University of Arkansas at Little Rock Law Review

Volume 45 | Issue 4 Article 5

2023

Constitutional Law—The Current System for Abolishing Child Pornography Online is Ineffective: The Alternative Measure for Eradicating Online Predators

Virginia Kendall

CONSTITUTIONAL LAW—THE CURRENT SYSTEM FOR ABOLISHING CHILD PORNOGRAPHY ONLINE IS INEFFECTIVE: THE ALTERNATIVE MEASURE FOR ERADICATING ONLINE PREDATORS

I. INTRODUCTION

"Teen" is a shortened word for teenager or an individual between thirteen and nineteen;[1] in 2018, it was the seventh most searched term on Pornhub, a wholly owned subsidiary of MindGeek.[2] Sixteen-year-old Jane Doe #1 became one of those "teens"[3] after an Alabama man drugged, raped, and filmed the sexual abuse, which he uploaded on MindGeek's websites.[4] Not only did he rape Jane Doe #1, but the man also profited off her rape through views and downloads.[5] MindGeek users viewed her rape over 2,400 times.[6] Jane Doe #1's story is not a rarity; thousands of Jane and John Does are revictimized daily by perpetrators uploading their sexual abuse on the internet.[7] Subsequently, as a result of "[t]wenty-first century technology and the proliferation of the internet and mobile devices," companies such as Pornhub and MindGeek not only profit but "[help] facilitate the crime of child sex trafficking and other forms of child exploitation."[8] In 2021, the National Center for Missing and Exploited Children ("NCMEC") announced its Tipline had received 29.3 million reports of child abuse, a record high, including incidences of child pornography on the internet.[9] This statistic amounts to an average of

1. *Teenager*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/teenager (last visited Feb. 20, 2023).

2. Complaint at 4, 15, Jane Doe #1 v. MG Freesites, LTD, 7:21-cv-00220-LSC (N.D. Ala. Feb. 11, 2021), ECF No. 1.

3. *See id.* at 1.

4. *Id.* at 25.

5. *Id.* (noting he entered into a business agreement with MindGeek under its Modelhub program, a program for amateur pornographers to upload and create a revenue stream based on video views).

6. *Id.*

7. *See id.* at 6–7 (noting the Complaint is for Jane Doe #1, Jane Doe #2, and all others in the class action lawsuit who are victims and survivors of child sexual abuse and trafficking); *see* David Finkelhor et. al, *Prevalence of Online Sexual Offenses Against Children in the US*, JAMA NETWORK OPEN, at 2 (Oct. 14, 2022), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2797339.

8. Exec. Order No. 13,903, 85 Fed. Reg. 6721 (Jan. 31, 2020).

9. *CyberTipline 2021 Report*, NAT'L CTR. FOR MISSING AND EXPLOITED CHILD. [hereinafter NCMEC, *CyberTipline*], https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata (last visited Feb. 20, 2023); NAT'L CTR. FOR MISSING AND EXPLOITED CHILD., 2021 CYBERTIPLINE REPORTS BY ELECTRONIC SERVICE PROVIDERS (ESP) 1 (2022) [hereinafter NCMEC, 2021 REPORT], https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-esp.pdf.

563,461 reported instances of child abuse per week.[10] As the internet grows, so does a pedophile's digital playground.[11]

Today the federal government defines child pornography as "any visual depiction . . . of sexually explicit conduct where . . . the production . . . involves the use of a minor engaging in sexually explicit conduct."[12] Outside of the legal system, child pornography is generally referred to as Child Sexual Abuse Material ("CSAM").[13] With the digital age increasing societies' ability to transfer information immediately, without additional barriers,[14] Congress passed several laws limiting the spread, distribution, and manufacture of child pornography.[15] The Protection of Children Against Sexual Exploitation Act of 1977 prohibited the commercial distribution and manufacture of child pornography created with minors sixteen and under.[16] Then, in 1988, Congress passed the Child Protection and Obscenity Enforcement Act, which made it illegal to use a computer to depict or advertise child pornography.[17] These acts were a part of legislative efforts to reduce the amount of child pornography online.[18]

The Protection of Children Against Sexual Exploitation Act of 1977 and Child Protection and Obscenity Enforcement Act of 1988 are both over forty years old and have not achieved the intended goal of eliminating child

---

10. *See* NCMEC, *CyberTipline*, *supra* note 9; NCMEC, 2021 REPORT, *supra* note 9.

11. *See* Michael J. Henzey, *Going on the Offensive: A Comprehensive Overview of Internet Child Pornography Distribution and Aggressive Legal Action*, 11 APPALACHIAN J.L. 1, 53 (2011).

12. 18 U.S.C. § 2256; *Child Sexual Abuse Material (CSAM)*, NAT'L CTR. FOR MISSING AND EXPLOITED CHILD. [NCMEC, *CSAM*] , https://www.missingkids.org/theissues/CSAM (last visited Feb. 20, 2023).

13. NCMEC, *CSAM*, *supra* note 12.

14. Robert Kormoczi, *What Is the Digital Age?*, TIMES INT'L (June 24, 2020), https://timesinternational.net/the-digital-age/.

15. RICHARD WORTLEY & STEPHEN SMALLBONE, 41 PROBLEM-SPECIFIC GUIDES SERIES: CHILD PORNOGRAPHY ON THE INTERNET 7 (2015). Between 1978 and 1998, Congress passed the Sexual Exploitation of Children Act, Child Protection Act, Child Protection and Obscenity Enforcement Act, Child Pornography Protection Act, and the Child Protector and Sexual Predator Punishment Act. *Id.* All of these acts helped develop the laws against child pornography in the United States. *Id.*

16. Protection of Children Against Sexual Exploitation Act of 1977, Pub. L. No. 95-225, 92 Stat. 7 (1978); WORTLEY & SMALLBONE, *supra* note 15, at 7.

17. Child Protection and Obscenity Enforcement Act of 1988, Pub. L. No. 100-690, 102 Stat. 4181; WORTLEY & SMALLBONE, *supra* note 15, at 7.

18. *See, e.g.*, Artemus Ward, *Protection of Children Against Sexual Exploitation Act of 1977 (1977)*, THE FIRST AMEND. ENCYC., https://www.mtsu.edu/first-amendment/article/1088/protection-of-children-against-sexual-exploitation-act-of-1977 (last visited Feb. 20, 2023) (noting Congress passed legislation to combat child pornography after heavy media attention following a 1976 NBC News publication that indicated child pornography was a "huge and growing business").

pornography online.[19] Thus, to combat the spread of pedophiles on mainstream media sources,[20] Congress must enact new legislation to allow for alternative measures, such as hash value matching. Hash value matching is a process that generates a unique numerical identifier known as a value and then digitally compares the value with NCMEC's values of known child pornography images.[21] Currently, many corporations use hash value matching to assign a value to images or other files on their platforms.[22] After a value is assigned, the corporations use a hash matching software program to digitally compare the values with NCMEC's list of known exploitative child abuse images.[23] Although many private corporations currently use hash value matching, there is a circuit split about the reliability of a corporation's confirmed match without human verification.[24]

This Note argues that the Supreme Court has a duty to prevent pedophiles from continually victimizing innocent children; therefore, the Supreme Court must establish that hash value matching is reliable evidence without circumventing the probable cause requirement by incorporating this Note's proposed test for determining the admissibility and reliability of private party hash value matching when used with or without human confirmation. Section II of this Note discusses hash value matching in detail by examining historical context,[25] constitutional implications,[26] jurisprudence,[27] and statutes.[28] Section III discusses how establishing a test for the use of hash value matching provides clarity and benefits for those tasked with investigating and reporting child pornography.[29]

---

19. *See* Matthew K. Wegner, *Teaching Old Dogs New Tricks: Why Traditional Free Speech Doctrine Supports Anti-Child-Pornography Regulations in Virtual Reality*, 85 MINN. L. REV. 2081, 2088 (2001).

20. Henzey, *supra* note 11, at 55–56.

21. Rebekah A. Branham, *Hash It Out: Fourth Amendment Protection of Electronically Stored Child Exploitation*, 53 AKRON L. REV. 217, 218 (2019).

22. *See* Nicholas Weaver, *Encryption and Combating Child Exploitation Imagery*, LAWFARE (Oct. 23, 2019, 9:00 AM), https://www.lawfareblog.com/encryption-and-combating-child-exploitation-imagery.

23. *Id.*

24. *See* United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016); United States v. Reddick, 900 F.3d 636 (5th Cir. 2018); United States v. Wilson, 13 F.4th 961 (9th Cir. 2021); United States v. Miller, 982 F.3d 412 (6th Cir. 2020).

25. *See infra* Section II, Part A.

26. *See infra* Section II, Part B.

27. *See infra* Section II, Part C.

28. *See infra* Section II, Part D.

29. *See infra* Section III.

II. HASH VALUE MATCHING

A hash value is like a digital fingerprint of an image.[30] It is typically defined as a number represented through a sequence of characters and numbers that produces an algorithm based on each digital file.[31] NCMEC uses hash value matching to assign a unique identifier, or a value, to child sexual abuse images when it identifies an image containing known CSAM.[32] Once an image receives a value, it is uploaded to a database and shared with electronic and internet service providers ("Providers").[33] Only images identified by NCMEC as containing CSAM are flagged and given a hash value.[34] When an image is assigned a value, the image is digitally divided into "squares and assign[ed] a numerical value that represents the unique shading found within each square."[35] By comparing the value to a possible CSAM image, the program can measure the similarities between a given square and determine if there is a hash match between the image and the value based on each having identical numerical identifiers in that square.[36]

Providers use these values assigned to known CSAM to digitally compare with images on its platforms on the internet.[37] If an unassigned image on a Provider's platform contains the same sequence of characters and numbers as a value previously identified on NCMEC's database, then there is a match.[38] This technology allows private companies to quickly identify, or "match," suspicious material from a large number of sexual abuse images without the need for human-run searches.[39] When a Provider runs a hash program that digitally compares known values to images on its platform and an image matches a known value identified on NCMEC's database, then the

30. United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016).

31. United States v. Miller, 982 F.3d 412, 418 (6th Cir. 2020).

32. NCMEC, *CyberTipline*, *supra* note 9.

33. *Id.*; *Internet Service Provider*, CORNELL L. SCH. (July 2020), https://www.law.cornell.edu/wex/internet_service_provider_(isp)#:~:text=An%20Internet%20service%20provider%20%20and%20state%20level ("An Internet service provider (ISP) is an entity that provides broadband service to subscribers."); 18 U.S.C. § 2510(15) (noting an electronic communication service is "any service which provides to users thereof the ability to send and receive wire or electronic communications").

