Seattle Journal of Technology, Environmental & Innovation Law

Volume 13 | Issue 2 Article 4

5-6-2023

From Hashtag to Hash Value: Using the Hash Value Model to Report Child Sex Abuse Material

Jessica McGarvie
jmcgarvie@seattleu.edu

From Hashtag to Hash Value: Using the Hash Value Model to Report Child Sex Abuse Material

Jessica McGarvie[1]

I. INTRODUCTION

"Just how you can go find a car—it was a picture, a description, and a price."[2] Approximately 500 Child Sex Abuse Materials (CSAM), also known as child pornography, will be traded online roughly every sixty seconds.[3] The proliferation of CSAM has continued in the last fifteen years, and the problem was only accelerated by the rise of the internet and social media.[4] A study by Thorn, an international anti-human trafficking organization, found that 70% of child sex trafficking victims were sold online.[5]

As a result, major tech media companies, such as Google, Microsoft, and Meta (formerly known as Facebook), have been scanning for CSAM on their platforms for years.[6] Apple, on the other hand, did not have anything similar in place.[7] In fact, around 2019, the National Center

[1] Juris Doctorate Candidate 2023, Seattle University School of Law. Thank you to my grandmother, Ann "Grammar Queen" Chang, who sparked my love for writing and never fails to correct my grammatical or spelling errors—even in text messages. A very special thank you to Professor Annette L. Hayes, a career federal prosecutor who has experience prosecuting CSAM cases firsthand and was so gracious to help me edit this article. Lastly, thank you to my fiancé, Joshua Lowthorp, who tirelessly supports me in all my endeavors, including this one.

[2] Thorn, *We Are Thorn.*, YOUTUBE (Nov. 14, 2013), https://www.youtube.com/watch?v=Se4OvAGJu4U&ab_channel=Thorn [https://perma.cc/35GF-WEFZ].

[3] Microsoft Digital Crimes Unit, *Microsoft PhotoDNA Cloud Service*, YOUTUBE (July 14, 2015), https://www.youtube.com/watch?v=4TCj40IZHdk&t=2s&ab_channel=MicrosoftDigitalCrimesUnit [https://perma.cc/V3F7-K6ZD].

[4] *Technology Has Made It Easier To Harm Kids.*, Thorn, https://www.thorn.org/child-sexual-exploitation-and-technology/ [https://perma.cc/4KP3-88B8] (last visited Feb. 6, 2022, 10:00 PM); Thorn, *supra* note 2.

[5] Thorn, *supra* note 2.

[6] Joanna Stern, *Apple's Child-Protection Features and the Question of Who Controls Our Smartphones*, THE WALL STREET JOURNAL (Aug. 13, 2021), https://www.wsj.com/articles/apple-child-protection-features-11628861782?mod=searchresults_pos3&page=1 [https://perma.cc/ZHS6-2KEV]. *See* Tracy Ith, *Microsoft's PhotoDNA: Protecting children and businesses in the cloud*, MICROSOFT (July 15, 2015) https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/ [https://perma.cc/N84G-KLBQ] (Microsoft has used the technology since 2015); Paul Sawers, *Google releases AI-powered Content Safety API to identify more child abuse images*, VENTUREBEAT (Sept. 3, 2018), https://venturebeat.com/ai/google-releases-ai-powered-content-safety-api-to-identify-more-child-abuse-images/ [https://perma.cc/BLZ5-QZV7] (Google has used this technology since 2018); Casey Newton, Facebook open-sources algorithms for detecting child exploitation and terrorism imagery, THE VERGE (Aug. 1, 2019), https://www.theverge.com/2019/8/1/20750752/facebook-child-exploitation-terrorism-open-source-algorithm-pdq-tmk [https://perma.cc/RY68-BUU9] (Facebook has used this technology since 2019).

[7] Michael H. Keller & Gabriel J.X. Dance, Child Abusers run Rampant as Tech Companies Look the Other Way, NEW YORK TIMES (Nov. 9, 2019), https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html [https://perma.cc/GQ28-LSDA].

for Missing & Exploited Children (NCMEC) released a report documenting how often tech companies reported cases of CSAM on their platforms.[8] Apple was relatively low on the list compared to other similarly prominent tech companies.[9] The inattentiveness of Apple prompted members of Congress to demand that Apple do more to combat the issue.[10] In response, Apple announced two Child Safety Features in August of 2021.[11] The more controversial of the two would scan an Apple user's photos that were backed up to iCloud for CSAM ("CSF" or "Feature").[12] After these Child Safety Features were announced, intense backlash among the public, privacy experts, politicians, and even Apple employees followed regarding the Fourth Amendment and privacy implications.[13]

The Hash Value Model (HVM) technology used in Apple's CSF does not violate the Fourth Amendment and maintains a user's privacy; however, guidance on how to gather evidence of CSAM using the HVM in criminal prosecution must be clarified to remedy the circuit split throughout the United States. Part I describes the mechanics of the HVM and explores how Apple and other tech companies use it to combat CSAM. Part II provides a history of the Fourth Amendment's intersection with technology and discusses two cases that illustrate the current circuit split on how to gather evidence in CSAM cases using the HVM legally. Finally, Part III addresses common critiques of Apple's CSF and proposes three solutions to the current circuit split.

II. BACKGROUND

A. CSAM and the Reporting Process

[8] NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN, 2019 REPORTS BY ELECTRONIC SERVICE PROVIDERS 1 (2019), https://www.missingkids.org/content/dam/missingkids/pdfs/2019-reports-by-esp.pdf [https://perma.cc/6JRN-XX6S].

[9] *Id.*

[10] *Id.*; *See* @mhkeller, TWITTER (Nov. 19, 2019, 7:53 AM), https://twitter.com/mhkeller/status/1196818679683530752 [https://perma.cc/3PGX-HYCS].

[11] Tatum Hunter, *Apps offer teens some one-and-done settings to stay safer online*., THE WASHINGTON POST (Nov. 3, 2021), https://www.washingtonpost.com/technology/2021/11/03/social-media-safety-teens/ [https://perma.cc/F23D-26J6].

[12] Tom Rolfe, *Child Safety on iOS—Apple walks back photo-scanning plans*, TAPSMART (Dec. 9, 2022), https://www.tapsmart.com/news/child-safety-ios/ [https://perma.cc/GV2F-VPPC].

