COMMENT

CHILD PORNOGRAPHY STATUTES AND THE CLOUD: UPDATING JUDICIAL INTERPRETATIONS FOR NEW TECHNOLOGIES*

ABSTRACT

When Congress passed the Protection of Children from Sexual Predators Act of 1998, it did not quite envision a world in which cloud storage and the internet would radically alter and increase child pornography possession and dissemination. The Act amended the existing possession statute to criminalize possession of "matter" containing visual depictions of child pornography. The statutory language requiring possession of "matter" was understandable in the context of the 1990s, where a defendant would presumably possess some physical object, whether a book or computer, that contained the child pornography.

However, the 2010s have seen a rapid increase in cloud storage usage. The primary benefit of cloud storage is to allow a user to completely avoid having to store data on their own physical medium. By keeping the data on remote servers, a user simply needs an internet connection to access their stored data from any location in the world. Despite its obvious benefits, cloud storage has created a method for individuals to potentially avoid falling within the language of the statute by failing to possess any physical object, or "matter." The definition of "matter" therefore

* J.D. Candidate at the University of Houston Law Center and Articles Editor of the *Houston Law Review*, Board 57. The Author thanks his husband Bin Ren, parents Douglas Carroll and Tara Tosta, and colleagues Maryam Ghaffar and Anita Liu for all of their support. Many thanks to Professor David Kwok for his suggestions and information while writing this article. Lastly, additional thanks to the Honorable Lee H. Rosenthal, Chief Judge of the Southern District of Texas, for the invaluable internship experience that made this Comment possible.

will have a major impact on whether cloud storage can be used by individuals to circumvent the possession statute.

The rapid growth of internet usage in the 1990s and 2000s, and the emergence of cloud storage technologies in the 2010s have caused the circuit courts to interpret the "matter" provision of the statute in a variety of ways. This Comment first analyzes the different court interpretations in light of the statute's language and legislative history to determine which interpretation would be most effective in responding to the growth of cloud storage. It then considers approaches taken by the states, as well as possible solutions found in different criminal statutes.

TABLE OF CONTENTS

I. INTRODUCTION

The Protection of Children from Sexual Predators Act of 1998 was a major effort by Congress to rework the federal child pornography statutes.[1] One of the most significant amendments

1. Protection of Children from Sexual Predators Act of 1998, Pub. L. No. 105-314, 112 Stat. 2974 (codified as amended in scattered sections of 18 U.S.C.).

was a change to § 2252(a)(4)(B), which now criminalizes possession of one or more "books, magazines, periodicals, films, video tapes, or other matter" that contain visual depictions of child pornography.[2] The statute's enumerated list of "matters" focuses heavily on traditional forms of media, which, at the time, were the primary vehicles for the dissemination of child pornography and media consumption in general.[3]

The late 1990s was an era of rapid growth in internet usage, and the emergence of digital media marked a monumental shift in how the average American views media of all forms.[4] Although this growth has had many benefits, an unfortunate consequence has been a surge in the sharing and consumption of child pornography.[5] Almost immediately, courts struggled to apply a possession statute focused on traditional media to the internet, and each circuit has adopted varying standards for two crucial elements of the statute: (1) what constitutes "other matter;" and (2) what constitutes "possession."[6]

Circuits that have limited the interpretation of "other matter" to physical objects[7] have been the most problematic for a few

---

2. 18 U.S.C. § 2252(a)(4)(B) (2012) (previous versions of the statute criminalized possession of "3 or more" matters). The Statute reads, in relevant part:

> Any person who 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 using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, 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 . . . .

Id.

3. *Id.*

4. Between 1995 and 2000, the share of Americans who used the internet increased from 14% to 46%. By 2005, the share had further increased to 66%. SUSANNAH FOX & LEE RAINIE, PEW RESEARCH CTR., THE WEB AT 25 IN THE U.S. 4, 13 (2014), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2014/02/PIP_25th-anniversary-of-the-Web_0227141.pdf [https://perma.cc/4Z24-LZAY].

5. U.S. DEP'T OF JUSTICE, THE NATIONAL STRATEGY FOR CHILD EXPLOITATION PREVENTION AND INTERDICTION: A REPORT TO CONGRESS 9, 11 (2010) ("The Internet and advances in digital technology have provided fertile ground for offenders to obtain child pornography, share child pornography, produce child pornography, advertise child pornography, and sell child pornography.").

6. *See infra* Part II.A (discussing court interpretations of "other matter"); *infra* Part II.C (discussing court interpretations of "possession").

7. United States v. Lacy, 119 F.3d 742, 748 (9th Cir. 1997) (concluding that "the 'matter' is the physical medium that contains the visual depiction").

reasons.[8] This Comment discusses the emergence of cloud computing and how it allows an individual to store child pornography on the cloud without ever importing it to a physical medium.[9] To make the statute workable in the digital era, the current circuit split will likely need to be resolved in favor of circuits that define the "matter" as individual files or some form of digital matter.[10] This more flexible interpretation is better suited to technology that does not involve the possession of physical mediums by the user.

The second element of "possession" has also been subject to different interpretations by the circuits.[11] Although most circuits are open to "constructive possession" in child pornography cases, their definitions of "constructive possession" vary.[12] Some interpretations make reference to possession of an "object, either directly or through another person or persons."[13] These

8. One issue that frequently arises but is outside the scope of this Comment is that because digital storage devices are now capable of storing enormous amounts of data, different types of "matters" can contain anywhere from a single image to terabytes of child pornography. *See* United States v. Vig, 167 F.3d 443, 447–48 (8th Cir. 1999) (declining to adopt the *Lacy* holding when interpreting the pre-amendment § 2252(a)(4)(B) criminalizing possession of "3 or more" matters, noting that "[t]o conclude . . . that a hard drive is the computer equivalent of a book, magazine, periodical, etc., would result in the absurd scenario where an individual who possesses three books with one visual depiction apiece violates the statute, but an individual with hundreds of images on a hard drive does not"). Before the emergence of cloud computing, these conflicting interpretations had not been as problematic in practice because multiple circuits have found the plain meaning of the amended statute's "1 or more" language to mean there may only be one conviction for possession of multiple matters. Whether an individual possessed one hard drive, twenty magazines, or thirty books ultimately resulted in a single conviction. *See* United States v. Polouizzi, 564 F.3d 142, 155 (2d Cir. 2009) ("The language '1 or more,' . . . indicates that a person commits one violation of the statute by possessing more than one matter containing a visual depiction of child pornography."); *see also* United States v. Emly, 747 F.3d 974, 979–80 (8th Cir. 2014) (relying on *Polouizzi* to conclude that conviction on three counts under § 2252(a)(4)(B) was multiplicitous and therefore unconstitutional).

9. *See* Audrey Rogers, *From Peer-to-Peer Networks to Cloud Computing: How Technology is Redefining Child Pornography Laws*, 87 ST. JOHN'S L. REV. 1013, 1048 (2013) ("[S]ince the [pornographic] images are stored on a remote server, some have questioned whether and who possesses them.").

10. *Vig*, 167 F.3d at 449 (holding that "computer image files are encompassed within the meaning of 'other matter' in section 2252(a)(4)(B)").

11. *See infra* Part II.C.

12. *See* United States v. Villasenor, 236 F.3d 220, 222–23 (5th Cir. 2000) (defining "constructive possession" under § 2252(a)(4)(B) as "the ownership, dominion or control over an illegal item itself or dominion or control over the premises in which the item is found"); *see also* United States v. Haymond, 672 F.3d 948, 955 (10th Cir. 2012) ("A person who, although not in actual possession, knowingly has the power at a given time to exercise dominion or control over an object, either directly or through another person or persons, is then in constructive possession of it.").

