Kuchinski*,[421] the Fifth Circuit referred to Winkler's "pattern of child pornography receipt and possession" when concluding that Winkler knowingly received the files.[422] This is notable because while the Fifth Circuit found that their case was like *Dobbs*, it employed reasoning contrary to the Tenth Circuit's analysis there. The Tenth Circuit adamantly refused to accept a pattern of prior receipt of child pornography as proof for the receipt of the images at issue.[423] This contradiction illustrates that uniform application of the law has been compromised by the difficulty of grappling with possession and receipt in the computer context. The *Winkler* court went through the history of child pornography convictions when images are found exclusively in the cache. Because of that complex history and the variety of analyses employed, the Fifth Circuit came to the conclusion based on a theory of guilt that had been rejected by the Tenth Circuit.

The cases summarized by the Fifth Circuit were highly fact specific, and the court noted this as a reason for the differences in analyses.[424] For example, one of the primary facts that influenced the Fifth Circuit's affirmation of Winkler's guilt was the fact that Winkler was a member of a paid-for membership child pornography website.[425] Emphasis on the facts is key when images are found exclusively in the cache. Because the cache saves every image, associating guilt with the fact that the images are found there leads to inconsistent results.[426] Looking to all the facts surrounding the user's behavior will lead courts to a more consistent result. This is a logical approach that takes technology out and puts common sense in. Although the Fifth Circuit confused the different courts' analyses, the court was still able to reach the right result because the facts illustrated that Winkler knowingly received child pornography images when he purchased a subscription to access the images online.[427]

C. A Solution

The solution to uniform possession and receipt prosecutions lies outside the confusing computer context. Congress attempted to clarify the law with 2008 amendments—but with the current Tenth Circuit analysis—the amendments will do little to provide courts with a consistent standard by which to analyze knowing receipt. Thus, this Note proposes that courts look outside the computer context and instead at the circumstantial evidence surrounding the crime in order to reach consistent results when images are found solely in a user's temporary internet storage.

[421] *See id.* at 698–99.
[422] *See id.* at 699.
[423] *See* United States v. Dobbs, 629 F.3d 1199, 1206–07 (10th Cir. 2011).
[424] *See Winkler*, 639 F.3d at 699.
[425] *See id.*
[426] *See supra* Part III.A.1.
[427] *See Winkler*, 639 F.3d at 699.

1. The 2008 Amendments: So Close, But Not Enough

The 2008 amendments are a step in the right direction because they further criminalize conduct associated with the search for child pornography. But there is one problem with the criminalization of "knowing[] access[] with intent to view."[428] This problem was illustrated in *Dobbs*.

In *Dobbs*, knowing access would have been easy to prove because of Dobbs's web searches for child pornography.[429] The government presented evidence proving that Dobbs visited websites containing child pornography either by typing in a web address or by searching for the website through a search engine.[430] But "intent to view" becomes difficult to prove if it must be proven that a defendant like Dobbs had the intent to view the two images at issue.

It would have been impossible for the government to prove that Dobbs had the intent to view the two images for the same reason it was impossible for the government to prove that Dobbs knowingly viewed the two images.[431] If his intent must relate to the two images in question, and not the overall body of images found on a website, then courts will be stuck when images are found exclusively in the cache.

It is clear that circuit courts are applying a variety of analyses in the complex situation when images are found exclusive in the cache.[432] Although the 2008 amendments attempted to make this analysis easier, the amendments will not be helpful if the subtle differences in courts' analyses result in inconsistent reversals of guilt, like that in *Dobbs*. While the 2008 amendments may make certain cases more straightforward, such as those in which there is direct proof that a defendant has knowingly possessed or received the images in question, ultimately they do not solve the problem of how to uniformly determine a defendant's guilt or innocence when images are found exclusively in the cache.

There is also a problem with the placement of "knowing[] access[] with intent to view" in the possession statute. *Dobbs* was a receipt case.[433] The 2008 amendments appear in the same section as knowing possession.[434] Thus, such a standard may not even be employed in cases like *Dobbs* if knowing receipt is prosecuted but knowing possession is not.