[13] Kellen Browning, *Cybersecurity Experts Sound Alarm on Apple and E.U. Phone Scanning Plans*, THE NEW YORK TIMES (Oct. 14, 2021), https://www.nytimes.com/2021/10/14/business/apple-child-sex-abuse-cybersecurity.html [https://perma.cc/4SKD-9HYV]; Gordon Kelly, *Snowden Slams Apple CSAM: Warns iPad, iPhone, Mac Users Worldwide*, FORBES (Apr. 28, 2021), https://www.forbes.com/sites/gordonkelly/2021/08/28/apple-iphone-warning-csam-threat-edward-snowden-upgrade-ios-15-privacy/?sh=29991ef71978 [https://perma.cc/PYJ3-7VME]; *Apple criticism from the Bundestag*, IFUN (Aug. 18, 2021), https://www.ifun.de/apple-kritik-csam-bundestag-174310/ [https://perma.cc/HSL2-G448]; Julia Love, *Apple's child protection features spark concern within its own ranks*, REUTERS (Aug. 12, 2021), https://www.reuters.com/technology/exclusive-apples-child-protection-features-spark-concern-within-its-own-ranks-2021-08-12/ [https://perma.cc/4PGD-73R4].

1. What is CSAM and What Images Qualify?

Title 18 of the US Code defines "child pornography" as any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.[14] Federal law prohibits the production, distribution, importation, reception, or possession of CSAM, and possession can result in fines or up to thirty years in prison.[15] It also prohibits anyone outside of the United States from knowingly producing, receiving, transporting, shipping, or distributing child pornography with intent to import or transmit the visual depiction into the United States.[16] Unfortunately, in the year 2020 alone, 21.7 million reports of suspected CSAM were made to NCMEC, breaking the record for the highest number of reports ever received in one year.[17]

2. Reporting CSAM Using the Hash Value Model

The HVM is the primary way tech companies scan for CSAM.[18] A "hash value" is often likened to a digital fingerprint.[19] When an image is uploaded to a platform, an algorithm of complex calculations, commonly known as MD5 or SHA-1, is executed and generates a unique, fixed-length string that represents the photo's hash value.[20] In the simplest of terms, the algorithm converts the photo into a unique set of numbers and letters that can identify copies of the photo without actually viewing it.[21] The HVM is a departure from how CSAM was previously detected, which involved manually searching through images.[22]

[14] 18 U.S.C. § 2256(8)(A).

[15] *Guide To U.S. Federal Law On Child Pornography*, THE UNITED STATES DEPARTMENT OF JUSTICE (May 8, 2020), https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography [https://perma.cc/DJ3E-JVK2].

[16] *Id.*

[17] Brenna O'Donnell, *NCMEC Releases 2020 Exploitation Stats*, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN (Feb. 24, 2021), https://www.missingkids.org/blog/2021/rise-in-online-enticement-and-other-trends--ncmec-releases-2020- [https://perma.cc/6YJ3-ASPJ].

[18] Sarah Perez, *Why The Gmail Scan That Led To A Man's Arrest For Child Porn Was Not A Privacy Violation*, TECHCRUNCH (Aug. 6, 2014) https://techcrunch.com/2014/08/06/why-the-gmail-scan-that-led-to-a-mans-arrest-for-child-porn-was-not-a-privacy-violation/ [https://perma.cc/93A7-6WT5].

[19] *Introduction to Hashing: A Powerful Tool to Detect Child Sex Abuse Imagery Online*, THORN (Apr. 12, 2016), https://www.thorn.org/blog/hashing-detect-child-sex-abuse-imagery/ [https://perma.cc/WD72-9S7L].

[20] *What is Hashing?*, SENTINEL ONE, https://www.sentinelone.com/cybersecurity-101/hashing/ [perma.cc/ZYN2-DDAY] (last visited Feb. 6, 2022, 10:00 PM).

[21] Tyler O'Connell, *Two Models Of The Fourth Amendment And Hashing To Investigate Child Sexual Abuse Material*, 53 U. PAC. L. REV. 293, 301 (2021).

[22] Tracy Ith, *Microsoft's PhotoDNA: Protecting children and businesses in the cloud*, MICROSOFT (July 15, 2015) https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/ [https://perma.cc/N84G-KLBQ].

Once a hash value has been generated for an image, it will go through a database of known CSAM, often put together by other platforms and child-safety organizations, including the NCMEC.[23] This process helps prevent, for example, innocent images of naked children in bathtubs taken by parents from being reported to NCMEC because these bathtub images would not be in the CSAM database.[24] Depending on the platform, when an image is flagged, a content moderator for the tech company might view the actual image to ensure it is, in fact, CSAM.[25]

3. National Center for Missing and Exploited Children and Their Role

Once CSAM has been detected on a platform, the tech company is required by federal law to report it to authorities.[26] NCMEC is often the liaison between tech companies reporting CSAM and authorities.[27] Upon receiving a CSAM tip, NCMEC will review it, perform follow-up research on the reported individual, and cross reference the tip with other tips to identify serial CSAM predators.[28] The NCMEC will then turn it over to law enforcement, who handle the remainder of the investigation.[29]

The NCMEC is a private, non-profit corporation whose mission is to "help find missing children, reduce child sexual exploitation, and prevent child victimization."[30] It was established in 1984 to oversee operations relating to missing and exploited children and is funded in part by federal grants.[31] One of its programs works with families, law enforcement agencies, electronic service providers, tech companies, and others on methods to reduce the existence and distribution of CSAM.[32] In addition, NCMEC sends alerts to tech companies who are inadvertently

[23] India McKinney & Erica Portnoy, *Apple's Plan to "Think Different" About Encryption Opens a Backdoor to Your Private Life*, ELECTRONIC FRONTIER FOUNDATION (Aug. 5, 2021), https://www.eff.org/deeplinks/2021/08/apples-plan-think-different-about-encryption-opens-backdoor-your-private-life [https://perma.cc/6LH8-VTHB]; *Microsoft Expands PhotoDNA to Fight Child Abuse Imagery*, THORN (July 29, 2015), https://www.thorn.org/blog/microsoft-expands-photodna-to-fight-child-abuse-imagery/ [https://perma.cc/USY4-2V5Y].

[24] Joanna Stern & Tim Higgins, *Apple Executive Defends Tools to Fight Child Porn, Acknowledges Privacy Backlash*, THE WALL STREET JOURNAL (Aug. 13, 2021), https://www.wsj.com/articles/apple-executive-defends-tools-to-fight-child-porn-acknowledges-privacy-backlash-11628859600?mod=searchresults_pos4&page=1 [https://perma.cc/W7BW-WTVE].

[25] Stern, *supra* note 6.

[26] 18 U.S.C. § 2258A.

[27] *About Us*, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, https://www.missingkids.org/footer/about [https://perma.cc/4PA6-VXC7] (last visited Feb. 6, 2022, 10:00 PM).

[28] *Child Sexual Abuse Material (CSAM)*, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, https://www.missingkids.org/theissues/csam [https://perma.cc/78ST-VHZK] (last visited Feb. 6, 2022, 10:00 PM).