13. *Haymond*, 672 F.3d at 955 (requiring "dominion or control over an *object*" (emphasis added)).

interpretations that imply physicality are problematic in the cloud computing context where the item that is controlled is entirely digital and is operated through automatic processes rather than by any person. Problematic language should be replaced so as to avoid these references to physical mediums.

Although there is room for the courts to change their interpretations of § 2252(a)(4)(B), there are undeniable statutory deficiencies that should be addressed by Congress. As the circuits that have interpreted the enumerated examples have discussed, it is unusual to make the leap from a list of physical mediums to nonphysical.[14] It is also unclear why Congress chose to criminalize possession of the matter that contains the visual depictions. Many state child pornography statutes instead criminalize possession of the visual depictions directly.[15] Congress should take action to eliminate the "matter" portion of the statute altogether. Criminalizing possession of a "visual depiction" is flexible enough for the courts to apply the statute to new technologies such as cloud computing without the unnecessary "matter" element.

A combination of statutory reform and the resolution of circuit splits will allow us to better respond to the production and dissemination of child pornography in a new technological age. This Comment will begin in Part II with a discussion of the current federal statutes and caselaw concerning child pornography to understand how the courts and federal prosecutors have applied it to modern technologies such as cloud computing. Part III will then discuss which court interpretations are most adaptable to cloud computing and how the circuit splits would ideally be resolved. Part IV then considers potential solutions beyond current interpretations by: (1) comparing how various state child pornography statutes are written and whether they are more amenable to handling cloud computing cases; (2) comparing the child pornography statutes to other areas of law where cloud computing is regularly used for criminal or civil violations; and (3) analyzing other areas of the federal child pornography statutes to better understand which charges may be most effective in prosecuting individuals who use cloud computing to store and share child pornography.

---

14. *Vig*, 167 F.3d at 448 (noting that the statutory tools of *ejusdem generis* and *noscitur a sociis* in this situation lead to absurd results).

15. *See, e.g.*, S.D. CODIFIED LAWS § 22-24A-3 (2013) (holding a person criminally liable if they "knowingly possess[] . . . any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act"); *see also* TEX. PENAL CODE § 43.26(a) ("A person commits an offense if the person knowingly or intentionally possesses . . . visual material that visually depicts a child younger than 18 years of age at the time the image of the child was made who is engaging in sexual conduct . . . .").

II. UNDERSTANDING THE CURRENT LAW

A. Defining "Matter"

The courts' struggles in interpreting § 2252(a)(4)(B) can largely be explained by the unusual wording of the statute. The history of 18 U.S.C. § 2252 is indicative of a Congress that has consistently struggled to keep up with changes in our understanding of child abuse and the extent of child pornography, leaving possession as an afterthought to the commercial side of child pornography.

Earlier enactments of various federal child pornography statutes failed to even mention possession and instead criminalized only the commercial aspects of distribution and sale.[16] It was not until a 1990 amendment that the statute first criminalized possession using the "other matter" language.[17] The emphasis on the commercial side of child pornography continued as the statute criminalized knowing possession of "3 or more" such matters, leaving those in possession of two or fewer outside the scope of the statute.[18] When the House introduced the Protection of Children from Sexual Predator's Act, it failed to address the "3 or more" language.[19] Although the House report's stated purpose extensively discussed the internet, the primary focus was the use of the internet to lure, kidnap, or abuse children rather than its potential use for disseminating and accessing child pornography.[20]

---

16. *See* 18 U.S.C. § 2252(a)(1)–(2) (1982) (requiring receipt or transportation "for the purpose of sale or distribution for sale").

17. Crime Control Act of 1990, Pub. L. No. 101–647, § 323, 104 Stat. 4789 (1990) (codified as amended at 18 U.S.C. § 2252(a)(4)(B) (1994)).

18. The statute reads:

> Any person who . . . knowingly possesses 3 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 mailed or 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 . . . .

18 U.S.C. § 2252(a)(4)(B) (1994) (emphasis added).

19. *See* H.R. REP. NO. 105–557, at 3 (1998) (making only "technical correction[s]" to § 2252(a)(4)(B)).

20. *Id.* at 10 (noting the purpose of the bill was to "crack[] down on pedophiles who use and distribute child pornography to lure children into sexual encounters"). The greater concern remained on the supply side of production and distribution of child pornography rather than demand. *Id.*

It was not until the bill reached the Senate that an amendment was proposed, replacing all language of "3 or more" to "1 or more."[21]

As access to the internet and personal computers proliferated in the late 1990s,[22] much of the caselaw defining "matter" developed concurrently. The circuits were usually faced with a common scenario in which the government wished to define "matter" based on individual computer files, while defendants argued "matter" should refer to the computer, computer disk, or hard drive.[23] Because most of these early decisions involved convictions under the 1990 statute, the courts were interpreting "matter" in the context of the "3 or more" requirement.[24]

In *Lacy*, the Ninth Circuit applied standard statutory interpretation tools in finding the computer hard drive was "matter" under § 2252(a)(4)(B).[25] As that court noted, the enumerated examples in the statute refer exclusively to "physical media capable of containing images."[26] The *Lacy* decision came a year before the 1998 amendment adopted by Congress, and the Department of Justice was well aware of the statute's deficiencies in the digital age. The same House report that failed to make any substantive changes to the possession statute included a suggestion from the Department of Justice that the enumerated list be updated to include "computer disk" as an example.[27] Assistant Attorney General Harkins also wanted guidance that one computer disk containing three images may constitute a

21. 105 CONG. REC. S12,212 (daily ed. Oct. 9, 1998) (proposal of Sen. Hatch of amendment no. 3812).

22. *See supra* note 4 and accompanying text.

23. United States v. Vig, 167 F.3d 443, 448 (8th Cir. 1999) (finding the individual computer file was the "other matter" rather than the defendant's hard drive); United States v. Lacy, 119 F.3d 742, 748 (9th Cir. 1997) ("Although both the disks and the GIF files could be viewed as 'containing' the visual depiction, we conclude the 'matter' is the physical medium that contains the visual depiction . . . ."); *see also* United States v. Hall, 142 F.3d 988, 998–99 (7th Cir. 1998) (finding the district court was allowed to qualify individual computer files as "matter" under § 2252(a)(4)(B) instead of the computer as a whole).

24. *See infra* note 31 (noting the possession statute was amended in 1998 to lower the required number of possessed 'matters' from three to one).

25. *Lacy*, 119 F.3d at 748 ("This interpretation [of 'matter' as a hard drive rather than computer file] is supported by two principles of statutory interpretation, *noscitur a sociis* and *ejusdem generis*.").

26. *Id.*

27. *See* H.R. REP. NO. 105–557, at 30–31 (1998) ("We suggest that the phrase 'computer disk' be inserted in the phrase 'three or more books, magazines, periodicals, films, video tapes, or other matter' to clarify that possession of three or more computer disks, each of which contains at least one visual depiction of child pornography, also violates the possession statute, just as possession of one computer disk, containing three or more visual depictions of child pornography, violates the possession statute."). A nearly identical statute has since included that recommendation by adding "computer disk" into its list of "materials." 18 U.S.C. § 2252A (2012).

violation, suggesting that both the physical medium and the individual files could satisfy the "other matter" requirement.[28]

The Eighth Circuit discussed and rejected the *Lacy* decision, finding that it led to an absurd result.[29] The Eighth Circuit acknowledged the statutory tools used by the Ninth Circuit as leading to a conclusion that "matter" be defined as a physical medium, but was unwilling to adopt a definition that would have allowed the defendant in that case to avoid conviction entirely.[30] The Eight Circuit's rationale for defining "matter" as individual computer files has since been upended by the 1998 amendment removing the "3 or more" language.[31] Under the current "1 or more" language, possession of one hard drive containing hundreds of images would now lead to a conviction just as possession of three individual photos would. The absurd result the Eighth Circuit discussed is even less relevant now that most circuits have interpreted "1 or more" to mean there may only be a single conviction for possession, regardless of the number of matters possessed.[32]