34. *See* NCMEC, *CyberTipline*, *supra* note 9.

35. Microsoft News Ctr., *Tackling Proliferation of Child Abuse Material with PhotoDNA*, MICROSOFT (Nov. 18, 2013), https://news.microsoft.com/en-gb/2013/11/18/tacklingproliferatio/#:~:text=In%20December%202009%2C%20Microsoft%20donated%20PhotoDNA%20to%20NCMEC,help%20stop%20these%20images%20from%20being%20redistributed%20online.

36. *Id.*

37. Weaver, *supra* note 22.

38. Branham, *supra* note 21, at 218; United States v. Reddick, 900 F.3d 636, 637 (5th Cir. 2018).

39. Branham, *supra* note 21, at 219.

company creates a report and forwards it to NCMEC.[40] After NCMEC confirms the image and the known hash value for a match, it shares the report with the appropriate law enforcement agency and a criminal investigation begins.[41] In this capacity, hash value matching's purpose is to find CSAM and reduce the growing quantity online.[42]

Part A of this Section discusses the historical background leading up to today's hash technology that Providers use to report CSAM.[43] Part B analyzes NCMEC's impact on discovering CSAM online and details the Fourth Amendment's role relating to the private party doctrine and warrantless searches.[44] Part C examines different circuit approaches[45] and explains the result of the circuit split.[46] Finally, Part D discusses the statutes that establish the laws Providers follow relating to reporting CSAM.[47]

A. Historical Background

Internet expansion fueled the epidemic of child pornography;[48] consequently, eliminating the spread and distribution of CSAM must be a priority. In 1998, NCMEC created CyberTipline in response to an increase in online sources reporting the sexual exploitation of minors on their platforms.[49] Today, CyberTipline receives reports from the public and Providers about the sexual exploitation of minors.[50] This Note focuses specifically on the reports from Providers.

More than a decade after the creation of CyberTipline—in light of the prevalence of online child pornography—Microsoft, in partnership with Dartmouth College, created PhotoDNA.[51] PhotoDNA is a software program that instantly analyzes files against known illicit image signatures to find hash value matches.[52] Microsoft developed this program to create a more accurate and reliable way to match unidentified child sexual abuse images to known values than the value matching systems previously used by law enforcement

40. Weaver, *supra* note 22.
41. Branham, *supra* note 21, at 220.
42. *See id.* at 218.
43. *See infra* Section A.
44. *See infra* Section B.
45. *See infra* Section C, 1–4.
46. *See infra* Section C, 5.
47. *See infra* Section D.
48. Henzey, *supra* note 11, at 6.
49. NCMEC, *CSAM*, *supra* note 12.
50. *Id.*
51. Branham, *supra* note 21, at 219; Microsoft News Ctr., *supra* note 35.
52. Branham, *supra* note 21, at 219; *PhotoDNA*, MICROSOFT, https://www.microsoft.com/en-us/photodna (last visited Feb. 20, 2023).

and technology companies.[53] In 2015, after Microsoft donated PhotoDNA to NCMEC in 2009,[54] Microsoft made it available as a service on Azure, a public cloud computing platform.[55] This allowed cloud service companies of all sizes to use PhotoDNA.[56] Since becoming publicly accessible, over 1,400 companies have used PhotoDNA and make reports to NCMEC.[57] In 2021, NCMEC disclosed that the CyberTipline received 29.3 million reports, with Providers creating 29.1 million of the reports.[58] Of those Providers that reported child sexual abuse images to NCMEC, the list included companies like Google, Microsoft, Twitter, AOL, TikTok, and Facebook.[59]

Of the more than 1,400 companies registered to report child abuse to NCMEC,[60] Google is one of the largest reporters.[61] Per Google's terms of service, it actively removes illegal images depicting child sexual abuse from its platform.[62] When Google is alerted to possible sexual abuse images, it is either through hash value matching of a value to a known CSAM image or an alert to new and unknown CSAM that requires a human employee confirm the shown abuse in the image before the reporting process can continue.[63] These employees are trained on the federal definition of child pornography and can accurately identify such to assign a value to the image.[64] After receiving the alert to unknown CSAM, to properly identify it and assign a hash, Google

53. Microsoft News Ctr., *supra* note 35 (noting that Microsoft expanded on MD5 and SHA-1 matching which were the first means that law enforcement and technology companies used hash value techniques to match images).

54. *Id.*

55. *PhotoDNA*, *supra* note 52; Logan McCoy, *Microsoft Azure Explained: What It Is and Why It Matters,* CCB TECH., https://ccbtechnology.com/what-microsoft-azure-is-and-why-it-matters/ (last visited Feb. 20, 2023) (explaining that Azure provides users with different services, such as PhotoDNA).

56. *PhotoDNA*, *supra* note 52.

57. NCMEC, *CSAM*, *supra* note 12 (noting NCMEC has over 1,400 registered reporters for CyberTipline).

58. NCMEC, 2021 REPORT, *supra* note 9; NCMEC, *CyberTipline*, *supra* note 9.

59. NCMEC, 2021 REPORT, *supra* note 9; United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016); Branham, *supra* note 21, at 243.

60. NCMEC, *CSAM*, *supra* note 12.

61. NCMEC, 2021 REPORT, *supra* note 9. In 2021, Google was the fourth highest reporter with 875,783 reports sent to NCMEC. *Id.* Facebook was the top reporter with 22,118,952 reports. *Id.*

62. *Google Terms of Service*, GOOGLE (Jan. 5, 2022), https://www.gstatic.com/policies/terms/pdf/20220105/it7r24p9/google_terms_of_service_en_us.pdf; Mark Hachman, *How Google Handles Child Pornography in Gmail, Search*, PCWORLD (Aug. 5, 2014, 10:34 AM), https://www.pcworld.com/article/440661/how-google-handles-child-pornography-in-gmail-search.html.

63. Susan Jasper, *How We Detect, Remove and Report Child Sexual Abuse Material*, GOOGLE (Oct. 28, 2022), https://blog.google/technology/safety-security/how-we-detect-remove-and-report-child-sexual-abuse-material/; Hachman, *supra* note 62.

64. United States v. Miller, 982, F.3d 412, 430–31 (6th Cir. 2020); Jasper, *supra* note 63.

compares it with known CSAM images on its internal repository, which includes images that are shared from NCMEC's database.[65] Google uses its database of known child sexual abuse images and scans Gmail for any images with the same digital value.[66] If any files "match," Google creates and submits a report that includes the files and user's IP address to NCMEC.[67] In 2013, NCMEC shared "10,498 notices of suspected child sexual abuse images" with Providers to compare with the hash values on its platform.[68] As of 2021, NCMEC's database contained more than 5 million images.[69] Google has contributed 1.99 million known images of child sexual abuse to NCMEC's database of known hash values.[70]

Private CSAM searches, such as those run by Google, are purely voluntary.[71] As a result, a company avoids liability for failing to report CSAM if it lacks knowledge of the facts or circumstances.[72] A company lacks knowledge of the facts or circumstances if it is unclear that an image is an apparent or imminent violation of any of the federal statutes for child pornography.[73] While private CSAM searches are purely voluntary, in 2021, NCMEC received reports from hundreds of corporations that used hash value matching to identify 85 million child abuse files.[74] Despite the fact that NCMEC received 85 million files,[75] every year, countless household names—like Apple—do not consistently report high numbers of CSAM.[76]

In 2019, following an article about the proliferation of child sexual abuse images online, members of Congress pressured Apple to do better to combat

---

65. Hachman, *supra* note 62; *Google Transparency Report*, GOOGLE, https://transparencyreport.google.com/child-sexual-abuse-material/reporting (last visited Feb. 20, 2023); Jasper, *supra* note 63.

66. *Miller*, 982 F.3d at 417.

67. *Id.*

68. Hachman, *supra* note 62.

69. NCMEC, *CyberTipline*, *supra* note 9.

70. *Google Transparency Report*, *supra* note 65.

71. 18 U.S.C. § 2258A(f); Branham, *supra* note 21, at 220.

72. *See* 18 U.S.C. § 2258A(a)(1)(A)(i).

73. 18 U.S.C. § 2258A(a)(2) (noting the United States Code sections for child pornography are 18 U.S.C. §§ 2251, 2251A, 2252, 2252A, 2252B, and 2260).

74. *See* NCMEC, *CyberTipline*, *supra* note 9 (including 39.9 million image files and 44.8 million video files).

75. *Id.*

76. *See* NCMEC, 2021 REPORT, *supra* note 9 (Apple making 160 reports); NAT'L CTR. FOR MISSING AND EXPLOITED CHILD., 2020 REPORTS BY ELECTRONIC SERVICE PROVIDERS (ESP) 1 (2021), https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf (Apple making 265 reports); NAT'L CTR. FOR MISSING AND EXPLOITED CHILD., 2019 REPORTS BY ELECTRONIC SERVICE PROVIDERS (ESP) 1 (2020) [hereinafter NCMEC, 2019 REPORT], https://www.missingkids.org/content/dam/missingkids/pdfs/2019-reports-by-esp.pdf (Apple making 205 reports).

child pornography on its platform.[77] Eighteen months later, Apple announced its hash value matching program to search the images of every user's iPhone in the United States before uploading them to iCloud.[78] Apple's technology would require each photo uploaded onto a user's iCloud to receive a hash value.[79] If thirty or more of a user's photos matched to known CSAM, an Apple employee would review the images and follow its procedure for reporting the user to the authorities.[80] However, Apple faced criticism based on societal fears that the technology could spy on citizens;[81] consequently, less than one month after the announcement, Apple conceded to the critics and delayed the launch without a set launch date.[82] Until more Providers, such as Apple, begin actively investigating child pornography on internet platforms,[83] thousands of victims will go unnoticed.