[29] NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, *supra* note 27.

[30] *Id.*

[31] 34 U.S.C. § 11293(b).

[32] NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, *supra* note 27.

hosting CSAM on their platforms.[33] Their Child Victim Identification Program has identified over 19,100 CSAM victims since 2002.[34]

B. Apple's Child Safety Feature

Apple's CSF has three parts and works very similarly to the process described above; however, there are some differences.[35] First and vitally, Apple's CSF requires the user opt into having their photos "backed up," or uploaded, to their iCloud account.[36] iCloud is an Apple service that stores, among other things, a user's photos in Apple's version of "the cloud."[37] The cloud is a general term used to describe software and services that run on the Internet, instead of locally on a computer.[38] If a user does not opt into having their photos backed up to iCloud, the CSF does not apply to the user.[39]

Second, when a photo is taken on an Apple device, the hash value is created on the device itself.[40] If the user has opted to have their photos stored in iCloud, the hash value will then be compared to a CSAM database embedded in the Apple device's software.[41] If the hash value from the image matches a hash value within the CSAM database, the user's account is flagged.[42]

Third, the image with its hash value is uploaded to iCloud.[43] If thirty images are flagged as CSAM in an Apple user's iCloud, their account will be flagged, and Apple will gain access to the flagged images to confirm they are CSAM.[44] Apple chose the 30 image threshold to provide a "drastic safety margin" in hopes of avoiding false positives.[45] Apple will only review those specific images, not any other images on an individual's iCloud.[46] If the images are confirmed to be CSAM, the

[33] *Our Impact*, NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, https://www.missingkids.org/ourwork/impact [https://perma.cc/3GWL-R2NH] (last visited Feb. 6, 2022, 10:00 PM).

[34] NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, *supra* note 28.

[35] Stern, *supra* note 6.

[36] *Id.*

[37] *iCloud User Guide*, APPLE, https://support.apple.com/guide/icloud/introduction-to-icloud-mm74e822f6de/icloud [https://perma.cc/4BKE-DEUH] (last visited Feb. 6, 2022, 10:00 PM).

[38] Bonnie Cha, *Too Embarrassed to Ask: What Is 'The Cloud' and How Does It Work?,* Vox (Apr. 30, 2015), https://www.vox.com/2015/4/30/11562024/too-embarrassed-to-ask-what-is-the-cloud-and-how-does-it-work [perma.cc/5MSQ-MDUG].

[39] Stern, *supra* note 6.

[40] *Id.*

[41] McKinney, *supra* note 23.

[42] Stern, *supra* note 6.

[43] *Id.*

[44] *Id.*

[45] APPLE, *Security Threat Model review of Apple's Child Safety Features* 10 (2021), https://www.apple.com/child-safety/pdf/Security_Threat_Model_Review_of_Apple_Child_Safety_Features.pdf [https://perma.cc/77U6-5SZK] (last visited Apr. 1, 2022).

[46] Stern, *supra* note 6.

moderator will report the Apple user's account to NCMEC.[47]

C. Existing Photo Scanning Programs

The HVM has been in use for decades.[48] Companies, including Microsoft, Google, Meta, and Twitter all use the HVM to combat CSAM.[49] These companies have received similar backlash to Apple.[50] In 2014, for example, Google detected CSAM in an email sent by John Henry Skillern through his Gmail account.[51] The case was referred to NCMEC and Houston police arrested him.[52] Some were concerned that scanning emails sent through Gmail would result in monitoring less nefarious illegal activity, like the distribution of pirated TV shows.[53] However, these companies have assured that their methods of scanning are only targeted at CSAM and not other criminal activity.[54] The following section details more specifically how Google and Microsoft scan their platforms for CSAM.

1. Google

Google began scanning for CSAM in 2008.[55] It developed a four-pronged approach: deter, detect, remove, and report.[56] In the first prong, it uses an algorithm that is continuously updated to block search results that lead to CSAM.[57] For example, when a query appears to be searching for CSAM, Google instead queries for adult sexual content.[58]

In the second prong, Google uses trained specialist teams and advanced technology to identify CSAM on its platform.[59] Like Apple, Google uses the HVM to scan for CSAM images.[60] However, unlike Apple, Google's technology also has the capability to scan for CSAM videos.[61] In addition to using The HVM, Google uses machine learning

[47] *Id.*
[48] Bart Preneel, Topics in Cryptology - CT-RSA 2010 1 (Josef Pieprzyk ed., 1st ed. 2010).
[49] Perez, *supra* note 18.
[50] James O'Toole, *Google snoops on Gmail to catch pedophiles*, CNN (Aug 14, 2014), https://money.cnn.com/2014/08/14/technology/enterprise/gmail-pedophiles/ [https://perma.cc/FX4H-SA9P].
[51] *Google 'reveals user' over Gmail child abuse images*, BBC (Aug. 4, 2014), https://www.bbc.com/news/technology-28639628 [https://perma.cc/HQ79-G48U].
[52] *Id.*
[53] O'Toole, *supra* note 50.
[54] Mark Hachman, *How Google handles child pornography in Gmail*, PCWORLD (Aug. 5, 2014), https://www.pcworld.com/article/440661/how-google-handles-child-pornography-in-gmail-search.html [https://perma.cc/S9Z7-9K6P].
[55] Perez, *supra* note 18.
[56] *Fighting child sexual abuse online*, GOOGLE, https://protectingchildren.google/#introduction [https://perma.cc/H54M-TYCR] (last visited Feb. 6, 2022, 10:00 PM).
[57] *Id.*
[58] *Fighting abuse on our own platforms and services*, GOOGLE, https://protectingchildren.google/#fighting-abuse-on-our-own-platform-and-services [https://perma.cc/6GWF-9B4S] (last visited Feb. 6, 2022, 10:00 PM).
[59] *Id.*
[60] *Id.*
[61] *Id.*

technology that scans for never-seen-before CSAM.[62] When never-seen-before CSAM is identified, a trained specialist views the image to confirm it is CSAM.[63]

In the third prong of Google's approach, it removes any CSAM it detects and may choose to terminate the user's account.[64] Finally, in the fourth prong of Google's approach, it reports any CSAM detected on their platform to NCMEC.[65] In these reports, Google includes the user's identification, the victim's identification, and other helpful contextual facts.[66] This program has become successful, reporting over 1.6 million CSAM hash values to NCMEC in the first six months of 2021 alone.[67]