Although both the Ninth Circuit and Eighth Circuit interpretations have support, legislative history tends to support the Ninth Circuit's position that "matter" is limited to physical mediums. Congress declined to include the Department of Justice's recommendations and left the enumerated list in its pre-amendment form. This supports the conclusion that interpreting "other matter" to be restricted to physical mediums is more in line with the plain meaning of § 2252(a)(4)(B).[33]

B. Cloud Computing and "Other Matters"

If the absurd result discussed by the Eighth Circuit was largely eliminated by the 1998 amendment, it may have made its return in the context of cloud computing.[34] While the late 1990s

28. H.R. REP. NO. 105—557, at 30–31.

29. United States v. Vig, 167 F.3d 443, 448 (8th Cir. 1999) ("To conclude, as defendants argue, that a hard drive is the computer equivalent of a book, magazine, periodical, etc., would result in the absurd scenario where an individual who possesses three books with one visual depiction apiece violates the statute, but an individual with hundreds of images on a hard drive does not.").

30. *Id.*

31. Protection of Children from Sexual Predators Act of 1998, Pub. L. No. 105-314, 112 Stat. 2974 (codified as amended in scattered sections of 18 U.S.C.) (changing "3 or more" to "1 or more").

32. *See* United States v. Emly, 747 F.3d 974, 977–78, 980 (8th Cir. 2014); United States v. Polouizzi, 564 F.3d 142, 153, 155–56 (2d Cir. 2009).

33. *See supra* note 27 and accompanying text.

34. Federal Courts have begun to address the legal issues around cloud computing.

saw a surge in internet usage, the 2010s have seen a similar explosion in personal cloud storage use.[35] Although users frequently have the option to download or upload content from their personal devices to the cloud, it is often the case that individuals store data exclusively on the cloud. Because § 2252(a)(4)(B) criminalizes possession of "matter" that contains the visual depiction, it is unclear what qualifies as "matter" when child pornography is stored on the cloud.

Applying the "physical medium" interpretation leads to the potentially absurd result that the server itself is the "matter" which contains the visual depictions. Under that interpretation, it is the cloud companies that are in possession of the child pornography. The industry would likely push back against such an interpretation, but regardless, the companies would not satisfy the "knowing" prong, as it is unlikely the companies are actively aware they possess child pornography.[36] But if the cloud companies

---

One court deemed it the "newest technology," and went on to explain:

> [F]iles are stored in a shared pool of computer resources on the Internet, accessible from any computer. Users do not download and install applications on their own device or computer; all processing and storage is maintained by the cloud server. The latest commercial uses promote file storage and access. For example, a person may store files from his computer onto a cloud service provider, such as Dropbox. The cloud system allows him to access his files from any computer by logging onto his cloud server. A cloud user may permit shared access to his files by designating users. Thus, similar to peer-to-peer networks, once a person allows access to his files, others may see them at any time. Unlike peer-to-peer networks, private cloud services require that a person designate who may have shared access.
>
> *The cloud is just the latest battleground between law enforcement and child pornographers*. The ability of child pornographers to use cloud computing for their wares has already been recognized. While some cloud providers are employing filtering techniques to suppress access to illegal images, there is a growing concern the cloud will provide deeper cover for pornographers. At the same time, cloud technology is beginning to raise possession and distribution questions.

United States v. R.V., 157 F. Supp. 3d 207, 231 (E.D.N.Y. 2016) (alteration in original) (quoting Rogers, *supra* note 9, at 1032–33).

35. Popular personal cloud storage company Dropbox alone grew from 50 million users in 2010 to more than 500 million users in 2018. Victoria Barret, *Dropbox: Inside the Story of Tech's Hottest Startup*, FORBES (Oct. 18, 2011, 8:30 AM), https://www.forbes.com/sites/victoriabarret/2011/10/18/dropbox-the-inside-story-of-techs-hottest-startup/#20bce9076437 [https://perma.cc/P3H7-9WRB]; Benjamin Rains, *Should You Buy Dropbox (DBX) Stock?*, ZACKS (July 12, 2018), https://www.zacks.com/stock/news/311337/should-you-buy-dropbox-dbx-stock [https://perma.cc/V6PJ-XTS4].

36. In reality, companies like Dropbox actively work with law enforcement to find and expose users who use the service for possession of child pornography. *See* Kate Knibbs, *Dropbox Refuses to Explain Its Mysterious Child Porn Detection Software*, GIZMODO (Aug. 12, 2015, 2:36 PM), https://gizmodo.com/dropbox-refuses-to-explain-its-mysterious-child-porn-de-1722573363 [https://perma.cc/HH8A-GWGG]. In the unlikely situation where the government attempts to prosecute a cloud company for possession, § 2252(c) would likely provide an affirmative defense:

cannot be prosecuted, it is unclear if cloud storage users who use the cloud to possess child pornography can.

Although no circuit has directly addressed this issue in the context of § 2252(a)(4)(B) yet, it has been addressed in dicta and within the context of similar statutes.[37] In *United States v. Forrester*, the Armed Forces Court of Appeals was faced with a defendant convicted for possession of child pornography on four separate "materials."[38] The Manual for Courts-Martial provides similar language to § 2252(a)(4)(B), requiring that the defendant knowingly possess "material that contains" a visual depiction.[39] The court of appeals concluded this meant possession of "physical media or storage location 'that contains' the offensive images."[40] The addition of "storage location" to its interpretation of "material" supported the defendant's possession conviction for not only an HP computer and two Seagate hard drives containing depictions of child pornography, but also for images located in a Gmail account, even though the data was stored on Google's servers.[41]

> 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.

18 U.S.C. § 2252(c) (2012).

37. *See* United States v. Chilaca, 909 F.3d 289, 292 n.2 (9th Cir. 2018) ("Neither party contests that the Dropbox account is a medium that can be the subject of a unit of prosecution under § 2252(a)(4)(B), and we so assume for purposes of this appeal."). Because of the double jeopardy issue that often arises with § 2252(a)(4)(B), the issue of possession in the cloud is often moot if possession of a physical matter was also charged. It would only take one instance of possession to support a violation, and any additional matters possessed cannot be separately charged. *Id.* at 295 ("We, like all other circuits that have considered the issue, interpret § 2252(a)(4)(B)'s use of the phrase "1 or more" to mean that the simultaneous possession of different matters containing offending images at a single time and place constitutes a single violation of the statute.").

38. United States v. Forrester, 76 M.J. 479, 482 (C.A.A.F. 2017).

39. MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, ¶ 68b (2016) [hereinafter MCM].

40. *Forrester*, 76 M.J. at 486.

41. *Id.* The court of appeals also discussed the potential for violation of the double jeopardy clause, but the military law refers to a sister statute § 2252A, which replaces the word "1 or more" with "any," which the court found allowed for multiple convictions. *Id.* at 487; *see also* United States v. Hinkeldey, 626 F.3d 1010, 1014 (8th Cir. 2010) (distinguishing between § 2252A and § 2252 to allow for multiple convictions under § 2252A); United States v. Planck, 493 F.3d 501, 504 (5th Cir. 2007) (allowing for multiple convictions of possession under § 2252A).

Although the court of appeals appears to have misconstrued precedent from the Fifth Circuit,[42] such a broad interpretation of § 2252(a)(4)(B) may be similarly necessary for convictions of possession on the cloud. The circuits could conclude that the definition of "matter" must be stretched to include a digital storage location, but it remains a questionable interpretation, especially in the criminal context where courts must deal with the rule of lenity. In particular, child pornography is not an area where Congress is divided and unwilling to act.[43] Should the courts conclude digital storage locations are not covered by "matter," Congress always has the ability to expand the definition. Congress needs to address the flaws of the statute, and the circuits should avoid questionable interpretations that paper over those flaws.