B. The Fourth Amendment Explained in Light of Hash Value Matching

Hash matching is a search under the Fourth Amendment when the government conducts the search rather than a private company.[84] The Fourth Amendment guarantees a person's protection against unreasonable searches and seizures of his or her person, houses, papers, and effects.[85] This protection requires law enforcement to obtain a search warrant based on probable cause before conducting a search.[86] In this context, a search within the meaning of the Fourth Amendment is the government's infringement upon an expectation of privacy that society is prepared to recognize as reasonable.[87] Removing child pornography is vital; however, the government cannot circumvent the

77. Jack Nicas, *Are Apple's Tools Against Child Abuse Bad for Your Privacy?*, N.Y. TIMES (Oct. 14, 2021), https://www.nytimes.com/2021/08/18/technology/apple-child-abuse-tech-privacy.html.

78. *Id.*; *Expanded Protections for Children*, APPLE, https://www.apple.com/child-safety/ (last visited Feb. 20, 2023).

79. Nicas, *supra* note 77.

80. *Id.*

81. Jonathan Mayer & Anunay Kulshrestha, *We Built a System Like Apple's to Flag Child Sexual Abuse Material—and Concluded the Tech Was Dangerous*, WASH. POST (Aug. 19, 2021, 12:09 PM), https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/.

82. Reed Albergotti, *Apple Delays the Rollout of Its Plans to Scan iPhones for Child Exploitation Images*, WASH. POST (Sept. 3, 2021, 3:57 PM), https://www.washingtonpost.com/technology/2021/09/03/apple-delay-csam-scanning/.

83. *See* NCMEC, 2021 REPORT, *supra* note 9 (indicating the differences in reporting on various Provider platforms).

84. United States v. Miller, 982 F.3d 412, 417 (6th Cir. 2020).

85. U.S. CONST. amend. IV.

86. *Id.*; Katz v. United States, 389 U.S. 347, 357 (1967).

87. Branham, *supra* note 21, at 221.

Fourth Amendment without a valid exception.[88] Nevertheless, an exception applies to hash value matching: the private party doctrine.[89] This exception may apply when a Provider, such as Google, hash matches images on its platform with NCMEC's database, assuming the Provider is not acting with or as a government agent when it sends a report of the match to law enforcement and law enforcement opens the report to investigate.[90] When law enforcement receives a CSAM report, an agent's investigation into the reported material by examining the image is a government search that must conform to the Fourth Amendment.[91]

The Supreme Court's decision in *Katz v. United States* clarified the protections given to an individual under the Fourth Amendment by holding that a person has an expectation of privacy in public places, such as a telephone booth, when the person makes efforts to exclude the public.[92] The Court established two important conclusions that still stand today. First, the Fourth Amendment not only protects a person's rights against seizures of tangible items but also extends to recording oral statements that he or she sought to exclude from the outside world.[93] Second, without probable cause and a search warrant, a law enforcement officer cannot execute a search that infringes on a person's constitutionally protected rights.[94] To this end, the Supreme Court effectively expanded a person's Fourth Amendment right to focus on the individual's expectation of privacy rather than physical location.[95]

The Supreme Court's opinion in *United States v. Jacobsen* further examined the Fourth Amendment's warrant requirement and established the private party exception, which tests the invasion of privacy against the degree to which law enforcement expanded the initial private search.[96] In *Jacobsen*, FedEx employees, within the course of business, conducted a private search of a package after a forklift damaged it and uncovered a white substance presumed to be drugs.[97] After FedEx called law enforcement, an agent opened

88. United States v. Wilson, 13 F.4th 961, 974 (9th Cir. 2021).

89. United States v. Jacobsen, 466 U.S. 109, 113 (1984); United States v. Ackerman, 831 F.3d 1292, 1300–01 (10th Cir. 2016); United States v. Montijo, No. 2:21-cr-75-SPC-NPM, 2022 U.S. Dist. LEXIS 4577, *7 (M.D. Fla. Jan. 10, 2022).

90. *Jacobsen*, 466 U.S. at 113; *Ackerman*, 831 F.3d at 1300–01; *Montijo*, 2022 U.S. Dist. LEXIS at *7.

91. *See* United States v. Miller, 982 F.3d 412, 417 (6th Cir. 2020).

92. *See* Katz v. United States, 389 U.S. 347, 349 (1967).

93. *Id.* at 352–53.

94. *Id.* at 357.

95. *Id.* at 353; Tyler O'Connell, *Two Models of the Fourth Amendment and Hashing to Investigate Child Sexual Abuse Material*, 53 U. PAC. L. REV. 293, 305 (2021).

96. United States v. Jacobsen, 466 U.S. 109, 115 (1984); United States v. Bonds, No. 5:21-cr-00043-KDB-DCK, U.S. Dist. LEXIS 196765 2, 8 (W.D.N.C. Oct. 13, 2021).

97. *Jacobsen*, 466 U.S. at 111.

the package to determine its contents.[98] Since FedEx previously opened the box, the agent did not expand the search when he reopened it.[99] Additionally, the agent conducted a chemical test to determine if it was cocaine.[100] The presumptive chemical field test also was not an expansion of the initial search because the agent could only learn whether the powder was or was not cocaine.[101] *Jacobsen* established that the private party doctrine is applicable when law enforcement conducts a secondary search that does not exceed the bounds of the initial search.[102]

As a result of the holding in *Jacobsen*, when a Provider conducts a hash value search with human confirmation that is not the result of government interference, law enforcement can view the matched images under the private party exception because the government search is not an expansion of the initial private search.[103] Therefore, when law enforcement investigates CSAM after a Provider search, the Fourth Amendment only requires a search warrant if law enforcement expands upon the initial hash value search.[104]

C. Landmark Judicial Decisions Resulting in a Circuit Split

With the rapid expansion of technology resulting in laws becoming ineffective to combat child pornography on the internet,[105] a split ensued among the federal circuit courts regarding the evidentiary weight of hash value matching.[106] The circuit courts generally agree a Provider can conduct hash value matching searches, and if a human within the company views the material from the match, the government may view the exact same material.[107] However, the root of the disagreement is whether the hash value match is sufficiently reliable on its own to establish probable cause[108] or whether a

98. *Id.*
99. *Id.* at 119.
100. *Id.* at 112.
101. *Id.* at 122.
102. *Id.* at 116.
103. United States v. Wilson, 13 F.4th 961, 974 (9th Cir. 2021); *Jacobsen*, 466 U.S. at 111–12, 119, 122.
104. *See Jacobsen*, 466 U.S. at 117–18.
105. Henzey, *supra* note 11, at 53.
106. *See generally* United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016); United States v. Reddick, 900 F.3d 636 (5th Cir. 2018); United States v. Wilson, 13 F.4th 961 (9th Cir. 2021); United States v. Miller, 982 F.3d 412 (6th Cir. 2020).
107. Rachel Haney, *Best of ABA Section Science and Technology Law Addressing the Increase of Online Child Sexual Abuse in the Pandemic*, 38 GPSOLO 77, 78 (2021).
108. Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (explaining that probable cause exists where an officer has facts or circumstances within his knowledge that are sufficient to inform a man of reasonable caution to believe a crime is being or has been committed).

Provider needs an employee to confirm the match before law enforcement can investigate.[109]

1. The Tenth Circuit

When the United States Court of Appeals for the Tenth Circuit analyzed the search with respect to the private party doctrine, it held NCMEC is a government entity or agent that cannot expand or exceed a private search without a warrant.[110] In this case, AOL intercepted an email Ackerman sent that contained child pornography images.[111] Through AOL's hash matching automated system designed to "thwart the transmission of child pornography," AOL identified one of four images attached to Ackerman's email as child pornography.[112] Once AOL created a report and sent it to NCMEC, who viewed all four images without a search warrant, NCMEC sent it to law enforcement who then viewed the images without a search warrant.[113]

In *Ackerman*, the court classified NCMEC as a government entity or agent because it receives substantial federal funding, law enforcement officers participate in its daily functions, and NCMEC's law enforcement powers go beyond that of private citizens.[114] Subsequently, since NCMEC is a government entity, the court considered whether NCMEC simply repeated AOL's search or exceeded the scope of the initial search and violated Ackerman's constitutional rights.[115] Since NCMEC is a government entity, the court found that NCMEC exceeded the scope of the initial search when it viewed Ackerman's entire email.[116] Even though AOL reported one match, NCMEC expanded the search by viewing the other three attachments since AOL's program did not match those attachments.[117] Government agents expanding beyond the initial Provider search, such as viewing all three email attachments when the Provider only matched to one, prevents the private party doctrine from applying; thus, the Fourth Amendment requires the agents to obtain a search warrant.[118]

---

109. Haney, *supra* note 107, at 78; *see Ackerman*, 831 F.3d at 1294; *Reddick*, 900 F.3d at 639; *Wilson*, 13 F.4th at 967; *Miller*, 982 F.3d at 419.

110. *Ackerman*, 831 F.3d at 1308–09.

111. *Id.* at 1294.

112. *Id.* At the time AOL received the hash match, no AOL employee viewed the images from Ackerman's email. *Id.* However, AOL previously identified and deemed the image from the match as child pornography. *Id.*

113. *Id.*

114. *Id.* at 1296, 1298.

115. *Id.* at 1295.

116. *Ackerman*, 831 F.3d at 1306.

117. *Id.* at 1294, 1304, 1306.

118. *Id.* at 1294, 1308.