2. Microsoft

In 2015, Microsoft worked with Dartmouth, NCMEC, and the International Center for Missing and Exploited Children to create PhotoDNA, a tool almost identical to Apple's proposed CSF.[68] Both Meta and Twitter, among many others, use PhotoDNA to scan for CSAM.[69] In addition, PhotoDNA has also been used by law enforcement around the world as a visual image and forensic tools.[70] Subsequently, Microsoft donated PhotoDNA to NCMEC.[71]

One major obstacle Microsoft overcame when creating PhotoDNA was detecting CSAM when perpetrators distorted the image to evade detection.[72] Microsoft's solution was to utilize the HVM, which can determine whether two images are identical using their hashes, even if one is distorted.[73] In addition, a PhotoDNA hash value is not reversible and, therefore, cannot be used to recreate an image.[74] Microsoft claims that this process "protects user privacy[.]"[75]

III. LEGAL INTRODUCTION

The Legal Introduction will be discussed in four sections. The first

[62] *Id.*
[63] *Id.*
[64] *Google's Efforts to Combat Online Child Sexual Abuse Material FAQs*, GOOGLE, https://support.google.com/transparencyreport/answer/10330933 [https://perma.cc/F6M4-XUE7] (last visited Feb. 6, 2022, 10:00 PM).
[65] GOOGLE, *supra* note 56.
[66] GOOGLE, *supra* note 64.
[67] *Google's efforts to combat online child sexual abuse material*, GOOGLE, https://transparencyreport.google.com/child-sexual-abuse-material/reporting [https://perma.cc/F8QP-K4Y3] (last visited Feb. 6, 2022, 10:00 PM).
[68] Ith, *supra* note 48.
[69] *Id.*
[70] *Help stop the spread of child exploitation*, MICROSOFT, https://www.microsoft.com/en-us/photodna?cid=msnc-us [https://perma.cc/HR7L-TTC4] (last visited Feb. 6, 2022, 10:00 PM).
[71] *Id.*
[72] Ith, *supra* note 48.
[73] *Id.*
[74] MICROSOFT, *supra* note 70.
[75] Ith, *supra* note 48.

section will outline the federal laws that require tech companies to report CSAM on their platforms. The second section will provide a brief history of how the Fourth Amendment has interacted and evolved with technology. The third section will give an overview of the third-party doctrine and case law that shaped its narrow application. The fourth and final section will give an overview of the private search doctrine and detail two recent federal circuit cases that illustrate a fracture among circuits on how to handle CSAM reporting using the HVM.

A. Federal Law

The transportation, distribution, sale, or possession of CSAM is illegal in the United States.[76] Federal law requires tech companies to report any CSAM identified on their platform.[77] 18 U.S.C. § 2258A(a) states that electronic communication service providers must report to the NCMEC, "as soon as reasonably possible after obtaining actual knowledge" of "any facts or circumstances from which there is an apparent violation of … child pornography [statutes]."[78] However, federal law does not require tech companies to "affirmatively search, screen, or scan" for CSAM.[79]

B. A Brief History of The Fourth Amendment and Technology

The Fourth Amendment safeguards individual liberties by prohibiting unreasonable intrusions by the government, specifically unreasonable searches and seizures by the government.[80] Both of these protections have been extended to digital searches.[81] Despite its extension to the digital realm, the Fourth Amendment has often lagged behind technological advancements.[82]

For example, one of the first prominent cases concerning the Fourth Amendment and communications was *Ex parte Jackson*, which found that a letter or sealed package could not be intercepted and have its contents examined while it was in the mail without first obtaining a warrant.[83] Later, in the early twentieth century, another case arose that questioned the traditional notions of Fourth Amendment protections. In 1928, *Olmstead v. United States* examined whether the Fourth Amendment extended to phone tapping.[84] The Court ultimately held that the Fourth Amendment did not extend to phone tapping.[85] Things changed, however, in the mid-twentieth century when the Court once again

[76] 18 U.S.C. § 2252.

[77] 18 U.S.C. § 2258A.

[78] *Id.*

[79] 18 U.S.C. § 2258A(f); 18 U.S.C. § 2258E

[80] U.S. Const. amend. IV.

[81] *See* Riley v. California, 573 U.S. 373 (2014).

[82] Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U.L. REV. 1441, 1448 (2017).

[83] *Ex parte Jackson*, 96 U.S. 727 at 732.

[84] Olmstead v. United States, 277 U.S. 438, 455, 48 S. Ct. 564, 565, 72 L. Ed. 944 (1928).

[85] *Id.* at 466.

addressed phone tapping. In *Katz v. United States*, the Court held that the defendant had a reasonable expectation of privacy while using a telephone booth because the Fourth Amendment protected people—not areas—against unreasonable searches and seizures. [86] Justice Harlan's concurrence pointed future courts to two questions in determining whether a similar inquiry is subject to the Fourth Amendment: (1) whether the individual, by his conduct, has "exhibited an actual expectation of privacy" and (2) whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[87]

C. The Third-Party Search Doctrine

One relevant carve out to the Fourth Amendment is the Third-Party Search Doctrine (TPSD). The TPSD allows the government to gather information from third parties without first obtaining a search warrant.[88] The logic behind this carve-out is if the information is shared with others, that information is no longer private and, therefore, does not require a warrant.[89] This carve out permits the government to lawfully access vast information, such as websites that an individual visits; who they have emailed; the phone numbers they dial; and their utility, banking, and education records, among other things.[90] Therefore, it can be argued that the data uploaded to a platform like Apple would fall under the TPSD because Apple is a third-party who is not constitutionally bound to the Fourth Amendment.

The TPSD has prevailed, despite some disdain. One issue is that a person has no Fourth Amendment complaint if they share information with a third party and that third party subsequently shares the information with the government without the person's permission or knowledge.[91] For example, Greg Nojeim, senior counsel at the Center for Democracy and Technology argued, "[i]f strict application of the doctrine ever served us well, it no longer does, leading to absurd results. This is particularly true in an age where so much more information is communicated through intermediaries."[92]

However, the TPSD is a relatively narrow carve out to what third parties can share with the government. There is a legitimate expectation of privacy to the *content* of, for example, a phone call, but not the *data*

[86] *Katz v. United States*, 389 U.S. 347, 348, 88 S. Ct. 507 (1967).

[87] *Id.* at 351, 361.

[88] Rebekah A. Branham, *Hash It Out: Fourth Amendment Protection of Electronically Stored Child Exploitation*, 53 AKRON L. REV. 217, 234 (2019).

[89] Richards, *supra* note 82, at 1467.

[90] *Id.*

[91] David Gray, *Fourth Amendment Remedies As Rights: The Warrant Requirement*, 96 B.U.L. REV. 425, 431 (2016).