C. Defining "Possession" in the Context of Cloud Computing

Section 2252(a)(4)(B) provides no definition for "possession." Generally, requirements for possession have not seen the same circuit split as the definition of "matter."[44] Most circuits have explicitly acknowledged that constructive possession of child pornography is sufficient for a conviction under § 2252(a)(4)(B).[45]

---

42. In expressing its concern about the use of cloud computing to evade a possession charge, the majority noted "[t]hough Appellant may not have physically controlled the server on which the child pornography within his e-mail account was located, he constructively possessed the child pornography by storing it and retaining the capacity to return to retrieve it." *Forrester*, 76 M.J. at 486 n.7. The Armed Forces Court of Appeals cited to a Fifth Circuit decision in which a defendant was convicted on two counts for possession of child pornography on a USB and computer. However, both devices were found through an illegal search and seizure, and the devices themselves and their content were suppressed by court order. The prosecution instead introduced evidence that the defendant stored an "extensive collection" of child pornography on the cloud and also introduced evidence that his home computer was linked to the cloud service account. The Fifth Circuit ultimately held that a jury could reasonably conclude he had possessed child pornography on his computer and USB. United States v. Woerner, 709 F.3d 527, 540–41 (5th Cir. 2013). If anything, it appears the Fifth Circuit was troubled by relying on his cloud storage accounts for evidence, and the circuit emphasized how a jury could make the necessary links to the computer and USB devices as the required "materials" under § 2252A(a)(5)(B). *Id.* at 540. ("Slightly more difficult is the question whether the evidence supports the jury's verdict that Woerner possessed two 'materials' containing child pornography.").

43. The House passed the 1998 amendment by a vote of 400 to 0. 105 CONG. REC. H10,638 (daily ed. Oct. 12, 1998) (final roll call vote).

44. *See* sources cited *supra* note 23 (discussing different circuit interpretations of "matter").

45. *See* United States v. Villasenor, 236 F.3d 220, 223 (5th Cir. 2000) ("Constructive possession is sufficient for an offense under § 2252(a)(4)(B)."); *see also* United States v. Little, 864 F.3d 1283, 1289 (11th Cir. 2017) ("The government can establish possession 'by proof of "either actual or constructive" possession.'"); United States v. Haymond, 672 F.3d 948, 955 (10th Cir. 2012) ("[P]ossession of child pornography may be actual or constructive.").

However, different definitions of constructive possession still lead to varying results when applied to cloud computing.

Because § 2252(a)(4)(B)'s sister statute § 2252A(a)(5)(B) is generally interpreted as allowing for multiple convictions for possession,[46] circuits have addressed possession in the context of cloud computing under that statute.[47] In the Eleventh Circuit case *United States v. Rivenbark*, the defendant was convicted on counts of transporting and possessing child pornography for sharing a hyperlink to his Dropbox account which contained child pornography.[48] The district court had instructed the jury that possession was satisfied by "intentionally viewing images."[49] The circuit court ultimately upheld the jury instruction citing its own precedent that "possession 'necessarily' includes intentionally viewing child pornography, even if it is never downloaded."[50]

This interpretation is highly questionable. Both § 2252(a)(4)(B) and § 2252A criminalize any person who "knowingly possesses, or knowingly accesses with intent to view."[51] The disjunctive "or" indicates that these are two separate means of violating the statute. The circuit attempted to explain how its interpretation is consistent with two separate offenses by claiming "possession can include the completed act of 'intentionally viewing images,' which is different than having access and intent to view images but not actually viewing them."[52]

---

46. *See* sources cited *supra* note 41.

47. The statute criminalizes:

> [K]nowingly possess[ing], or knowingly access[ing] with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer . . . .

18 U.S.C. § 2252A(a)(5)(B) (2012). Minor distinctions from § 2252(a)(4)(B) include replacing "1 or more" with "any," and replacing "other matter" with "other material." *Id.*

48. United States v. Rivenbark, 748 F. App'x 948, 950 (11th Cir. 2018) (per curiam) (affirming conviction for possession under § 2252A(a)(5)(B)).

49. *Id.* at 957. Rivenbark argued that the jury instruction was effectively an amendment of the indictment, by instead charging he accessed with intent to view, rather than possessed, the child pornography. *Id.* at 956.

50. *Id.* at 956 (citing United States v. Woods, 684 F.3d 1045, 1059 (11th Cir. 2012)).

51. 18 U.S.C. §§ 2252(a)(4)(B), 2252A(a)(5)(B).

52. *Rivenbark*, 748 F. App'x at 957 ("The key distinction is that, to establish possession in this case, the government had to prove that Rivenbark actually viewed the child pornography. By contrast, under the 'access with intent to view' prong, the government had no such burden." (citation omitted)).

This interpretation misreads the statute, which convicts any person who "knowingly *accesses*" a material containing a visual depiction.[53] The plain reading of the statute is that "having access" is not sufficient to convict for access; the person must have actually accessed the material. The circuit's interpretation flips the plain meaning of the statute. The circuit's interpretation defining the access prong as "having access and intent to view" reads more like a common definition of "knowingly possesses."[54] The court's definition of possession—the "completed act of 'intentionally viewing images'"—instead reads more like a common definition of "knowingly accesses with intent to view."[55] The court may have flipped the natural meanings of the two provisions to avoid overturning the defendant's conviction. This result has expanded the definition of "possession" to include both the possession and access prongs.

Most circuits have not adopted such a broad interpretation of possession.[56] However, the circuits with narrow interpretations leave it unclear whether focus of the possession is on the matter containing the visual depictions or on the visual depictions themselves.[57] In *United States v. Little*, the Eleventh Circuit applied a standard definition of "constructive possession" against a defendant convicted of receipt and possession under § 2252(a)(4)(B).[58] The Eleventh Circuit noted that the child pornography images were stored on "external servers," but concluded it was possible for the jury to find "[the defendant] constructively possessed [the images] . . . even though he had received them in Texas and never actually accessed them while in Tampa."[59] The circuit did not address what qualified as the

53. 18 U.S.C. § 2252A(a)(5)(B) (emphasis added).

54. *Rivenbark*, 748 F. App'x at 957.

55. *Id.*

56. *See* cases cited *supra* note 12 and accompanying text.

57. *See* United States v. Vig, 167 F.3d 443, 448 (8th Cir. 1999); United States v. Hall, 142 F.3d 988, 998 (7th Cir. 1998); United States v. Lacy, 119 F.3d 742, 748 (9th Cir. 1997).

58. United States v. Little, 864 F.3d 1283, 1289 (11th Cir. 2017) ("Constructive possession is established when a person, though lacking such physical custody, still has the power and intent to exercise control over the object."). The circuit was faced with a venue problem. The defendant had received child pornography by e-mail in Texas and then moved to Tampa, Florida. Because the defendant was charged with possession in Tampa, the circuit had to determine whether the jury could reasonably conclude the defendant had possessed child pornography in Tampa specifically, and not just in Texas. *Id.* at 1287–88.

59. *Id.* at 1289. The circuit qualified this assertion by requiring intent to exercise control. *Id.* at 1289 n.2 ("We do not hold or mean to imply that a defendant possesses child pornography simply because he has an electronic device through which he can access an e-mail that has an image of it attached. Here there was also evidence from which a jury could reasonably find that Little, while in the district in which he was charged, had the intent to

"matter," and the language implies that the constructive possession was of the "visual depictions" themselves.[60]

The plain meaning of the statute requires possession of a matter that contains the visual depictions, not possession of the visual depictions directly. Especially in the context of cloud computing, which for many circuits will involve matters of first impression for a rapidly growing problem, the circuits should clearly state what qualifies as the "matter" so that it can be properly applied as precedent.