As discussed in Part I.B.4, knowing possession and knowing receipt are different crimes. Knowing receipt requires more proof because receipt actively perpetuates the crime of child pornography in a way that pure possession may not.[435] The 2008 amendments were added to the possession statute, § 2252(a)(4)(B), but they may actually speak more to the

[428] 18 U.S.C. § 2252(a)(4)(A) (2006 & Supp. V 2011).
[429] *See supra* Part II.A.1.a.
[430] *See* United States v. Dobbs, 629 F.3d 1199, 1202 (10th Cir. 2011).
[431] *See id.* at 1212–13 (Briscoe, J., dissenting); *see also supra* Part II.A.2.b.
[432] *See supra* Parts I.C.1–4, II.A–B.
[433] *See Dobbs*, 629 F.3d at 1201.
[434] *See* 18 U.S.C. § 2252(a)(4)(B) (2006 & Supp. V 2011).
[435] *See supra* note 108 and accompanying text.

behavior that one demonstrates when one knowingly receives child pornography under § 2252(a)(2). A user does not knowingly access child pornography images without knowingly seeking those images on the internet. However, a user may knowingly possess without knowingly accessing.[436] Therefore, if a court employs a *Dobbs* analysis, the 2008 amendments may not only fail to capture the conduct they intended to, they may also be of little use to a court dealing with a knowing receipt possession when images are found exclusively in the cache.

2. Circumstantial Evidence Holds the Key to Uniformity

The severe criminal penalties imposed[437] for a violation of § 2252(a)(2) and § 2252(a)(4)(B) speak to Congress's intent to punish those who receive, possess, and seek out child pornography images.[438] The number of incidents and perpetrators has increased since the introduction of web technology,[439] and one way to combat the extensive number of online images and the continued exploitation of children is to punish offenders harshly. Additionally, Congress's intent to convict users when images are found exclusively in their cache was made clear with the addition of the 2008 amendments.[440] This is a definitive statement by Congress that knowingly seeking out child pornography is a crime, just like possession or receipt of the images.

Thus, it is clear that if child pornography images are found in the cache, guilt under the statute is proper unless there is a convincing showing of mistake.[441] Therefore, a statutory analysis that could capture the conduct of all seven defendants analyzed in this Note, plus any future defendants who are prosecuted based solely on images found in their cache—without including mistake cases—would be beneficial to courts when they are handed a difficult case like *Dobbs*.

Courts need to stretch *Winkler*'s highly fact specific analysis.[442] Instead of focusing on the fact that the images are in the cache, courts should accept that cached images were accessed by the defendant even if he did not view *every* image. Instead, the focus should be on the circumstantial evidence surrounding the crime. What search terms did the defendant type into his web browser? If search terms were used that would normally produce results associated with child pornography, that is a piece of evidence

[436] Like a user may knowingly possess without knowingly receiving. *See supra* notes 99–100 and accompanying text.

[437] Dobbs was sentenced to eleven years in prison based on the prosecution of two images before his conviction was reversed. *See Dobbs*, 629 F.3d at 1202. Kuchinski was sentenced to nearly six years. *See* United States v. Kuchinski, 469 F.3d 853, 857 (9th Cir. 2009). Romm to fifteen years. *See* United States v. Romm, 455 F.3d 990, 993 (9th Cir. 2006).

[438] *See supra* notes 59–60 and accompanying text.

[439] *See supra* note 45 and accompanying text.

[440] *See supra* Part I.B.3.

[441] *See supra* notes 86–89 and accompanying text.

[442] *See* United States v. Winkler, 639 F.3d 692, 699–700 (5th Cir. 2011); *see also supra* Part III.B.3.

indicating knowing receipt or possession. If search terms were used that would normally produce results associated with adult pornography, that is a piece of evidence pointing against knowing receipt. Did the defendant pay for access to a child pornography website? Does the defendant have a history of child pornography possession or receipt? Does the defendant have illicit images stored on some other electronic device? Did the defendant try to hide the images on his computer in an intentionally mislabeled folder? How many images are in the cache? How many searches likely to return child pornography results were run? Has the defendant confessed to viewing, possessing, receiving, or accessing child pornography? Answers to these questions will necessarily point to guilt or innocence under the statute, as Congress intended.[443] Furthermore, this analysis does not read terms into the statute that do not exist in order to find a way to establish guilt in the conceptually challenging computer context.

CONCLUSION

The Tenth Circuit came to a different result than the Eleventh and Fifth Circuits when determining what constitutes knowing receipt of child pornography images because of the difficulty in proving knowing receipt when images are found exclusively in a temporary storage device that saves images automatically. Further, the precedential cases used in the circuit courts' analyses provide little help because of the variety of approaches and inconsistent results. In order to uniformly prosecute child pornography defendants as Congress intended, the focus should shift from the cache and instead hone in on the evidence surrounding a defendant's behavior. Dobbs and Kuchinski should have been found guilty of child pornography receipt and possession because the evidence surrounding their behavior pointed to their knowledge, and therefore, their guilt.

[443] *See supra* Part I.B.1.