[92] John Villasenor, *What You Need to Know about the Third-Party Doctrine*, THE ATLANTIC (Dec. 30, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/ [https://perma.cc/A8EH-3P7E].

produced by the phone call.[93] However, when the data can reveal information where an individual has a legitimate expectation of privacy, like data showing their physical movements, that data can also become protected.[94] In *Smith v. Maryland*, the court likened the data distinction to the old switchboard phone system, where an operator would connect a caller's phone line to its desired destination.[95] This made the operator a third-party who could remember the phone number and provide that data to the police.[96] Likewise, when one dials a phone number, they are communicating data to the phone company regarding who they wish to call.[97]

D. The Private Search Doctrine

The Private Search Doctrine (PSD) is also a carve out to the Fourth Amendment. Under the PSD, the Fourth Amendment remains implicated "if the authorities use information with respect to which the expectation of privacy has not already been frustrated."[98] Put more simply, the Fourth Amendment protects individuals against unreasonable search and seizure by the government; however, it *does not* protect against searches conducted by private individuals or entities. Although the TPSD and the PSD are similar in many respects, there has been much more contention among the circuits about how to apply the PSD to cases where CSAM is reported using the HVM.[99]

Often, the contention lies in the platform's process for reporting CSAM using the HVM, specifically, whether a private entity has viewed the CSAM or just its hash prior to submitting it to law enforcement.[100] These contentions stem from two important privacy cases, *United States v. Jacobsen*[101] and *United States v. Walter.*[102]

1. United States v. Jacobsen

In *Jacobsen*, FedEx observed one of their packages was damaged, and per policy, employees opened the package to discover five tubes.[103] When employees opened the tubes, they discovered several bags of white powder.[104] The employees notified the Drug Enforcement Agency (DEA), who examined the contents and determined the white powder was

[93] Smith v. Maryland, 442 U.S. at 737, 744 (1979).
[94] Carpenter v. United States, 201 L. Ed. 2d 507 (2018).
[95] Richards, *supra* note 82, at 1å472.
[96] *Supra,* note at 93, at 744.
[97] Richards, *supra* note at 82, at 1473.
[98] United States v. Jacobsen, 466 U.S. 109, 117 (1984).
[99] O'Connell, *supra* note 21, at 312.
[100] *Id.*
[101] *Jacobsen*, 466 U.S. at 117.
[102] *Walter*, 447 U.S. 649 (1980).
[103] *Supra*, note 101, at 111.
[104] *Id.*

cocaine.[105] The DEA then obtained a warrant to search the place to which the package was addressed and the correspondents were arrested.[106] The respondents argued that the warrant was the product of an illegal search and seizure.[107] However, the Supreme Court held that the DEA was not required to obtain a warrant before conducting the field test because the initial search was conducted by FedEx, a private party.[108] This holding illustrates the importance of the private party and their conduct when evoking the PSD, but it left a large question: what is considered a private search? This question was put to the test in *Walter*.

2. United States v. Walter

An Atlanta, Georgia, company mistakenly received several strange packages with suggestive drawings on their sides in September 1975.[109] An employee opened the boxes to discover several films.[110] They held one film strip up to the light to identify the contents but were unsuccessful.[111] The FBI picked up the packages and viewed the film, which they determined depicted "homosexual activities."[112] Petitioners argued that the warrantless projection of the films constituted an illegal search, even though the government had acquired the films from a private party.[113] The Supreme Court agreed, holding that the FBI exceeded the scope of the antecedent actions because the individual who received the film had not actually viewed it, and the FBI had to screen the film to confirm the crime had occurred.[114]

Smith, Jacobsen, and *Walter* are examples of how the modern Fourth Amendment allows tech companies to report CSAM using the HVM—if they follow the right steps. However, much confusion still exists about the legality of the reporting process. The following two circuit cases were recently decided and are an illustration of how cases with similar facts can lead to opposite results.

3. United State v. Reddick

In 2015, Henry Reddick uploaded CSAM to his Microsoft SkyDrive, which created a hash through PhotoDNA and was flagged by Microsoft.[115] Microsoft created a CyberTip that was sent to NCMEC, who

[105] *Id.* at 111-12.
[106] *Id.* at 112.
[107] *Id.*
[108] *Id.* at 115.
[109] *Supra* note 102, at 651-52.
[110] *Id.*
[111] *Id.* at 652.
[112] *Id.* at 651.
[113] *Id.* at 649.
[114] *Id.* at 657.
[115] United States v. Reddick, 900 F.3d 636, 637-38 (5th Cir. 2018).

then sent it to the police.[116] There is no evidence that a Microsoft employee reviewed the images before forwarding the CyberTip to NCMEC.[117] In turn, the police opened the image and confirmed it was CSAM.[118] The police executed a warrant and obtained Reddick's home computer where they found more CSAM.[119] Reddick, however, argued that the police conducted an unlawful search when they viewed the images attached to the CyberTip without a warrant.[120]

The Fifth Circuit held the search was not a violation of the appellant's Fourth Amendment rights.[121] Under the private search doctrine, the Fourth Amendment was not implicated because it was performed by a private entity, Microsoft, rather than the police.[122] Further, the Court compared this case to *Jacobson*.[123] Microsoft discovered the images, like FedEx, and the police viewed the images to confirm they were in fact CSAM, like the police conducting the drug field test in *Jacobson*.[124] Accordingly, whatever expectation of privacy the appellant might have had in the hash values of his files was frustrated by Microsoft's private search.[125]

4. United States v. Wilson

In June of 2015, Luke Wilson's Gmail account was flagged by Google when he attached four files that included CSAM to an email.[126] Google automatically generated a CyberTip report and sent an electronic tip to NCMEC.[127] A Google employee did not review the flagged images associated with Wilson's account.[128] NCMEC subsequently sent the hash values and image descriptions to law enforcement, who requested to view the actual images.[129] After viewing the actual images, law enforcement obtained a search warrant for Wilson's email account, where they discovered more CSAM.[130]

Similar to *Reddick*, Wilson argued that law enforcement's warrantless viewing of the images amounted to an unlawful search.[131] The Ninth Circuit agreed and held the search was a violation of the appellant's Fourth Amendment rights.[132] The Court reasoned that the government

[116] *Id.* at 638.
[117] *Id.* at 637-8.
[118] *Id.* at 638.
[119] *Id.*
[120] *Id.*
[121] *Id.* at 639.
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] United States v. Wilson, 13 F.4th 961, 965 (9th Cir. 2021).
[127] *Id.*
[128] *Id.*
[129] *Id.*
[130] *Id.* at 966
[131] *Id.*
[132] *Id.* at 980.

search exceeded the scope of the antecedent private search because it allowed the government to learn new, critical information.[133] Google had not viewed the images; they only matched the hashes to the descriptions.[134] Therefore, law enforcement substantially expanded the information beyond the image descriptions to learn exactly what the images showed and to confirm they were CSAM.[135] The Court likened this case to *Walter*, explaining that the images attached to Mr. Wilson's email were only "suspected" CSAM until law enforcement confirmed through illegally viewing them.[136]

IV. THE REAL THREAT TO PRIVACY AND THE FOURTH AMENDMENT

Although opponents of Apple's CSF have expressed legitimate concerns about the feature's privacy and Fourth Amendment implications, these concerns about the HVM are not new and often reflect a misunderstanding of the technology. As discussed earlier, Google faced similar backlash in 2014 when the public became aware that the platform was using the HVM to scan Gmail for CSAM.[137] However, Google has detected over 1.6 million CSAM and contributed hashes to NCMEC.[138] The HVM maintains privacy and the Fourth Amendment rights of users while effectively catching predators, and Apple is simply following other tech companies that have been using the HVM for decades.