III. RE-INTERPRETING THE POSSESSION STATUTES

One alternative that would allow both the *Forrester* and *Little* decisions to stand is to define the "matter" or "material" as the external server.[61] Although it is clear that a defendant does not have actual possession of an external server,[62] certain definitions of "constructive possession" could plausibly cover the server. The Fifth Circuit defines "constructive possession" as "the ownership, dominion or control over an illegal item itself or dominion or control over the premises in which the item is found."[63] The second part of this definition seems well suited to § 2252(a)(4)(B). A court could reasonably construe that the premises is the external server

exercise active control over the attached images.").

60. The other possible interpretation is that the images themselves qualify as a "matter" under the statute. But this interpretation is even broader than that by the Eighth and Seventh Circuits qualifying computer "files" as the "matter." *See* cases cited *supra* note 23 and accompanying text. Such a broad interpretation also appears to conflict with the statute. Although there is not a statutory definition of "possession," there is a definition for "visual depiction." 18 U.S.C. § 2256(5) (2012) ("'[V]isual depiction' includes undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format."). The statutory definition of "child pornography" also includes an example of visual depiction as "a digital image, computer image, or computer-generated image" that further supports this interpretation. *Id.* § 2256(8). This precludes an interpretation of the images themselves as the "matter."

61. In *Forrester*, it is unclear if this is the conclusion that the Court of Appeals of the Armed Forces came to. The court noted that the defendant did not actually possess the external server, but did constructively possess the child pornography. It is possible the jump from possession of the "material" to possession of the child pornography directly was a mistake in wording. *See* United States v. Forrester, 76 M.J. 479, 486 n.7 (C.A.A.F. 2017) ("Though Appellant may not have physically controlled the server on which the child pornography within his e-mail account was located, he constructively possessed the child pornography by storing it and retaining the capacity to return to retrieve it.").

62. Even in *Little* where the circuit had an unusually broad definition of "constructive possession," it's definition of "actual possession" could not encompass a cloud storage user's possession of an external server. *Little*, 864 F.3d at 1288 ("Actual possession exists when a person has direct physical control over a thing.").

63. United States v. Villasenor, 236 F.3d 220, 222–23 (5th Cir. 2000).

(the "matter"), and the item is the visual depictions. A defendant could then have constructive possession of the images by exercising control over the server (the "premises") without actually possessing it.

An added benefit of this interpretation is that it does not require construing the definition of "matter" in a way that contradicts the tools of statutory interpretation. An external server is a "physical medium" that would satisfy the Ninth Circuit interpretation.[64]

This interpretation, however, has its flaws. First, the defendant does not have exclusive control over the external servers because cloud computers necessarily have joint control.[65] But, in the context of § 2252(a)(4)(B), this is not an insurmountable problem. The statute already requires knowing possession,[66] and the government has already tended to show the defendant's ability to access the cloud.[67]

A more serious problem is that data is often stored on multiple servers.[68] Assuming the cloud company can identify which server houses the data, the user likely does not know which server or servers are being used to store the data.[69] Although a user knows that he has control over *a* server, it is unclear if the statute would require he know exactly which server. The prosecution would have

64. *See* United States v. Lacy, 119 F.3d 742, 748 (9th Cir. 1997).

65. *See* United States v. De Leon, 170 F.3d 494, 497 (5th Cir. 1999) ("[C]ontrol over the place in which contraband or an illegal item is discovered is insufficient by itself in establishing constructive possession when there is joint occupancy of a place. We have found constructive possession in such cases only when there was 'some evidence supporting at least a plausible inference that the defendant had knowledge of and access to' the illegal item."), *cited in Villasenor*, 236 F.3d at 223 n.4.

66. 18 U.S.C. § 2252(a)(4)(B) (2012) (using the phrase, "[a]ny person who *knowingly* possesses." (emphasis added)).

67. *See* United States v. Forrester, 76 M.J. 479, 486 (C.A.A.F. 2017) (linking the data on the external server to the defendant's Gmail account); *see also Little*, 864 F.3d at 1289 (similarly linking the data on the server to the defendant's e-mail account).

68. In fact, storing data on multiple servers is one of the selling points of cloud storage because of the concept of "redundancy." The more places your data is stored, the more secure it is in the event of a failure at one location. Microsoft Azure's cloud pricing allows businesses to pay extra so that their data is stored in multiple locations around the world. *Disaster Recovery and Account Failover (Preview)*, MICROSOFT AZURE (Jan 23, 2020), https://docs.microsoft.com/en-us/azure/storage/common/storage-disaster-recovery-guidance?toc=%2fazure%2fstorage%2fqueues%2ftoc.json [https://perma.cc/5LXR-B7KU]. If you choose geo-redundant storage, Azure Storage will keep your data durable in two regions (primary and secondary). In both regions, Azure Storage constantly maintains multiple replicas of your data. *Id.*

69. This is especially problematic for the purposes of § 2252A(a)(5)(B) because, unlike § 2252(a)(4)(B), it allows for multiple counts of possession in the same transaction. *See supra* note 41. Convicting a defendant on multiple counts for possession on multiple servers leads to serious concerns where the defendant had no control over what servers were used.

to identify which server is controlled to establish constructive possession, which is difficult in the cloud computing context. As with all criminal statutes, if this is found to be ambiguous, the courts will necessarily resolve the issue in favor of the defendant.[70] If the courts find this to be an unreasonable interpretation, Congress can always amend the statute.[71]

IV. SOLUTIONS TO THE FEDERAL CHILD PORNOGRAPHY POSSESSION STATUTE

A. Looking to State Child Pornography Statutes

Most states have not adopted the federal statute's unusual requirement of possession of a "matter" that contains the "visual depiction."[72] Although similar to the federal statutes, most states chose to criminalize possession of visual depictions directly.[73] This has at least partially reduced the difficulty of applying possession statutes to the cloud computing context. However, even among states that follow this statutory scheme, courts have had difficulty applying possession to the cloud.[74]

In *State v. Linson*, the South Dakota Supreme Court was faced with a defendant charged with multiple counts of possession of child pornography after images were found in his internet cache.[75] Under the federal statute, the defendant would have to be charged with only a single count of possession for his computer. However, under South Dakota state law, which criminalizes possession of the visual depictions directly, the state supreme court found he could be charged with multiple counts.[76] The court

70. Johnson v. United States, 135 S. Ct. 2551, 2556–57, 2562 (2015) ("The prohibition of vagueness in criminal statutes 'is a well-recognized requirement, consonant alike with ordinary notions of fair play and the settled rules of law,' and a statute that flouts it 'violates the first essential of due process.'" (citation omitted)).

71. *See supra* note 43 and accompanying text.

72. *See supra* note 15 and accompanying text.

73. *Id.*

74. State v. Linson, 896 N.W.2d 656, 660–62 (S.D. 2017).

75. *Id.* at 658.

76. *Id.* at 660, 664–65. The South Dakota Supreme Court was faced with its own statutory deficiency, as the state statute criminalizes possession, but not accessing with the intent to view. *Id.* at 660. The court noted that under § 2252(a)(5)(B), a federal prosecutor could use evidence of the cache files to charge accessing with an intent to view. The South Dakota Court followed the reasoning that the combination of the cache files located on the computer, as well as evidence of search terms related to child pornography, could lead a jury to reasonably conclude that the defendant at some point "knowingly" possessed the child pornography on this computer. *Id.* at 660–63 ("Drawing a line between the mere viewing of images on a potentially mobile electronic device such as a computer and possessing those images highlights the difficulty of applying older legal concepts rooted in

did note that to satisfy the "knowing possession" element, evidence of the cache files alone was insufficient.