2. The Fifth Circuit

The Fifth Circuit's analysis of the private party doctrine in *Reddick* focused on a user's expectation of privacy on an internet platform during a hash value match search.[119] Henry Reddick uploaded child pornography images onto his Microsoft SkyDrive, a personal cloud storage device.[120] After he uploaded the images, Microsoft's PhotoDNA program automatically compared the images to a database for known exploitative images and got a match.[121] Microsoft reported the match to NCMEC.[122] Subsequently, NCMEC forwarded the information to Detective Ilse, who opened each file to confirm it was child pornography.[123]

The court relied upon *Jacobsen*[124] to analyze Detective Ilse's warrantless search and held the search was constitutional because Reddick uploaded the images to his SkyDrive, and his expectation of privacy was frustrated by Microsoft's initial search.[125] When Detective Ilse opened the files, he already knew the values matched child pornography and the visual confirmation merely dispelled any doubt the images were not child pornography.[126] The court found this because hash value matching "'allows law enforcement to identify child pornography with almost absolute certainty' since hash values are 'specific to the makeup of a particular image's data.'"[127] Consequently, the search did not violate Reddick's Fourth Amendment rights.[128] Thus, there was no significant invasion of privacy to constitute a separate search because the hash value match allowed the detective to know with "almost absolute certainty" that the report contained child pornography.[129] Detective Ilse's secondary search was constitutional under the private party doctrine because law enforcement effectively learned nothing from viewing the files.[130]

119. *See* United States v. Reddick, 900 F.3d 636, 638 (5th Cir. 2018).
120. *Id.* at 637–38.
121. *Id.* at 639. Although no one confirmed the images at the time of the match, it is unclear from the opinion whether Microsoft employees previously confirmed the images from the database. *Id.*
122. *Id.* at 638.
123. *Id.*
124. *Id.* at 639; *see* United States v. Jacobsen, 466 U.S. 109, 126 (1984).
125. *Reddick*, 900 F.3d at 639.
126. *Id.*
127. *Id.* (quoting United States v. Larman, 547 F. App'x 475, 477 (5th Cir. 2013)).
128. *Id.* at 640.
129. *Id.* at 639.
130. *Id.* at 640.

3. The Sixth Circuit

Two years later, in *United States v. Miller*, the Sixth Circuit found that Google's private search of Miller's Gmail did not violate his Fourth Amendment rights under the private party doctrine.[131] In his appeal, Miller did not question the reliability of the hash value matching program and the court found the agent's subsequent search following Google's initial search was reasonable.[132] Google's software indicated two of Miller's files contained child pornography.[133] Before Google even searched Miller's email, its employees confirmed the same images and uploaded them to Google's child pornography repository.[134] Google used this repository to match the images in Miller's email to child pornography and sent NCMEC a report of the matched values.[135] After NCMEC investigated the allegations, it turned the information over to law enforcement.[136] Once law enforcement obtained the report, Detective Schihl confirmed the files were child pornography.[137] While the court did note, conceivably, there was a chance to stumble upon new information from an unreliable match and exceed the initial search, it was unlikely as "the chance of two files coincidentally sharing the same hash value is 1 in 9,223,372,036,854,775,808."[138] Since Miller did not question the hash technology, the Sixth Circuit deferred to the lower court's ruling that the hash value matching technology was accurate and highly reliable.[139] The court used *Jacobsen* to analyze Detective Schihl's warrantless search and found the private party doctrine applied because he did not go further than Google's initial search and did not learn anything new.[140]

4. The Ninth Circuit

In *United States v. Wilson*, the court found Google's hash value match, which NCMEC conveyed to the San Diego Internet Crimes Against Children Task Force ("ICAC"), was a search within the meaning of the Fourth Amendment, and ICAC's agent violated Wilson's right to privacy by opening the

131. 982 F.3d 412, 429–30, 433 (6th Cir. 2020).
132. *Id.* at 430.
133. *Id.* at 417.
134. *Id.* at 429.
135. *Id.*; Pierre Grosdidier, *Hash Values and the Fourth Amendment: Do Authorities Need a Search Warrant to Open and View Files?*, 84 TEX. BUS. J. 578, 578 (2021).
136. *Miller*, 982 F.3d at 420.
137. *Id.*
138. Grosdidier, *supra* note 135, at 578; *Miller*, 982 F.3d at 430 (quoting United States v. Dunning, No. 7:15-cr-4-DCR-1, 2015 U.S. Dist. LEXIS 140993, *7 (E.D. Ky. Oct. 1, 2015)).
139. *Miller*, 982 F.3d at 418.
140. *Id.* at 429–30.

email attachments.[141] Google's private hash value search of Wilson's email uncovered four images matching child pornography.[142] After creating the report, Google sent it to NCMEC before an employee confirmed the images.[143] Once NCMEC received the report, again, without an employee's visual confirmation, it turned the report over to ICAC.[144] Agent Thompson, without a warrant, opened each attachment and determined that the email contained child pornography images.[145] The Ninth Circuit reversed the California Court of Appeal's holding that the government's warrantless search of the images was permissible under the private search doctrine.[146] Agent Thompson needed a search warrant for the unconfirmed hash value match because the private party doctrine did not apply after he expanded the search beyond the parameters of the match.[147] *Wilson* was the first case to question the reliability of the hash value match, and with little evidence introduced at trial, the court held it could not prove the hash value program was sufficiently reliable to conclude that two hashes indicated child pornography was present without prior human confirmation.[148]

5. The Result of the Circuit Split

The circuits that have analyzed the accuracy and reliability of hash value matching when used by private parties to report CSAM differ on if a hash value match is reliable for law enforcement to view the actual image after an initial private search without a search warrant or human confirmation. Some circuits, such as the Fifth and Sixth,[149] view hash value matching technology, without human confirmation, as inherently reliable as there is a one-in-one billion chance of a false match.[150] Whereas others, such as the Ninth and Tenth Circuits, do not find hash value matches accurate indicators of the presence of child pornography unless there has been human confirmation before the Provider reports the match.[151] As a result, the circuits are split as to the reliability of hash value matching when it applies to the use of the private party

141. 13 F.4th 961, 979–80 (9th Cir. 2021).
142. *Id.* at 965.
143. *Id.*
144. *Id.*
145. *Id.*
146. *See id.* at 966 n.5, 971–72.
147. *Wilson*, 13 F.4th at 973–74.
148. *Id.* at 971–72, 979.
149. *See generally* United States v. Reddick, 900 F.3d 636 (5th Cir. 2018); United States v. Miller, 982 F.3d 412 (6th Cir. 2020).
150. *Miller*, 982 F.3d at 429–30.
151. *See generally* United States v. Wilson, 13 F.4th 961 (9th Cir. 2021); United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016).

doctrine for the expansion of a Provider match before law enforcement must obtain a search warrant.

D. Statutes and Legislation Effecting Hash Value Matching

Child pornography is not only found on the "dark web;" it is virtually everywhere.[152] In an effort to eliminate child pornography, Congress enacted the Child Pornography Prevention Act, which criminalized virtual child pornography by including images modified or generated using a computer that made it appear that a minor is engaging in sexual conduct.[153] However, the Supreme Court struck this provision with *Ashcroft v. Free Speech Coalition*, holding that absent any harm to a minor from the digitally created child pornography, the material would receive First Amendment protections.[154] On the heels of the *Ashcroft* decision, Congress passed the PROTECT Act in 2003.[155] This Act criminalized known "production, distribution, receipt, or possession of images," including those images depicting a minor engaging in sexually explicit conduct in "a drawing, cartoon, sculpture, or painting" as child pornography.[156]

1. The PROTECT Our Children Act

Following the PROTECT Act, Congress enacted the PROTECT Our Children Act of 2008.[157] The PROTECT Our Children Act established various laws combating child abuse without mandating Providers actively monitor and investigate CSAM on its platforms.[158] For example, 18 U.S.C. § 2258A explains a Provider must report CSAM as soon as reasonably possible after gaining "actual knowledge of any facts or circumstances" of apparent or imminent violations of the child pornography statutes.[159] This statute is

152. NCMEC, *CSAM*, *supra* note 12; Christopher Campbell, *Web of Lives: How Regulating the Dark Web Can Combat Online Human Trafficking*, 38 J. NAT'L ASS'N L. JUD. 136, 146 (2018). The "dark-web" is a hidden part of the internet to most average users. *Id.* Typically, people use these networks for criminal purposes. *Id.* A user can intentionally remain anonymous and avoid any kind of detection. *Id.*

153. Alexandra L. Mitter, *Deputizing Internet Service Providers: How the Government Avoids Fourth Amendment Protections*, 67 N.Y.U. ANN. SURV. AM. L. 235, 240 (2011).

154. 535 U.S. 234, 241, 257 (2002); Mitter, *supra* note 153, at 240 (noting that there was no First Amendment violation because it was pornography that depicted minors, but did not use real minors; thus, it was not obscene).

155. Mitter, *supra* note 153, at 240; Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act of 2003, Pub. L. No. 108-21, 117 Stat. 650.

156. Mitter, *supra* note 153, at 240; PROTECT Act of 2003 § 504.

157. PROTECT Our Children Act of 2008, Pub. L. No. 100-401, 122 Stat. 4229; Mitter, *supra* note 153, at 245.

158. PROTECT Our Children Act of 2008; Mitter, *supra* note 153, at 245.

159. 18 U.S.C. § 2258A; Mitter, *supra* note 153, at 273.

voluntary, meaning a Provider is not required to actively look for and report child sexual abuse on its platform[160] unless it has "actual knowledge of any facts or circumstances" of apparent or imminent CSAM.[161] Additionally, 18 U.S.C. § 2258C(a) establishes that NCMEC may share elements relating to any apparent child pornography image of an identified child to stop the transmission of the image with Providers.[162] This establishes the authority to use hash value matching against NCMEC's list of known child pornography.[163] Consequently, NCMEC can send Providers the unique identities of child pornography images using hash values because the Providers cannot see the actual image.[164] The enactment of the PROTECT Our Children Act expanded the child pornography laws and implemented a duty on Providers to report CSAM in an effort to remove it from the internet.[165]

2. Immunity Statutes for Providers

Congress passed Section 230 of the Communications Decency Act of 1996 ("Section 230") to promote the continued growth of the internet, and in order to promote that growth, it included protections for Providers against lawsuits for their users' posts, such as those that are CSAM.[166] Section 230 grants a Provider civil and criminal immunity for failing to report or investigate child pornography.[167] Under Section 230, a Provider is not liable as a speaker for the material posted on its platform, including child pornography images.[168]

Congress also enacted 18 U.S.C. § 2258B to provide civil and criminal immunity for investigating and reporting CSAM.[169] This statute stipulates that a Provider, including its directors, officers, employees, or any agent of the Provider, will have immunity for their performance arising out of