The real concern should lie with the federal circuit fracture that has left tech companies and law enforcement puzzled about how to effectively report CSAM. As illustrated in *Reddick* and *Wilson*, similar facts have led to different outcomes, depending on the circuit. The discussion below addresses some of the common critiques opponents have made about Apple's CSF and proposes solutions to the circuit split.

A. Addressing Concerns about Apple's CSF

1. The Technology Will be Used to Spy on People

A concern scholars have expressed is that Apple's CSF will be weaponized by foreign governments, like China, to surveil dissidents.[139] For example, Princeton University's Johnathan Mayer argued this point in

[133] *Id.* at 973.
[134] *Id.* at 972.
[135] *Id.* at 973.
[136] *Id.*
[137] BBC, *supra* note 51.
[138] GOOGLE, *supra* note 63.
[139] Robert McMillan, *Apple Plans to Have iPhones Detect Child Pornography, Fueling Privacy Debate*, THE WALL STREET JOURNAL (Aug. 5, 2021), https://www.wsj.com/articles/apple-plans-to-have-iphones-detect-child-pornography-fueling-privacy-debate-11628190971 [https://perma.cc/PE5Z-4NUK].

a Washington Post article.[140] He described that he created a prototype of Apple's CSF in 2019 to identify CSAM in an end-to-end encrypted device, like an Apple device, and he and his team found that the system had one major flaw: it could easily be repurposed for surveillance and censorship.[141] There was nothing preventing someone from modifying the algorithm to search for images other than CSAM.[142]

Yet Mayer assumes that this technology and the CSAM database would be accessible to any government to use and modify. First, Apple responded to criticism that it would bow to governments who will misuse the technology to target dissidents.[143] It reassured the public that it would resist pressure from all foreign governments, including China.[144] This assurance has always been at the core of Apple's values.[145] For example, in 2008, after a tragic mass shooting in San Bernardino, the government requested that Apple unlock the shooter's phone.[146] Apple refused, citing its dedication to user privacy and released a letter explaining its reasoning for refusing the government's request:

> But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone. . . The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers[.][147]

Although Apple's CSF appears to contradict their strict stance on sharing private information with the government, it is important to remember the privacy safeguards Apple has embedded into reporting process. First, Apple never sees a user's photos unless they are flagged.[148] Furthermore, Apple is required by federal law to report CSAM identified on their platform "as soon as reasonably possible after obtaining actual knowledge."[149] Therefore, unlike the "backdoor" the United States government requested after the San Bernardino shooting in order to see the contents of the shooter's phone, Apple has narrowly tailored their

[140] Anunay Kulshrestha, *Opinion: We built a system like Apple's to flag child sexual abuse material*, THE WASHINGTON POST (Aug 19, 2021), https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/ [https://perma.cc/6EJX-W5T4].

[141] *Id.*

[142] *Id.*

[143] Browning, *supra* note 13.

[144] *Id.*

[145] Devlin Barrett, *Roots of Apple-FBI Standoff Reach Back to 2008 Case*, THE WALL ST. J. (Apr. 7, 2016), https://www.wsj.com/articles/roots-of-apple-fbi-standoff-reach-back-to-2008-case-1460052008?mod=article_inline [https://perma.cc/8KFQ-S2F8].

[146] *Id.*

[147] *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/ [https://perma.cc/6XHW-MSGS].

[148] Stern, *supra* note 6.

[149] 18 U.S.C. § 2258A.

policy to scan for specific data using the HVM in order to comply with federal law.

Second, Apple explained that no government would or could control the CSAM database.[150] The CSAM database would be collected from outside parties, like the NCMEC, and the images collected would make up a larger, uniform database used across the world.[151] By drawing from multiple CSAM databases, any single perpetual hash appearing in one single CSAM database or in CSAM databases from the one single, sovereign jurisdiction would be discarded from Apple's CSAM database.[152] Furthermore, even if Apple included hash values from one sovereign jurisdiction, like China, and these hash values were aimed at targeting dissidents, the matches would be reviewed by Apple.[153] Image review would not be automated.[154] All positive matches must be visually confirmed by an Apple content moderator *before* Apple sends the user's information to a participating child safety organization, like the NCMEC.[155] Therefore, attempted nefarious use of the technology by Apple would be curbed by these processes.

2. Auditability of the CSAM Database

Another point of concern is that Apple's CSAM database cannot be audited.[156] Many were alarmed at the idea of a "mini" NCMEC CSAM database being embedded in every Apple device.[157] However, Apple insists that the database can be audited and that there are "multiple levels of auditability."[158] Apple has pledged to release a Knowledge Base article containing a root hash of the CSAM hash database included with each version of every Apple operating system that supports the feature.[159] This enables third party technical auditors to confirm that any given root hash within the CSAM database was generated only from a participating child safety organization.[160] This way, not only are child safety organizations able to protect sensitive information, but outside auditors can independently keep Apple accountable.[161] Apple also notes that participating child safety organizations can perform audits as well.[162]

[150] Chance Miller, *Apple details the ways its CSAM detection system is designed to prevent misuse*, 9TO5MAC (Aug. 13, 2021), https://9to5mac.com/2021/08/13/apple-details-the-ways-its-csam-detection-system/ [https://perma.cc/P2R6-T8AE].
[151] Stern, *supra* note 6.
[152] *Id.*
[153] APPLE, *supra* note 45.
[154] *Id.* at 8.
[155] *Id.* at 13.
[156] McKinney & Portnoy, *supra* note 23.
[157] *Id.*
[158] Stern, *supra* note 6.
[159] APPLE, *supra* note 153.
[160] *Id.*
[161] *Id.*
[162] *Id.*

3. Collisions

Finally, there are major concerns about collisions, also known as false positives, which occur when the algorithm identifies a non-CSAM image as CSAM.[163]

Although the possibility of a collision is very real, the chance of a collision occurring is one in one billion.[164] Apple further counters this criticism by boasting that they conditioned their HVM technology to consider the possibility of false positives.[165] For example, Apple assessed the performance of their HVM technology by matching 100 million non-CSAM photographs against NCMEC's CSAM database, which provided only three false positives and were verified by human moderators.[166] They further assessed its performance against a 500,000 adult pornography dataset, which produced zero false positives.[167] As discussed earlier, Apple also safeguards against the threat of a false positive by implementing the thirty-image threshold in which a user's account would only be flagged if thirty images were flagged.[168]

B. Fourth Amendment Concerns

In addition to the above critiques, there has been some confusion about whether Apple's CSF violates the Fourth Amendment. However, under both the TPSD and the PSD, law enforcement may obtain a user's personal information from Apple or other tech companies if the user's conduct violates federal law.