In the context of cloud computing, a possession conviction would likely be simpler. If the cloud user has exclusive control over the cloud storage account, it seems that knowledge could be reasonably inferred if child pornography were found on the account. Unlike with an automatic cache system where the "knowledge" prong is not easily satisfied due to the automatic storing of the files in the cache,[77] storage on the cloud presumably requires a conscious decision by the user. However, for accounts that regularly share the files, as is common,[78] the prosecution would again face similar difficulties of proving "knowing" possession.[79]

When state courts have addressed cloud computing, they have similarly come to the conclusion that storage on the cloud alone, without evidence that the defendant knowingly stored the child pornography, is insufficient.[80] Much like South Dakota, New York state law does not require possession of a separate matter that contains child pornography to support a possession conviction, instead criminalizing possession of the depictions directly.[81] However, because of the "knowing" requirement, New York courts require more than mere possession: "In the case of digital images and videos . . . [t]here must be some 'affirmative act,' such as printing, saving or downloading, to establish [possession]."[82] While

---

a brick-and-mortar world to today's virtual world.").

77. Applying the possession statute to child pornography files found in the cache has led to similarly complex caselaw, as courts have struggled to determine whether the defendant "knowingly" possessed or received the files. *See* Katie Gant, *Crying over the Cache: Why Technology Has Compromised the Uniform Application of Child Pornography Laws*, 81 FORDHAM L. REV. 319, 336–38 (2012) (discussing the variety of methods courts have employed when determining whether and what evidence is needed in addition to the cached images to satisfy the "knowing" prong of the federal child pornography statute).

78. For example, Apple advertises iCloud's capabilities for shared storage between family members. *Share an iCloud Storage Plan with Your Family*, APPLE, https://support.apple.com/en-us/HT208147 [https://perma.cc/HWF8-FF4H] (last visited Dec. 22, 2019).

79. *See supra* note 77 and accompanying text; *see also infra* note 109 and accompanying text.

80. People v. Henry, 166 A.D.3d 1289, 1290–92 (N.Y. App. Div. 2018) (relying on evidence that the defendant had "recently accessed" the child pornography to satisfy the "knowing" requirement of possession).

81. N.Y. PENAL LAW § 263.16 (McKinney 2012) ("A person is guilty of possessing a sexual performance by a child when, knowing the character and content thereof, he knowingly has in his possession or control, or knowingly accesses with intent to view, any performance which includes sexual conduct by a child less than sixteen years of age."). Similar to federal law, the statute allows for a conviction of possession *or* accessing with intent to view. *See* 18 U.S.C. § 2252(a)(4)(B) (2012).

82. *Henry*, 166 A.D.3d at 1290.

the affirmative act is considered necessary to demonstrate that the possession is knowing, this complicates possession charges in the cloud computing context. Although cloud companies readily scan for and report child pornography that is stored in user accounts,[83] they may be less readily able to link the act of uploading or downloading to a particular individual if more than one person has access to an account or shared Wi-Fi.[84] In *People v. Henry*, while the possessed images were linked to the defendant's Windows Live account, the uploading and downloading was linked to an IP address that, he argued, was shared with his roommate.[85] The IP address alone is likely insufficient to establish knowing possession by an individual as an IP address is often used by multiple persons.[86] Therefore, states have generally still required an act of uploading or downloading to an electronic device to establish possession.[87]

B. Looking to Other Areas of Law

Child pornography is not the only area of law where cloud computing has been problematic. Copyright law and its attempts to address the explosion of piracy may provide insight for a potential rewrite of the federal child pornography statute.[88] The Digital Millennium Copyright Act (DMCA) contains a "safe harbor" provision that protects service providers from

83. *See supra* note 36.

84. In *Henry*, the prosecution established exclusivity regarding his account by presenting evidence to show the defendant had changed the default setting in his Windows Live account to prevent others from accessing it. *Henry*, 166 A.D.3d at 1292.

85. *See Henry*, 166 A.D.3d at 1290–91 (noting that Microsoft was able to provide police with the IP address from which the images were uploaded to its cloud storage service). The defendant argued others with access to his Wi-Fi may have accessed the images. *Id.*

86. Patrick Collins, Inc. v. Doe 1, 288 F.R.D. 233, 235 (E.D.N.Y. 2012) ("An IP address is a 'numeric label[ ] specific to a computer network that serve[s] to identify and locate that network on the Internet, but not to further identify the defendant. In fact, a single IP address may host one or more devices operated or owned by multiple users . . . .'" (alterations in original) (quoting Media Prods., Inc. v. Does 1-26, No. 12 Civ. 3719, 2012 WL 3866492, at *1 (S.D.N.Y. Sept. 4, 2012))). In *Henry*, that burden was overcome by evidence of the defendant's access to the images found on his personal laptop. *Henry*, 166 A.D.3d at 1292.

87. *Doe 1*, 288 F.R.D. at 235; *see also Henry*, 166 A.D.3d at 1292 (noting the prosecution had linked accessing of the images to the defendant's personal laptop).

88. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of U.S.C.). A common issue is whether service providers such as cloud storage companies may be liable for possessing infringing materials. *See* Ventura Content, Ltd. v. Motherless, Inc., 885 F.3d 597, 600–01 (9th Cir. 2018) (dealing with a civil case of a copyright owner suing a service provider for copyright infringement after users uploaded and stored the infringing material onto the service).

infringement when they unknowingly and temporarily possess the infringing materials.[89] However, if the requirements of the provision are not met, the service provider may be liable for civil damages to the copyright owner. A similar statutory provision could be added in the child pornography context to increase the burden on the cloud storage companies by subjecting them to potential civil liability, if not criminal.[90] However, such a provision presents several problems. First, unlike in the copyright context where the burden is on the copyright owner to bring a DMCA claim, it's unclear what third party would bear the burden of bringing civil charges for storage of child pornography. Second, cloud companies already go beyond existing statutory requirements in assisting federal prosecutors in identifying users who upload child pornography.[91]

C. Looking to Other Child Pornography Charges

One potential solution is to better strategize how to properly charge a cloud storage user with violating the federal child pornography statute. Although possession is often the charge that has arisen with cloud computing, it is far from the only applicable charge.[92] However, as a result of the fast pace of technological change, prosecutors may be reluctant to bring charges related to child pornography and the cloud under untested statutes.[93] As the caselaw develops, these additional options will likely allow for effective criminal prosecution for child pornography stored on the

89. 17 U.S.C. § 512(b)(1) (2012) ("A service provider shall not be liable for monetary relief, or, . . . for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider . . . .").

90. *See supra* note 36 and accompanying text.

91. Cloud companies are already required to report a user if the company obtains actual knowledge that the user is abusing the cloud storage service to keep child pornography. 18 U.S.C. § 2258A(a). However, this requires the companies to report only if they come across the child pornography, not to actively search for it. In fact, the companies note that their user agreements allow them to actively scan all files for child pornography, and they regularly do so. *See* Julie Bort, *Microsoft Tipped off Authorities to a Man Allegedly Storing Explicit Photos of Children in the Cloud*, BUS. INSIDER (Aug. 7, 2014), https://www.businessinsider.com/microsoft-scans-cloud-for-child-porn-2014-8 [https://perma.cc/ZYK3-ZVF6].

92. *See infra* Sections IV.C.1–.2 (discussing how other charges could be applied).