160. 18 U.S.C. § 2258A; Mitter, *supra* note 153, at 273.
161. Branham, *supra* note 21, at 220; 18 U.S.C. § 2258A.
162. 18 U.S.C. § 2258C(a).
163. 18 U.S.C. § 2258C(a)(2)–(3).
164. *Id.*
165. Melissa Hamilton, *The Child Pornography Crusade and Its Net-Widening Effect*, 33 CARDOZO L. REV. 1679, 1684–85 (2012); Mitter, *supra* note 153, at 268.
166. ASHELY JOHNSON & DANIEL CASTRO, OVERVIEW OF SECTION 230: WHAT IT IS, WHY IT WAS CREATED, AND WHAT IT HAS ACHIEVED, 1 (2021); *See* Anirudh Krishna, Note, *Internet.gov: Tech Companies as Government Agents and the Future of the Fight Against Child Sexual Abuse*, 109 CALIF. L. REV. 1581, 1590–91 (2021) (noting Section 230 was passed to promote innovation online and help Providers moderate its platform and users without fear of liability); Communications Decency Act of 1996, Pub. L. 104-104, 110 Stat. 56, § 509 (codified as amended at 47 U.S.C. § 230).
167. Krishna, *supra* note 166, at 1590; 47 U.S.C. § 230(c)(1).
168. Krishna, *supra* note 166, at 1591; 47 U.S.C. § 230(c)(1).
169. 18 U.S.C. § 2258B.

investigating or reporting child pornography to comply with 18 U.S.C. § 2258A.[170] Immunity applies as long as no Provider engages in (1) intentional misconduct; (2) acts or fails to act with actual malice or reckless disregard to a substantial risk of causing physical injury without legal justification; or (3) some other purpose unrelated to the performance of any responsibility or function under Sections 2258B, 2258A, 2258C, 2702, or 2703 when investigating and reporting online sexual exploitation of children.[171]

3. The Impact of 18 U.S.C. § 2258A on United States CyberTipline Reports

While Congress has granted Providers civil and criminal immunity for reporting CSAM, most of the 2021 CyberTipline reports were not from the United States.[172] However, even with 18 U.S.C. § 2258A prescribing a duty on Providers to report CSAM when it knows of the facts and circumstances because it is a voluntary duty, CSAM in this country cannot be properly identified and reported because proxies, anonymizers, and other technological advancements give predators the ability to go undetected.[173] Without NCMEC indicating which Providers reported CSAM originating from the United States and from how many United States users, it cannot be clearly established if the reported users are only active outside of the United States or if proxies and anonymizers are masking their true location.[174] Section 2258A's reportability requirement for a Provider to have "actual knowledge of any facts or circumstances" before it is mandated to report arguably impacts the amount of CSAM reported for United States users since it creates an additional level of knowledge before reporting is mandatory.[175]

---

170. 18 U.S.C. § 2258B(a).

171. 18 U.S.C. § 2258B(b).

172. *See* NAT'L. CTR. FOR MISSING AND EXPLOITED CHILD., 2021 CYBERTIPLINE REPORTS BY COUNTRY (2022) [hereinafter NCMEC, 2021 CYBERTIPLINE REPORTS BY COUNTRY], https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-country.pdf (noting the reported numbers are not indicative of the CSAM in a specific country since multiple factors can impact the reported country such as proxies, anonymizers, or even another country applying their own national standards for CSAM).

173. *Id.* (showing that in 2021, only 716,474 of the 29.3 million reports to NCMEC's CyberTipline were directed to IP addresses for United States users).

174. *Id.*; *Anonymize*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/anonymizers (last visited Feb. 20, 2023) ("[T]o remove identifying information from (something, such as computer data) so that the original source cannot be known . . . .").

175. NCMEC, 2021 CYBERTIPLINE REPORTS BY COUNTRY, *supra* note 172; 18 U.S.C. § 2258A(a)(1)(A).

III. HASH VALUE MATCHING: PRECEDENT IS VITAL FOR THE MATCH

Because the Supreme Court has rejected to hear any circuit court's decision on hash value matching,[176] the courts are no closer to having a uniform answer as to whether hash value matching conforms to the Constitutional probable cause requirement. The Supreme Court establishing precedent would encourage more Providers to monitor its platforms for CSAM generated or accessed in the United States. A Provider routinely using hash value matching software to locate CSAM on its platform does not transform into a government agent merely for the "mutual interest in eradicating child pornography;" instead, the courts interpret a Provider's actions as a private party search.[177] Between the circuits, the predominant issue is whether a hash value match, without human confirmation, is *reliable* probable cause to apply for a search warrant.[178] If the match alone is not sufficient for law enforcement to establish probable cause, the Provider must have an employee confirm the image or use one of the Fourth Amendment's warrant exceptions, such as the private party doctrine.[179] However, if the hash match is reliable on its own, in that it identifies the matched image depicts a minor engaging in sexually explicit conduct, it is sufficient evidence of probable cause for law enforcement to obtain a search warrant.[180] To explain the need for Supreme Court precedent for hash value matching, this Section focuses on the reliability of hash values and how a hash value match alone may be a reliable piece of evidence in a probable cause affidavit.

A. Reliability of Hash Values

Two child pornography images may be identical to the naked eye, but there is a one-in-one billion chance two images will have the same hash value.[181] Similar to cocaine testing in *Jacobsen*, hash value matching for this purpose is inherently reliable since it is doubtful a value has multiple matches.[182] This is because, as the court in *Miller* suggests, a *computer's virtual* search of an individual file through hash value matching creates more certainty than a *person's manual* search of that same file.[183]

---

176. *See* United States v. Miller, 982 F.3d 412 (6th Cir. 2020), *cert. denied*, 141 S. Ct. 2797 (2021).

177. United States v. Bebris, 4 F.4th 551, 562 (7th Cir. 2021).

178. United States v. Bonds, No. 5:21-cr-00043-KDB-DCK, 2021 U.S. Dist. LEXIS 196765, at *9–10, *10 n.6 (W.D.N.C. Oct. 13, 2021).

179. *Id.* at *10 n.6, *7–9.

180. *Miller*, 982 F.3d at 428.

181. Branham, *supra* note 21, at 219; Dennis Martin, *Demystifying Hash Searches*, 70 STAN L. REV. 691, 716 (2018).

182. Branham, *supra* note 21, at 222.

183. *Miller*, 982 F.3d at 418.

Federal law criminalizes possessing, distributing, producing, viewing, or receiving child pornography,[184] but it does not describe the reliability of a hash value.[185] However, the accuracy of the technology itself is abundantly clear without any additional confirmation.[186] Since a hash value match has a one-in-one billion chance that two matches will be the same, a Provider's match is sufficient for law enforcement to rely upon as an indicator of CSAM because the match informs the officer of the presence of child pornography without an unreasonable invasion of privacy.[187] Therefore, even without human confirmation, based on *Miller* and the accuracy of the technology itself, an officer can use a match as probable cause to apply for a search warrant.[188]

The question is not whether the file *will* contain child pornography but whether it is *fairly probable* that the file will contain child pornography.[189] A match without human confirmation affirmatively answers the fairly probable burden for evidence of a crime because the matching program determines with a high standard of probability that each file matched contains a known image of child pornography.[190] As previously stated, if the two hashes match, the Provider forwards its report to NCMEC.[191] Hash value equations are unique in that any megapixel changed in the image will result in a new hash value.[192] In fact, creating and matching hash values is done with such a "high degree of accuracy" that police officers have noted hash matching is "more than 99.9999% reliable,"[193] which is considered more accurate than DNA at 99.99% accuracy.[194] The hash technology indicates with a high probability of 99.9999% that a file contains child pornography[195] while remaining minimally intrusive because the match is not the actual image but the image's algorithm.[196]

For example, DNA without a description of the individual or some other identifier is not sufficient probable cause for a search warrant of a "John Doe" because it is merely genetic makeup without any information accurately

184. 18 U.S.C. § 2251.
185. *See* Krishna, *supra* note 166, at 1590.
186. *Miller*, 982 F.3d at 430; United States v. Reddick, 900 F.3d 636, 639–40 (5th Cir. 2018).
187. Branham, *supra* note 21, at 219; Martin, *supra* note 181, at 716.
188. *See Miller*, 982 F.3d at 430 (interpreting the lower court's record who did not find any issues with the hash value match's reliability).
189. Branham, *supra* note 21, at 237–38.
190. Martin, *supra* note 181, at 724; United States v. Dunning, No. 7:15-cr-4-DCR-1, 2015 U.S. Dist. LEXIS 140993, at *5–6 (E.D. Ky. Oct 1, 2015).
191. Weaver, *supra* note 22.
192. Microsoft News Ctr., *supra* note 35.
193. Branham, *supra* note 21, at 219, 239; Martin, *supra* note 181, at 716.
194. *Dunning*, 2015 U.S. Dis. LEXIS 140993 at *7.
195. Branham, *supra* note 21, at 219, 239.
196. Martin, *supra* note 181, at 717.

identifying with "particularity describ[ing] the person to be seized."[197] However, as for hash value matching, not only does it identify with fair probability that the value depicts a minor engaging in sexually explicit conduct but also it informs law enforcement of an IP address attached to the reported CSAM.[198] Thus, unlike DNA alone, a match without human confirmation is a reliable indicator that the file contains child pornography and provides law enforcement with the IP address that includes the user's name and physical address of the device identified in the match.[199] Law enforcement can then use the information to meet the requisite burden for probable cause because it describes the person with particularity and reasonable certainty due to the affidavit's inclusion of the user's IP address.[200] With such reliable technology, mandating human confirmation before law enforcement applies for a search warrant is over-burdensome.[201]

When Microsoft created PhotoDNA,[202] it could not foresee the decision in *Wilson* questioning the reliability of a match without human confirmation.[203] Surely, Microsoft did not create PhotoDNA with the intention for it to be supplementary technology used after a person indicated the material was consistent with child pornography.[204] Before a reliable hash program was created, many companies still reported exploitative images of child abuse; however, without PhotoDNA, law enforcement could not distinguish between new images and those already identified.[205] Consequently, the process was very time-consuming.[206] While not always discernable to the human eye,[207] searching the megapixels, as with PhotoDNA, avoids false matches, which is

197. Frank B. Ulmer, *Using DNA Profiles to Obtain "John Doe" Arrest Warrants and Indictments*, 58 WASH. & LEE L. REV. 1585, 1600, 1604 (2001).