First, under the TPSD, the government can gather information shared with third parties because it is no longer private information and therefore does not require a warrant.[169] In this case, when a user uploads an image to iCloud, the user shares this information with Apple, a third party. The government can then obtain this information from Apple. For example, uploading an image to the iCloud could be likened to having a film developed by a private photo development shop where a developer identifies an image as CSAM and reports it to the police. Apple can be considered a "developer" when they process a user's images into iCloud and identify an image as CSAM.

Second, the PSD carves out private searches conducted by private parties from Fourth Amendment protections.[170] Therefore, when Apple scans a user's iCloud, it is not conducting an illegal search and seizure because Apple is a private entity, and the user has given Apple consent. As such, the information Apple finds and shares with law enforcement is

[163] Kulshrestha, *supra* note 140.

[164] THORN, *supra* note 19.

[165] APPLE, *supra* note 153.

[166] *Id.*

[167] *Id.*

[168] *Id.*

[169] Richards, *supra* note 82, at 1467.

[170] *Jacobsen*, *supra* note 101 at 117.

subject to the PSD. However, as evidenced by *Reddick* and *Wilson*, things become complicated when information gathered under the PSD is provided to law enforcement.

C. The Future of Reporting CSAM using the HVM

The real concern in using the HVM to report CSAM is the lack of consensus among circuits on how to analyze cases where CSAM is reported using the HVM; however, there are some solutions.

1. Solution 1: The Supreme Court

The first, and likely the best, solution would be for the Supreme Court to take up the issue and create a standard test. Yet, to date, the Supreme Court has denied certiorari, despite several attempts to appeal cases where the CSAM was reported using the HVM. However, an indicator of how the Court would react to a case where CSAM was reported using the HVM is *United States v. Ackerman*. In that case, AOL flagged one of Ackerman's emails because the hash value of one of the four attachments matched a confirmed CSAM hash value.[171] AOL did not open Ackerman's email or view any of the attachments, including the attachment that matched the confirmed CSAM hash value.[172] However, the NCMEC opened the email and viewed all four attachments to confirm they were CSAM.[173]

Then-Judge Gorsuch of the Tenth Circuit acknowledged that *Ackerman* could be successfully analogized to *Jacobsen* only if AOL opened Ackerman's email and viewed the attachments to confirm they were CSAM prior to sending the CyberTip to NCMEC.[174] However, because this did not occur, NCMEC "'could [have] disclose[d]' information previously unknown to the government besides whether the one attachment contained contraband."[175] Therefore, the Tenth Circuit held that the NCMEC had acted as a government entity rather than a private actor by opening and viewing Ackerman's attachments.[176] The NCMEC's unwarranted search implicated the Fourth Amendment.[177]

Based on this case, it could be likely that Justice Gorsuch could find that the Fourth Amendment was not implicated if a tech company takes the right steps. He even pondered this situation later in the opinion:

> What if NCMEC hadn't opened Mr. Ackerman's email but had somehow directly accessed (only) the (one) attached

[171] United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016).
[172] *Id*. at 1306.
[173] *Id*.
[174] *Id*. at 1306-7
[175] *Id*.
[176] *Id*. at 1308
[177] *Id*.

> image with the matching hash value? Could the government have argued that, . . . NCMEC's actions didn't risk exposing any private information beyond what AOL had already reported to it? Or might even that have risked exposing new and protected information, maybe because the hash value match could have proven mistaken (unlikely if not impossible) or because the AOL employee who identified the original image as child pornography was mistaken in his assessment (unlikely if maybe more possible)?[178]

Justice Gorsuch's acknowledgment of HVM's validity by stating that it would be "unlikely if not impossible" for the hash value to be mistaken is noteworthy.

2. Solution 2: Circuits Adopt a Uniform Test

In the absence of a formal Supreme Court test, circuit courts have created their own. This leads to the second potential solution: all circuit courts adopt a uniform test. The First Circuit devised a three-part analysis to determine whether a private party acts as a government agent: (1) the extent of the government's role in instigating or participating in the search, (2) its intent and the degree of control it exercises over the search and the private party, and (3) the extent to which the private party aims primarily to help the government or to serve its own interests.[179] Similarly, the Fifth, Ninth, and Tenth Circuits created a two-part test, which asks: (1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends.[180] The remaining circuits have less precise tests.[181]

One major issue with all circuits adopting the same test is their ability to evenly apply it to something as abstract as the HVM. The biggest issue courts have struggled with is analogizing cases involving tangible items with cases involving technology.[182] For example, the Fifth and Ninth Circuits use the same test in analyzing whether a private party is acting as a government agent. Yet, in *Wilson*, a Fifth Circuit case, and in *Reddick*, a Ninth Circuit case, the courts reached different outcomes. In fact, the *Wilson* court argued that the *Reddick* case, was incorrectly decided.[183] The *Wilson* court stated:

[178] *Id*. at 1306

[179] United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009).

[180] *See Generally,* Branham, *supra* note 88 at 232.

[181] Anirudh Krishna, *Internet.gov: Tech Companies as Government Agents and the Future of the Fight Against Child Sexual Abuse*, 109 CALIF. L. REV. 1581, 1612 (2021).

[182] *Supra*, note 171 at 1308.

[183] *Supra*, note 126 at 978; *Supra*, note 115 at 639.

> We cannot accept [the Ninth Circuit's] analysis for several reasons. First, and most important, *Reddick* conflates *Jacobsen*'s first holding regarding the private search exception to the Fourth Amendment with its second holding regarding whether the field test constituted a search under the Fourth Amendment . . . in *Jacobsen*, the white powder was fully visible to the government officers when they repeated the steps taken by the FedEx employees to inspect the package. Not so here, as no human had viewed Wilson's images before. The part of *Jacobsen* that does elucidate the private search doctrine cannot govern here.[184]

The Ninth Circuit noted in their opinion that the Sixth Circuit also declined to follow the *Reddick* holding: The Sixth Circuit explained that the government agent's "inspection (unlike the [field] test [in *Jacobsen*]), qualifies as the invasion of a 'legitimate privacy interest' unless Google's actions had already frustrated the privacy interest in the files."[185]

3. Third Solution: Congressional Action

If the Supreme Court is unlikely to take up the issue and the circuit courts have difficulty analyzing cases where the HVM is used to report CSAM, Congress should act; although, this would be a difficult task.

The Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2022 (The Act) was introduced in January 2022.[186] The Act is co-authored by Senators Lindsey Graham (R-SC) and Richard Blumenthal (D-CT) and received bipartisan support.[187] Its goal is to develop recommended best practices that tech companies *may* choose to implement to prevent, reduce, and respond to the online sexual exploitation of children.[188] The Act creates the National Commission on Online Child Sexual Exploitation Prevention (Commission), which is chaired by the Attorney General and includes the Secretary of Homeland Security and the Chairman of the Federal Trade Commission.[189] The remaining members would be equally appointed by Majority and Minority leaders of the House and Senate.[190] The Act requires appointees to have specific knowledge or lived experience in order to sit on the Commission.[191] For example, the Act calls for appointees who have

[184] *Supra*, note 126 at 978.
[185] *Id*. at 979.
[186] The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act, S. 3538, 117th Cong. (2022).
[187] *Id*.
[188] *Id*. § 3(b).
[189] *Id*. §§ 3(a), 3(c)(1)(B).
[190] *Id*. § 2(c)(1)(C).
[191] *Id*. § 3(c)(2).

experience in investigating online child sexual exploitation, including two appointees with law enforcement experience and two appointees who have prosecutorial experience.[192] Importantly, four members of the Commission must be survivors of online child sexual exploitation or have current experience in providing services for victims of online child sexual exploitation in a non-governmental capacity.[193]

The Commission is tasked with developing and submitting to the Attorney General recommended best practices for tech companies that will help "prevent, reduce, and respond to the online sexual exploitation of children[.]"[194] While creating these recommended best practices, the Commission will aim to address the following, among other things: coordinating with non-profit organizations to preserve, remove from view, and report online child sexual exploitation; implementing a standard rating and categorization system to identify the type and severity of child sexual abuse material; training and supporting content moderators who review child sexual exploitation content; and, offering parental control products that enable customers to limit the types of websites, social media platforms, and internet content that are accessible to children.[195] The Commission will also consider the size, type of product, and business model of tech companies and whether these aspects make them susceptible to exploitation.[196]

The Act also calls for amending Section 230(e) of the Communications Act of 1934, which in its current form shields tech companies from liability for their users' actions.[197] Recall that 18 U.S.C. § 2258A(a) requires CSAM be reported only when the company obtains "actual knowledge" of "any facts or circumstances from which there is an apparent violation of . . . child pornography [statutes]."[198] However, the Act's amendment to Section 230(e) would give state attorney generals the authority to bring civil or criminal lawsuits against tech companies for *any* "advertisement, promotion, presentation, distribution, or solicitation of child sexual abuse material" if the company fails to certify compliance with the recommended best practices proposed by the Commission.[199] Tech companies can choose to create and implement private best practices to combat CSAM, but they will lose their Section 230(e) protections unless a judge determines their best practices for combatting CSAM are reasonable in comparison to the Commission's best practices.[200] Therefore, tech companies must "earn" their Section 230(e) protections by

[192] *Id.*
[193] *Id.* § 3(c)(2)(B)
[194] *Id.* § 4(a)(1)(A).
[195] *Id.* § 4(a)(3).
[196] *Id.* § 4(a)(1)(B)(i).
[197] *Id.* § 5.
[198] *Id.*
[199] *Id.*
[200] Ronald Newman, *ACLU Opposition to S. 3398, The Earn It Act*, ACLU (Mar. 9, 2020), https://www.aclu.org/letter/aclu-opposition-s-3398-earn-it-act [perma.cc/7NRF-H2UK].

opting into the Commission's best practices or creating their own, which would likely have to be very similar to the Commission's.[201]

The amendments to Section 230(e) have drawn the most controversy.[202] First, some argue Section 5 of the Act would turn tech companies into government actors.[203] However, the TPSD which allows third parties, such as tech companies, to relay information to law enforcement if the information is voluntarily provided to the tech company by the user.[204] Second, some argue that the amendment will result in the death of end-to-end encryption.[205] However, drafters later added a provision that prohibits encryption from being used as the sole justification for a lawsuit.[206]

While none of these solutions are perfect, they provide some structure to an area of law that has been slow to keep up with the burgeoning of technology and social media.

V. CONCLUSION

Judge Ketanji Brown Jackson once described sentencing a defendant in a criminal CSAM case: "When I look in the eyes of a defendant who is weeping because I'm giving him a significant sentence, what I say to him is, do you know that there is someone who . . . cannot leave her house because she thinks that everyone she meets will have seen her[?]"[207]

Although there are concerns about Apple's CSF and privacy, HVM technology has been used industry-wide for many years. Apple, in particular, has implemented processes that prevent exploitation, like releasing Knowledge Base article for third parties to audit, creating a uniform CSAM database drawn from smaller CSAM databases to prevent government intervention, and following a policy that is narrowly tailored to scan only for CSAM.

The real threat is how courts determine when a private tech company is turned into a government actor when using hashing technology to report and gather evidence of CSAM. Although the Fourth Amendment has been slow to evolve with the rise of technology, the government has utilized two relevant Fourth Amendment carve outs, TPSD and PSD, to gather evidence in CSAM cases—so long as the right steps are followed. The PSD has caused the most controversy and confusion in these cases,

[201] *Id.*
[202] *See* Brian Fung, *A controversial bill to protect kids online just advanced in the Senate*, CNN, https://www.cnn.com/2022/02/11/tech/earn-it-act-senate/index.html [https://perma.cc/2944-GSUA] (last updated Feb. 11, 2022).
[203] *Id.*
[204] *See supra* Part III.C.
[205] Fung, s*upra* note 226.
[206] *Supra* note 186.
[207] The Daily, *The Confirmation Hearing of Ketanji Brown Jackson*, THE NEW YORK TIMES, at 20:58 (Mar. 23, 2022), https://www.nytimes.com/2022/03/23/podcasts/the-daily/ketanji-brown-jackson-supreme-court-hearings.html? [https://perma.cc/27JZ-CG4K].

resulting in different outcomes even in cases with similar facts. As a result, it is vital that at least one of the proposed solutions be adopted: the Supreme Court should create a uniform test, all circuit courts should adopt the same test, or Congress should pass the EARN IT Act.