93. This problem for federal prosecutors is further complicated by the fact that there are two similar child pornography statutes, each with their own lines of caselaw. *See supra* note 47 and accompanying text. These separate statutes have already created issues with the Fifth Amendment, as multiple convictions are permissible under § 2252A(a)(5)(B), but would violate the double jeopardy clause under the nearly identical § 2252(a)(4)(B). *See supra* note 41. All of these considerations must be made on top of the varying sentences that accompany each charge.

cloud. Starting with § 2252(a)(4)(B) and § 2252A(a)(5)(B), prosecutors have the option to charge knowing possession "or" accessing with intent to view child pornography.[94] The courts frequently misquote the statutes as requiring that the defendant "knowingly possess and knowingly access with intent to view child pornography."[95] In *Busching v. United States*, the defendant pled guilty after he used his home computer to access more than 600 images of child pornography stored in his Dropbox account.[96] Although the two are interrelated because, as noted above, to prove possession in the cloud computing context, states regularly require additional evidence such as downloading and saving,[97] they could be prosecuted separately.[98]

The dual application of either accessing or possessing child pornography allows federal prosecutors flexibility to avoid many of the difficulties faced by state prosecutors under state statutes.[99] Many of the possession issues discussed above may be resolved if the cloud computing companies can provide data on when a particular user accessed the files.[100]

Federal statutes criminalize several activities related to child pornography beyond the possession and access prong, including

---

94. *See* 18 U.S.C. §§ 2252(a)(4)(B), 2252A(a)(4)(B).

95. Busching v. United States, No. TDC-15-0107, 2018 WL 3546720, at *1 (D. Md. July 24, 2018).

96. *Id.* As part of his plea agreement, Busching was charged with only one count of accessing with intent to view instead of the initial three counts in the indictment. *Id.* at *2. The two dismissed counts concerned Busching's creation of two additional Dropbox accounts that he then shared links to with users he met on the video chatting service Omegle. *Id.* at *1.

97. *See supra* note 82 and accompanying text.

98. That the two are conflated likely arises from the reality that a common method to establish "knowing" possession is to show that the defendant accessed the files and is therefore aware they contain child pornography. *See supra* notes 48–55 and accompanying text (discussing efforts to distinguish between possession and accessing with intent to view in the context of cloud computing).

99. *See supra* note 76. Other states that criminalize possession, but not accessing with intent to view, have run into similar issues. In *New v. State*, a defendant in Georgia was convicted of possession of child pornography under Georgia state law, even though the forensics experts were unable to determine whether the files were generated after downloading the images from a peer-to-peer network or viewed on a website. New v. State, 755 S.E.2d 568, 574 (Ga. Ct. App. 2014). The court, in effect, defined possession broadly to include accessing with intent to view. *Id.* at 575–76 ("[A] computer user who intentionally accesses child pornography images on a website 'gains actual control over the images, just as a person who intentionally browses child pornography in a print magazine "knowingly possesses" those images, even if he later puts the magazine down.' In this way, any backup or residual files become *evidence of* possession at a prior point; the files need not represent the literal contraband." (emphasis added) (quoting United States v. Kain, 589 F.3d 945, 950 (8th Cir. 2009))).

100. However, there continue to be issues providing evidence linking the defendant to the act of accessing the files. *See supra* note 85 and accompanying text.

transportation, production, distribution, receipt, and sale of child pornography.[101]

1. Transportation of Child Pornography. Under § 2252(a)(1), there is no requirement that any "matter" be transported or shipped, instead requiring transportation of the visual depictions directly.[102] Transportation may be a useful charge, as all provisions of the federal child pornography statutes require the visual depictions to be transported in interstate commerce for federal law to apply anyway.[103] The distinction with the other provisions is that the defendant's transportation of the visual depictions across state lines must be "knowing."[104] This would allow for users who upload child pornography into their cloud accounts to be prosecuted for transportation, without the legal ambiguity of whether they are in possession of that child pornography once it is uploaded and located exclusively on the cloud.[105] In practice, this may be limited by the reality that if the

101. 18 U.S.C. §§ 2252(a)(1)–(4), 2252A(a)(1)–(5) (2012).

102. *Id.* § 2252(a)(1) ("Any person who knowingly transports or ships . . . any visual depictions . . . ."); *see also id.* § 2252A(a)(1) ("Any person who knowingly mails, or transports or ships . . . including by computer, any child pornography . . . .").

103. *Id.* §§ 2252(a)(1)–(4), 2252A(a)(1)–(5). The statutes further indicate that the transportation may occur via computer. *Id.* Although sending images via the internet is well established as constituting interstate commerce, the circuits have developed their own caselaw for what evidence is required under the child pornography statutes. This was problematic in early years under the wording of the child pornography statutes, because federal prosecutors were uncertain whether it must be the "matter" or the visual depictions that travel in interstate commerce. *See* United States v. Wilson, 182 F.3d 737, 743–44 (10th Cir. 1999) ("We also find untenable the prosecution's theory that only the 'matter' must have traveled in interstate commerce. In our view, the language of § 2252(a)(4)(B) makes it abundantly clear that either the visual depictions (in this case the graphics files) or the materials used to produce the visual depictions must have traveled in interstate commerce."); *see also* United States v. Henriques, 234 F.3d 263, 266 (5th Cir. 2000) (adopting the Tenth Circuit's position in *Wilson* and applying it to the sister statute, § 2252A). *But cf.* United States v. Cotterman, 709 F.3d 952, 958–59 (9th Cir. 2013) (allowing charges relating to the "matter" when the child pornography is already on the computer, and the computer itself is taken across state lines).

104. 18 U.S.C. §§ 2252(a)(1), 2252A(a)(1). For the other charges, such as possession, only the possession of the visual depictions must be knowing. It is not necessary to show that the defendant was aware the visual depictions traveled in interstate commerce.

105. The courts have come to the conclusion that because the internet is so interstate in nature, the act of uploading and downloading to and from the internet is inherently a transmission in interstate commerce. *See* United States v. MacEwan, 445 F.3d 237, 244 (3d Cir. 2006) ("Because of fluctuations in the volume of Internet traffic and determinations by the systems as to what line constitutes the 'Shortest Path First,' a website connection request can travel entirely intrastate or partially interstate. Regardless of the route taken, however, we conclude that because of the very interstate nature of the Internet, once a user submits a connection request to a website server or an image is transmitted from the website server back to [the] user, the data has traveled in interstate commerce."). Evidence that the user knowingly uploaded the data to the cloud is then sufficient to demonstrate

images are not also located on an individual's computer, it is difficult to prove beyond a reasonable doubt that the defendant was the one to transport the visual depictions.[106] If the images were located on the computer, then a charge for possession becomes relatively simple as the computer would be the "matter," and the transportation charge would be unnecessary.[107] Prosecutors may have an easier time with cloud computing than other issues because most users link their accounts to an e-mail address and cell phone number, providing evidence linking the account to a defendant.[108]

As cloud computing has grown exponentially, the issue of "knowing" transportation has become more problematic where devices may automatically upload data to the cloud. Several companies have begun using cloud storage to allow users to access the same data from their phone, computer, or wherever they login to the service.[109] Although there are obvious commercial benefits in using the cloud to allow users to access content regardless of the device used, it creates problems for the "knowing" component of the federal pornography statutes. If a device uploads or backs up visual depictions by default, it is not clear that the user "knowingly" transported the visual depictions. Should the user later delete the visual depictions from the drive itself but leave the depictions on the cloud, a possession charge may be the only option. Although the user would not knowingly possess the visual depictions on the cloud, that data could be used to prove the user knowingly possessed the visual depictions at an earlier time on their device.[110]

---

the transportation was knowingly in interstate commerce.

106. *See supra* note 86 and accompanying text. If the only information that can be provided by the cloud company is the IP address, it may be insufficient to link to the defendant, especially where more than one individual uses the IP address, as with shared Wi-Fi.

107. Although the government could bring multiple charges, the courts have developed another line of caselaw determining whether multiple violations under different portions of the statute violate the double jeopardy clause. *See infra* note 113.