198. United States v. Miller, 982 F.3d 412, 417 (6th Cir. 2020).

199. *See* Branham, *supra* note 21 at 222; *Miller*, 982 F.3d, at 420 (noting once Google sends the reported CSAM, NCMEC takes the IP address listed in the report and searches for the name and address associated with the IP address using public search engines and "Whols lookup").

200. *See Miller*, 982 F.3d at 430; *see also* Ulmer, *supra* note 199, at 1600; Martin, *supra* note 181, at 703.

201. *See Miller*, 982 F.3d at 430 (acknowledging the hash value match without human confirmation was sufficient to use the evidence to obtain a search warrant); Ulmer, *supra* note 199, at 1600–01.

202. Branham, *supra* note 21, at 219; *PhotoDNA*, *supra* note 52 (noting PhotoDNA is Microsoft's hash value matching software that it gave to NCMEC and made available for all internet platforms).

203. *See* United States v. Wilson, 13 F.4th 961, 979 (9th Cir. 2021).

204. *See PhotoDNA*, *supra* note 52.

205. *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/.

206. *Id.*

207. Microsoft News Ctr., *supra* note 35.

understood by discussing the differences between previous technology and PhotoDNA.[208]

Before PhotoDNA, law enforcement and Providers used MD5 and SHA-1 hash value matching, which "require[d] *everything* about an image—the file type, the image size, the colour tones, everything—to be exactly the same between the original image and the copies you are trying to identify."[209] If an image was resized, cropped, retouched, or digitally changed in any way, the suspected image and known CSAM image did not match.[210] However, PhotoDNA instead "convert[s] the image into a common black-and-white format and size[s] the image to a uniform size, then divide[s] the image into squares and assign[s] a unique numerical value" to each square.[211] Hash value programs, like PhotoDNA, quickly search and identify thousands of files containing child pornography by looking at the megapixels, not the actual photo.[212] This way of matching images significantly increases the accuracy of matches because even if a user crops an image, the megapixels remain the same.[213] With PhotoDNA or similar technology, the odds of a hash program falsely matching an image to NCMEC's exploitative image database are practically non-existent[214] because, unlike previous methods, this can identify matches even if a user attempts to disguise the photo with cropping or retouching.[215]

Drug sniffing dogs are an effective analog to hash value matching.[216] These dogs are a constitutional tool used to conduct drug searches.[217] Hash value matching is more reliable than using drug dogs because, for example, even a positive alert does not accurately distinguish between drugs and drug residue.[218] Even after years of training and certifications, drug detection dogs may have numerous false alerts and those that are accurate give an officer

208. Krishna, *supra* note 166, at 1602; Branham, *supra* note 21, at 222; *see* Microsoft News Ctr., *supra* note 35.

209. Microsoft News Ctr., *supra* note 35.

210. *Id.*

211. *Id.*

212. Krishna, *supra* note 166, at 1602; Branham, *supra* note 21, at 222; *see* Microsoft News Ctr., *supra* note 35.

213. Microsoft News Ctr., *supra* note 35.

214. Branham, *supra* note 21, at 239; Martin, *supra* note 181, at 716.

215. Krishna, *supra* note 166, at 1602; Branham, *supra* note 21, at 222; *see* Microsoft News Ctr., *supra* note 35.

216. *See* Branham, *supra* note 21, at 238–39; Martin, *supra* note 181, at 714–15.

217. *See* Branham, *supra* note 21, at 238–39; Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 44–46 (2005); Martin, *supra* note 182, at 714–15.

218. *See* Branham, *supra* note 21, at 238–39; Salgado, *supra* note 217, at 44–46; Martin, *supra* note 181, at 716–17.

little information beyond a positive match for drugs.[219] Whereas a hash value match informs the Provider if a particular file correlates with known CSAM while also classifying the image in a category to label its severity[220] as "A1," "A2," "B1," or "B2".[221] These categories reveal factors such as if the image is of a prepubescent or pubescent minor and whether the minor's genital areas are exposed.[222] With this categorization, an officer knows the level of severity plus whether a reported match is or is not child pornography.[223] Conversely, without more investigation, a drug dog handler merely knows that drugs, the components, or drug residue is present but not the drugs location or quantity.[224] Unlike hash value matching, handlers can cause false positives by leading the dog to alert when there is, in fact, nothing present.[225] Finally, unlike a hash value match, the probable cause threshold for a drug dog alert leading to a search is a mere subjective sniff.[226] Whereas a hash value match indicates a child pornographic image is present, based on the accurate technology in addition to categorizing the image, identifying the file corresponding to the match, and the IP address linking the user.[227] By providing the additional information, unlike drug dog sniffs, hash value matches provide law enforcement with sufficient evidence to indicate it is fairly probable child pornography will be present.[228]

Under *Wilson*, hash value matches' accuracy and reliability for search purposes are dependent on human confirmation; therefore, law enforcement cannot use the private party doctrine for secondary searches when no human verifies the image because the officer is not merely confirming CSAM and

---

219. Martin, *supra* note 181, at 715–17 (noting the dog's alert can only uncover the presence or absence of narcotics).

220. *See* Branham, *supra* note 21, at 218; United States v. Bonds, No. 5:21-cr-00043-KDB-DCK, U.S. Dist. LEXIS 196765 2, 1 (W.D.N.C. Oct. 13, 2021); United States v. Wilson, 13 F.4th 961, 965 (9th Cir. 2021).

221. *Wilson*, 13 F.4th at 965. A1 indicates the file contains a "sex act involving a prepubescent minor," A2 indicates the file is a "lascivious exhibition involving a prepubescent minor," B1 indicates a "sex act involving a pubescent minor," and B2 indicates a "lascivious exhibition involving a pubescent minor." *Id.*

222. *Id.*; United States v. Gool, No. CR 06-0544-JAJ, 2008 U.S. Dist. LEXIS 31522, at *7 (S.D. Iowa Apr. 11, 2008) (defining lascivious exhibition as an image that displays a child either nude or partially clothed with genitals or pubic areas exposed).

223. *See* Martin, *supra* note 181, at 716.

224. *See* Jacey Lara Gottlieb, *Who Let the Dogs Out—and While We're at It, Who Said They Could Sniff Me?: How the Unregulated Street Sniff Threatens Pedestrians' Privacy Rights*, 82 BROOK. L. REV. 1377, 1380 (2017).

225. *Id.* at 1409–10.

226. *Id.* at 1379.

227. *Wilson*, 13 F.4th at 965; United States v. Miller, 982 F.3d 412, 417 (noting the Provider report sent to NCMEC contains where the material was found for identify purposes such as Gmail and the IP address associated with the Gmail).

228. *See* Branham, *supra* note 21, at 237–38.

rather they are the first to know whether the report details a crime.[229] Law enforcement can only be the first human to view the actual image that resulted in the match when there is a search warrant because physically viewing the images exceeds the scope of the initial match when there is no confirmation.[230]

Although the court in *Wilson* held that without human confirmation, the use of private party doctrine was unconstitutional, it should not have held that hash matching is unreliable.[231] Nowhere in 18 U.S.C. § 2258 does it require a human in the Provider's company to confirm the match for it to be reliable evidence indicating child sexual exploitation.[232] In fact, 18 U.S.C. § 2258C specifically mentions hash value matching as a tool to identify and stop the transmission of child pornography.[233] Moreover, in *Reddick*, the court acknowledges that by design the hash value algorithm runs "without the need for human searchers."[234] The lack of human confirmation does not make a hash value match insufficient evidence to establish probable cause for a warrant because the match identifies the user and the conduct contained in the match, with particularity, as a violation of child pornography statutes.[235]

Eliminating child sexual exploitation to protect children's physical and psychological well-being is a compelling interest for the government and Providers.[236] Therefore, using hash value matching is crucial to increasing the number of files reported, which in turn helps eliminate child pornography.[237] Compared to drug dogs and DNA, using hash value matching without prior human confirmation when applying for a search warrant is regarded in a more

229. *Wilson*, 13 F.4th at 974–75, 79 (noting human confirmation by a Google employee would supply Agent Thompson information about the reported images' contents to either apply for a warrant or use the private party doctrine to confirm the initial search).

230. *Id.* at 974–75, 979.

231. *Id.* at 979–80 (holding that after Wilson questioned the reliability of the hash value matching, the match itself was not sufficient for Agent Thompson to override Wilson's Fourth Amendment rights without a warrant or an exception).

232. Haney, *supra* note 107, at 78; 18 U.S.C. § 2258A (indicating a Provider must file a report with NCMEC if it has actual knowledge of facts or circumstances indicating apparent or imminent child pornography).

233. 18 U.S.C. § 2258C.

234. United States v. Reddick, 900 F.3d 636, 636–37 (5th Cir. 2018).

235. Branham, *supra* note 21, at 238; United States v. Miller, 982 F.3d 412, 430–31 (6th Cir. 2020).

236. New York v. Ferber, 458 U.S. 747, 756–57 (1982); Abhi Chaudhuri, *Continuing the Fight Against Child Sexual Abuse Online*, KEYWORD (Nov. 7, 2018), https://www.blog.google/technology/safety-security/continuing-fight-against-child-sexual-abuse-online/.

237. *See generally*, Samantha Cole, *Facebook Reported 20 Million Instances of Child Sexual Abuse in 2020*, MOTHERBOARD TECH BY VICE (Feb. 24, 2021, 12:04 PM), https://www.vice.com/en/article/7k9an4/facebook-pornhub-child-abuse-content-ncmec-report-2020. John Clark, the CEO of NCMEC, in an interview told Motherboard, "[w]e want more reports and for more companies to report and for those who do report to report more." *Id.*

favorable light and can lead a reasonable officer to believe the user, identified in the report, possesses child pornography in violation of the law.[238]

C. Policy Reasons to Use a Match Without Human Confirmation for a Search Warrant

Considering that the use of hash value matching is voluntary, if a match alone does not rise to the level of probable cause, the strides taken to reduce and eliminate child pornography are meaningless.[239] When a match operates as sufficient probable cause for a search warrant,[240] there is no need to force a Provider's employee to view the gruesome details of CSAM. Rather, the government should apply for a search warrant based on the match because it is with "almost absolute certainty" that when the officer conducts the search, he will find evidence of a child pornographic crime.[241] Not only will mandating human confirmation slow down the discovery process by increasing the amount of time it takes to find, report, and remove CSAM but also it unavoidably requires Providers to hire more employees to sift through traumatic child pornography images to keep up with the demand.[242] Furthermore, having employees confirm each match risks a drastic decline in CSAM reporting as the additional steps will not warrant the effort for a voluntary duty.[243]

---

238. *See* United States v. Wilson, 13 F.4th 961, 972–73 (9th Cir. 2021). The court indicated that the A1 categorization only functioned as a label to tell the officer the image was obscene. *Id.* The court noted, however, the categorization told the officer it was a prepubescent minor engaging in a sexual act and this description alone is far more than a label for obscenity. *Id.*

239. *See generally*, Cole, *supra* note 237 (comparing 2019 to 2020, NCMEC reported an increase of 97.5% in the number of reports which could indicate providers are doing more to identify and remove child abuse from their platform).