108. *See* United States v. Chilaca, 909 F.3d 289, 291 (9th Cir. 2018) (defendant was identified after Dropbox discovered the child pornography in his account and provided the cell phone number and e-mail address linked to the account).

109. Joe Belfiore, *Your Windows 10 PC Will Love All the Devices You Own*, WINDOWS BLOGS (May 26, 2015, 5:01 AM), https://blogs.windows.com/windowsexperience/2015/05/26/your-windows-10-pc-will-love-all-the-devices-you-own/ [https://perma.cc/4Y5R-6PZ4] ("All your files and content will be magically available on your PC and your phone: [w]ith the OneDrive app setup correctly on your phone, every photo you take on your phone will show up automatically in the Photos app on your Windows 10 PC.").

110. This would be very similar to how prosecutors have used evidence of cached images to prove possession of child pornography discussed above. *See supra* notes 74–79 and accompanying text.

2. Receipt or Distribution of Child Pornography. The federal statutes also apply to the receipt and distribution of child pornography.[111] Receipt and distribution are distinct from possession because both acts involve interaction with another party, and a conviction therefore generally results in a greater sentence.[112] An important consideration for prosecutors is that possession is considered by most courts to be a lesser included offense of receipt or distribution.[113] Caselaw regarding the distribution of child pornography is well developed, as the sentencing guidelines have allowed for a sentencing enhancement for a possession conviction when distribution is also shown.[114] The caselaw is generally consistent on what is required for "distribution," and it is well suited to cloud computing. [115] The courts hold that granting access to files containing visual depictions is sufficient to satisfy the "distribution" requirement, and the defendant does not need to be the actor transferring the files for distribution to be established.[116] By intentionally making a cloud drive available for others to access, a user may then be

111. The provision is materially identical to the possession and transportation provisions, replacing the phrase "knowingly possesses" with "knowingly receives, or distributes." 18 U.S.C. §§ 2252(a)(2), 2252A(a)(2) (2012).

112. A conviction for possession has a maximum sentence of ten years (or twenty years if the depicted child is under twelve years of age), while a conviction for distribution, transportation, or sale has a maximum sentence of twenty years (or forty years if the depicted child is under 12 years of age). *Id.* § 2252(b)(1)–(2).

113. *See* United States v. Benoit, 713 F.3d 1, 13 (10th Cir. 2013) (striking down convictions for both receipt and possession of child pornography after concluding that possession is a lesser included offense of receipt); *see also* United States v. Ehle, 640 F.3d 689, 694 (6th Cir. 2011) ("There is a double jeopardy violation in . . . convictions for both receiving and possessing the same child pornography.").

114. U.S. SENTENCING GUIDELINES MANUAL § 2G2.2(b)(1)–(3) (U.S. SENTENCING COMM'N 2016). *See also* United States v. Montañez-Quiñones, 911 F.3d 59 (1st Cir. 2018), (discussing the history of the distribution guidelines, and the difficulty courts have had in applying the guidelines to new technologies), *cert. denied*, 139 S. Ct. 1388 (2019).

115. That the caselaw is developed largely in the sentencing context is not problematic, as the courts have generally not distinguished between distribution for sentencing and distribution under the criminal statute. *See* United States v. Ryan, 885 F.3d 449, 453 (7th Cir. 2018) ("There is no reason why [the definition of distribute for sentencing] should not apply when interpreting 'distribute' in the criminal statute.").

116. The First Circuit has held that by allowing others to access files on a peer-to-peer network, the distribution requirement is met. United States v. Chiaradio, 684 F.3d 265, 282 (1st Cir. 2012) ("When an individual consciously makes files available for others to take and those files are in fact taken, distribution has occurred."). Pre-2016 versions of the sentencing guidelines did not explicitly require that the distribution be knowing, and some circuits required no intent for the sentencing enhancement. *Montañez-Quiñones*, 911 F.3d at 69 (Lipez, J., concurring) ("[T]he circuits were split on whether the enhancement required some mens rea despite the absence of language to that effect in the guideline."). Due to concerns about individuals not understanding the technology they were using leading to enhanced sentences, the guidelines were amended to require "knowing distribution." U.S. SENTENCING GUIDELINES MANUAL, *supra* note 114, § 2G2.2(b)(3)(F).

liable for distribution. In *Busching*, the defendant was indicted on three counts of possession of child pornography, with counts two and three concerning links to two of his Dropbox accounts that he provided to others he met on video chatting sites.[117] Although Busching did not distribute the visual depictions, the caselaw indicates prosecutors could have instead charged him with distribution for "mak[ing] files available for others to take."[118]

In Busching's case, that he "knowingly" distributed the child pornography was not in doubt as he admitted to intentionally creating links to the files that he then shared with others.[119] But, for many users who do not understand how the cloud functions and whether the files are accessible to others, liability is less straightforward. For visual depictions shared using peer-to-peer networks, courts have required the defendant "ha[ve] knowledge that by using a peer-to-peer file-sharing program, his child pornography was made accessible to others."[120] In practice, this requirement was loose, as courts have found that use of a peer-to-peer network can be circumstantial evidence proving the defendant is technologically savvy enough to have knowledge their depictions are accessible to others.[121] That is less apparent for cloud computing, especially for users who have depictions uploaded to the cloud by default.[122] Prosecutors would need additional evidence to demonstrate that the user who made the cloud files accessible did so knowingly.

The applicability of a distribution charge is then going to be fact-specific to the individual cloud user. The clearest benefit for prosecutors is that individuals who store and view child pornography exclusively on the cloud without downloading to a device may still be criminally liable if they share those files.[123] Most problematic for prosecutors would be providing evidence to

117. Busching v. United States, No. TDC-15-0107, 2018 WL 3546720, at *1 (D. Md. July 24, 2018); *see also supra* notes 95–96 and accompanying text.

118. *Chiaradio*, 684 F.3d at 282.

119. *Busching*, 2018 WL 3546720, at *1.

120. United States v. Cates, 897 F.3d 349, 359 (1st Cir. 2018).

121. *Id.* at 359 ("Although it is possible that a user might not know about [the peer-to-peer network's] file-sharing properties, the defendant was no Luddite. After installing the program, he used it to download child pornography for roughly three years before his arrest.").

122. *See supra* note 109 and accompanying text.

123. For example, in *Wilson*, the defendant was indicted for distribution of child pornography primarily by sharing links to her Dropbox accounts even without finding the images on any of her personal electronic devices. United States v. Wilson, 217 F. Supp. 3d 165, 167–72 (D.D.C. 2016). That possession is a lesser included offense of receipt and distribution indicates she could also be indicted for possession.

establish that another user in fact accessed the files stored on the cloud, and that the defendant knowingly provided access.[124]

V. CONCLUSION

Current federal child pornography law is complicated and outdated. Federal prosecutors are left to navigate two nearly identical criminal statutes with separate and conflicting lines of caselaw. The possession statute's requirement that a defendant possess "matter" which contains child pornography is an unnecessary vestige of previous child pornography statutes that emphasized production and distribution of child pornography over possession. This has left courts struggling to interpret what qualifies as "matter," and thus, the existing definition often excludes digitally stored data such as what exists on the cloud. Finally, there are several potential chargeable offenses, each with separate lines of caselaw. This leaves federal prosecutors in the position that when an individual possesses child pornography on the cloud, the charges filed will depend heavily on the jurisdiction and circuit where they are filed. There are solutions in the statute itself, and some circuits have already begun readjusting judicial interpretations to adapt them to new technologies like cloud computing. While these new interpretations may assist in holding possessors of child pornography liable as they increasingly use these new technologies, a rewrite of the statute is likely the only proper solution for these technological changes.

Dylan Carroll

124. In *Wilson*, this evidence was obtained as part of a sting operation with an undercover police officer. *Id*. at 168.