240. *See* United States v. Miller, 982 F.3d 412, 430–31 (6th Cir. 2020).

241. *Id.*; United States v. Reddick, 900 F.3d 636, 639 (5th Cir. 2018).

242. *New Report Shows an Increased Effort by Tech Companies to Detect CSAM on the Internet*, THORN (Mar. 18, 2022), https://www.thorn.org/blog/new-report-shows-an-increased-effort-by-tech-companies-to-detect-csam-on-the-internet/ (noting hash value matching increases the discovery of CSAM as indicated by the 1.22 days it took Providers to remove CSAM from its platform in 2021 compared to three days in 2020); *A Q&A with Law Enforcement Investigating Child Sexual Exploitation*, THORN (Oct. 8, 2019), https://www.thorn.org/blog/scale-law-enforcement-qa/ (noting two law enforcement officers were interviewed about their role in fighting CSAM and both indicated "the biggest barrier to eliminating CSAM" from the internet is the volume of material online). Based on the increase in reporting and the amount of volume online, to backtrack and require every Provider to confirm each match will do more harm in the fight to eliminate CSAM by increasing the time it takes to get predators off of the internet. *See* THORN, *supra.*

243. *See* THORN, *supra* note 205 (indicating before hash value matching the verification process was slow); *Why an Increase in Reports of CSAM is Actually a Good Thing*, THORN (Feb. 24, 2021), https://www.thorn.org/blog/why-an-increase-in-reports-of-csam-is-actually-a-good-thing/. If the verification process was slow before hash value matching, it follows that mandating human confirmation for each match will decrease the efficiency of hash matching.

1. Cost Benefit of Hash Value Matching

Even though several of the reporting Providers are multi-million-dollar or greater companies,[244] the cost to hire more employees would be financially imprudent and impractical for many, as CSAM reporting is voluntary.[245] Many companies may even avoid the financial cost by discontinuing active pursuit of CSAM, thus passing their obligation as a Provider on someone else. On average, a computer technician at Google has an annual salary of $67,629.[246] Based on that salary, depending on the company, it may be feasible to hire one or two more employees, but the number of employees needed will vary and become costly.[247] For example, if Google needed 100 more employees to keep up with the demand of manual confirmation for officers to use matches as probable cause, based on the average technician salary, it would cost 6.7 million dollars annually.[248] While the cost per Provider is not of concern to the federal circuit courts in deciding the reliability of hash value matching, understanding it lends support to the use of hash value matching without requiring human confirmation for probable cause; this reduces the potential risk of Providers discontinuing active pursuit on the internet if required to conform to the costly demand manual confirmation creates.

Subsequently, the cost of relying on hash matching without human confirmation to get a search warrant, conceivably, is nothing.[249] Using PhotoDNA to run hash value searches does not create any additional cost for the Provider.[250] Furthermore, if a company uses another program such as Safer—a program used to identify, remove, and report CSAM—at most, it will cost $178,447 annually to process over 100 million files a month.[251] Thus, the financial benefit of using PhotoDNA, or similar programs, can be seen as an incentive to actively pursue matches that law enforcement can use for probable cause on search warrants.

---

244. *See* NCMEC, 2021 REPORT, *supra* note 9; Daisuke Wakabayashi, *Google Reaches $1 Trillion in Value, Even as It Faces New Tests*, N.Y. TIMES (Jan. 16, 2020), https://www.nytimes.com/2020/01/16/technology/google-trillion-dollar-market-cap.html; Sean Dennison, *How Much Is Facebook Worth?*, GOBANKINGRATES (Feb. 10, 2022), https://www.gobankingrates.com/money/business/how-much-is-facebook-worth/.

245. *See* 18 U.S.C. § 2258A.

246. *Google Technician Salary*, ZIPRECRUITER, https://www.ziprecruiter.com/Salaries/Google-Technician-Salary (last visited Feb. 20, 2023) (noting this figure is for the average determined as of February 13, 2023).

247. *See id.*

248. *Id.*

249. *See PhotoDNA FAQ*, MICROSOFT, https://www.microsoft.com/en-us/photodna/faq (last visited Feb.. 20, 2023).

250. *Id.* (noting PhotoDNA is free for qualified customers and developers).

251. *Safer: Identify, Remove, and Report Child Sexual Abuse Material at Scale*, AWS MARKETPLACE, https://aws.amazon.com/marketplace/pp/prodview-vel6geeq73yco (last visited Feb. 20, 2023).

2. Mental Well-Being Resulting from Hash Value Matching

In addition to the financial benefit stemming from the use of hash matching without human confirmation is the decrease in the mental toll on those employed to uncover child pornography.[252] Providers visually confirming every match for the government's search to comply with the Fourth Amendment[253] inevitably increases the mental effects on private employees as well as law enforcement.[254] In particular, the University of Surrey researchers surveyed 101 police officers across the United Kingdom and found more than one-third suffered from secondary traumatic stress after investigating child pornography.[255] Not only are officers at risk for secondary traumatic stress but researchers at Walden University suggest those employed to uncover child abuse are at risk of developing burnout, compassion fatigue, and vicarious traumatization.[256] Based on doctrinal research, there is a connection between exposure for visually confirming child sexual abuse and prolonged psychological issues.[257] Hash value matching is a less invasive way to confirm child pornography that can protect the mental impact on the viewer because the Provider does not see the actual child pornography image.[258] Requiring human confirmation for hash matching will inevitably increase the number of people at risk of suffering from the physical and mental effects of visually confirming CSAM.[259] Whereas establishing matches alone for probable cause purposes reduces the risk of suffering burnout, compassion fatigue, and vicarious traumatization because employees will not automatically view child pornography as part of their job.[260]

---

252. *See* Krishna, *supra* note 166, at 1604 (noting content moderators at Facebook tasked with uncovering CSAM suffered from post-traumatic stress disorder). By decreasing the amount of manual CSAM review on Providers' employees, effectively there will be a decrease in the risk on their mental toll.

253. *See* United States v. Wilson, 13 F.4th 961, 972, 974 (9th Cir. 2021).

254. *See* Krishna, *supra* note 166, at 1604; *Police Officers at Risk of PTSD When Investigating Child Sexual Abuse Cases*, UNIV. OF SURREY (June 18, 2018), https://www.surrey.ac.uk/news/police-officers-risk-ptsd-when-investigating-child-sexual-abuse-cases.

255. *Police Officers at Risk of PTSD*, *supra* note 254 ("Secondary traumatic stress is the emotional response experienced when an individual is exposed to the first hand trauma of others and can lead to post traumatic stress disorder.").

256. Damon Landon Simmons, Police Stress: An Analysis of the Impact on Child Sexual Exploitation Investigators 49 (2018) (Ph.D. dissertation, Walden University) (ScholarWorks), https://scholarworks.waldenu.edu/dissertations/5527/.

257. *Id.* at 50.

258. 18 U.S.C. § 2258C(a)(2)–(3).

259. *See id.*

260. 18 U.S.C. § 2258C(a)(2)–(3); *Hash Values—Fingerprinting Child Sexual Abuse Material*, NETCLEAN (Oct. 30, 2018), https://www.netclean.com/2018/10/30/hash-values/ (on file with the UA Little Rock Law Review); *see* Simmons, *supra* note 256, 49.

3. Increase in Reported CSAM

Furthermore, in addition to the psychological benefits of allowing hash value matching without human confirmation for a warrant, the increase in reporting demonstrates its effectiveness.[261] NCMEC reporting numbers have considerably increased over the last fifteen years, and while many factors contributed, one to recognize is Providers and their use of hash value matching.[262] This increase indicates Providers' efforts to identify and remove CSAM are more robust and produce reports at a higher rate than previous human-run analysis methods.[263] In fact, of the 29.3 million reports to NCMEC, only 240,598 were from the general public.[264] These numbers indicate that the vast majority of reports are Provider submitted after proactively scanning and isolating CSAM on their platforms.[265]

Although hash value matching identifies and removes child pornography from the internet,[266] child pornography will continue to appear online without the government taking a firm approach to eliminate CSAM. Implementing hash value matching has substantially increased the number of reports each year.[267] Though the rise in reports does not indicate the actual number of abused children, the continued increase in CSAM reporting will lead to fewer CSAM victims online.[268] NCMEC works hard to remove CSAM, whether it is a new image or an old image that has resurfaced.[269] However, a victim's trauma does not immediately stop after identification and often follows them

261. *Compare* NCMEC, 2019 REPORT, *supra* note 76, *with* NCMEC, 2021 REPORT, *supra* note 9 (indicating Providers are reporting more CSAM based on the 12.9 million reports increase from 2019 to 2021).

262. O'Connell, *supra* note 95, at 300 (noting since 2004 NCMEC has seen over a 15,000 percent increase in reports that is in part a result of ease of access for purveyors but also Providers proactivity searching its platforms); *Let's Build a Better Internet for Every Child: Safer's Best-in-Class Technology Is Now Available for Anyone with an AWS Marketplace Account*, SAFER (May 24, 2021), https://safer.io/resources/csam-detection-safer-aws-marketplace-thorn/; *see* NCMEC, *CSAM*, *supra* note 12.

263. NCMEC, 2021 REPORT, *supra* note 9; THORN, *supra* note 244; *see* NCMEC, *CyberTipline*, *supra* note 9.

264. NCMEC, *CyberTipline*, *supra* note 9.

265. NCMEC, *CyberTipline*, *supra* note 9; O'Connell, *supra* note 95, at 299–300.

266. *Id.* at 218.

267. Krishna, *supra* note 166, at 1586 (noting that in 2019, over sixty-nine million child abuse images were reported, which was more than the forty-five million in 2018 and the one million in 2014); Brenna O'Donnell, *Rise in Online Enticement and Other Trends: NCMEC Releases 2020 Exploitation Stats*, NAT'L. CTR. FOR MISSING AND EXPLOITED CHILD. (Feb. 24, 2021), https://www.missingkids.org/blog/2021/rise-in-online-enticement-and-other-trends--ncmec-releases-2020- (noting that 2020 broke records for having the most child exploitation material reported at 21.7 million, which included 21.4 million from electronic service providers, and is a 97.5% increase from 2019).

268. Cole *supra*, note 237.

269. NCMEC, *CSAM*, *supra* note 12.

for the rest of their life.[270] In fact, for a female CSAM victim, this trauma costs approximately $282,734 over her lifetime.[271] Therefore, the Supreme Court should establish precedent that hash valuing matching may serve as reliable evidence for probable cause.[272] This precedent would not only minimize the traumatic and financial impact on Providers but also would enable unidentified sexual abuse material for children like Jane Doe #1 to be valued, matched, and removed across numerous Provider platforms, therefore, decreasing their revictimization.[273]

D. Proposed Test for Hash Value Matching

The disagreement on whether hash value matching is reliable evidence of child pornography will exist[274] until either the Supreme Court establishes precedent, or the various appellate courts align.[275] This Note proposes the Supreme Court establish the following test: when a court has a hash value matching case, it must determine (1) whether a Provider or government agent conducted the search; and (2) if a Provider conducted the initial search, whether the Provider utilized hash value matching. If the Provider used hash value matching, the court must look at (3) whether the Provider's employee confirmed the match before reporting the information to NCMEC. If the Provider did confirm the match, (a) the private party doctrine applies, and law enforcement could view the images without a search warrant if it does not exceed or expand the Provider's search. However, if the Provider did not confirm the match, (b) the match alone is only sufficient to establish probable cause to apply for a search warrant. This test admittedly does not vastly change some of the circuits' guidelines for the use of hash value matching; however, it clarifies the line of probable cause when there is a match without human confirmation. Therefore, law enforcement can easily identify when it must obtain a warrant before continuing further in the search for CSAM.

---

270. *Id.*

271. Elizabeth J. Letourneau et al., *The Economic Burden of Child Sexual Abuse in the United States*, CHILD ABUSE & NEGLECT 79, 417 (2018). This 2015 study focused on the major costs associated with child sexual abuse such as the cost of health care, productivity loses, child welfare, crime and violence, special education, and suicide death. *Id.* The study estimates for male victims of child sexual abuse it costs $74,691 over their lifetime. *Id.* However, these numbers are for nonfatal victims of child sexual abuse. For fatal child sexual abuse, it costs $1,128,334 for females and $1,482,933 for males. *Id.*

272. *See* Martin, *supra* note 181, at 716.

273. *See Police Officers at Risk of PTSD*, *supra* note 254; *see also* Simmons, *supra* note 256 at 49; NCMEC, *CyberTipline*, *supra* note 9.

274. *See* United States v. Miller, 982 F.3d 412, 429–30 (6th Cir. 2020); United States v. Wilson, 13 F.4th 961, 979 (9th Cir. 2021).

275. *See supra* Section II, Part C.

Even without human confirmation, hash value matches are unique; one change in the file prevents a match, thus making them inherently reliable to law enforcement under the private party doctrine or for purposes of obtaining a search warrant.[276] However, without human confirmation, learning the details of the match is like finding additional fingerprints of a suspect at a crime scene; a hash values unique qualities help strengthen the investigation without requiring law enforcement to investigate further before obtaining a search warrant.[277] Without a search warrant or human confirmation, law enforcement infringes on a person's expectation of privacy because viewing the details of the image greatly expands the officer's knowledge, even considering how much the officer knew after receiving the initial hash value match.[278]

Applying the proposed test to the cases illustrated in this Note demonstrates how it can be an effective standard to evaluate hash value matching. First, in *Wilson*, while the search of Wilson's email would remain unconstitutional for violating his right to privacy without a search warrant,[279] the analysis would change. Applying this Note's proposal, the facts support the first two elements because Google, a Provider, conducted a private search of Wilson's email using hash value matching.[280] Thus, the court would have next evaluated whether an employee at Google confirmed the images identified in the match before reporting it to NCMEC. However, when evaluating the third element, the test fails because no Google employee confirmed the images before Agent Thompson viewed them nor did he obtain a search warrant.[281] Under this analysis, Agent Thompson would not have needed human confirmation to establish sufficient probable cause for a search warrant because NCMEC's report indicated Wilson's email contained four images with an A1 categorization depicting a prepubescent minor engaging in a sexual act, and Wilson could be identified with particularity as the person who was engaging in the apparent violation of child pornography statutes through his IP address, primary email, and secondary email.[282] The hash value match alone would have been sufficient to indicate to a reasonable officer that it was fairly probable Wilson possessed child pornography through the A1 classification and the report identifying him, and as such, probable cause would have been easily satisfied for a warrant.[283] Thus, the court would have used element 3(b) and seen that there was no confirmation nor a search warrant, and, therefore, the search of Wilson's email would have still violated the Fourth Amendment.

276. *See* Branham, *supra* note 21, at 219.
277. *See id.* at 218–19, 237.
278. *Wilson*, 13 F.4th at 973–74.
279. *Id.* at 980.
280. *Id.* at 965.
281. *Id.* at 971–72.
282. *Id.* at 965.
283. *Id.* at 965–66.

Likewise, for *Ackerman*, while the holding that Ackerman's right to privacy was an expansion of the private party doctrine remains the same under this test, the rationale changes. The test applies to this case because AOL, as a Provider, conducted a search using hash value matching; thus, the first and second elements are met.[284] But the third element fails because when AOL sent NCMEC the report, only one of the four images had a hash match.[285] Under this Note's proposed analysis, viewing the three other images not matched would have required human confirmation or a search warrant.[286] As for element 3(a), the private party doctrine would have only applied to the one image that contained the confirmed match. However, under that element, expanding that search to the three other images would have been an expansion of the private party doctrine and, thus, would have required a search warrant.[287] The NCMEC analyst, acting as a government agent, would have easily had enough evidence to support probable cause for the remaining three images because the analyst had already viewed the matched image and would have known that it was fairly probable, to a reasonable officer, that the other three attachments also contained child pornography.[288]

Even though it appears counterintuitive to halt the entire investigation into child pornography simply because the program did not flag three of four images as matches, a user has a constitutional right to an expectation of privacy against unreasonable searches.[289] While it was fairly probable that the other three images contained child pornography, without human confirmation or a search warrant, the analyst pried into Ackerman's privacy without any safeguards such as a warrant or the private party doctrine.[290] Allowing government agents to go beyond the scope of a private search without human confirmation or a search warrant is an infringement on the fundamental right to privacy that fails even with the legitimate government interest of stopping the rise in child pornography online.[291]

VI. CONCLUSION

The current efforts to eradicate child pornography are slow and ineffective compared to the sheer volume of victims.[292]

---

284. United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016).
285. *Id.* at 1297.
286. *Id.* at 1306–07.
287. *Id.* at 1294.
288. *Id.*
289. *See id.* at 1295.
290. *Ackerman*, 831 F.3d at 1306.
291. *See id.* at 1308–09; New York v. Ferber, 458 U.S. 747, 756–57 (1982).
292. *See generally* NCMEC, *CSAM*, *supra* note 12; *see* NCMEC, *CyberTipline*, *supra* note 9 (identifying 4,260 potential new victims in 2021, in addition to the 19,100 plus victims NCMEC already identified).

Though the Supreme Court declined to hear the appeal from *United States v. Miller*,[293] the Court should establish binding hash value matching precedent. As it stands, until the Supreme Court hears a case involving Providers using hash value matching, uniformity will never exist.[294] Not only will the courts differ on the protections an individual should have against hash value matching[295] but also Providers will monitor their users differently,[296] allowing child pornography and its victims to go unnoticed. Additionally, individuals' Fourth Amendment protections will be different depending on the jurisdiction in which they live.[297] Supreme Court precedent will give Providers and law enforcement a clear standard to follow when using hash value matching.

Alternatively, until the Supreme Court adopts a hash value matching standard, the circuit splits should adopt the proposed hash value test illustrated above. Not only does the test allow for law enforcement officers to use hash value matches to apply for search warrants but also it indicates that in the event a Provider's employee views the hash match, law enforcement can view that same material without a search warrant and without violating a user's right to privacy. While there are fifty-six hotlines in forty-six countries[298] and NCMEC has identified over 19,100 victims, new victims appear daily in every corner of the internet.[299] Although everyone involved in the fight against CSAM continues to make strides every day, predators are revictimizing children each time they share sexually abusive images of children.[300] With the continued victimization rising, the Supreme Court has a duty to stop pedophiles from exploiting the future makers of tomorrow, like Jane Doe #1.[301]

---

293. *See* United States v. Miller 982 F.3d 412 (6th Cir. 2020), *cert. denied*, 141 S. Ct. 2797 (2021).

294. *See supra* Section II, Part C.

295. *Compare Miller*, 982 F.3d at 432 (indicating a trespass to property approach should be the proper standard), *with* United States v. Wilson, 13 F.4th 961, 971–72 (using the Jacobson private search exception standard).

296. *See* Hachman, *supra* note 63; *see also supra* Section II, Part C.

297. *See supra* Section II, Part C.

298. *The Facts*, INHOPE, https://www.inhope.org/EN/the-facts (last visited Feb. 20, 2023).

299. NCMEC, *CSAM*, *supra* note 12.

300. *Id.*

301. *See* Complaint, Jane Doe #1 v. MG Freesites, LTD et al, 7:21-cv-00220-LSC (N.D. Ala. Feb. 11, 2021), ECF No. 1.

*Virginia Kendall**

* J.D. Candidate Class of 2023, University of Arkansas at Little Rock, William H. Bowen School of Law; B.A. in Criminal Justice, University of South Carolina, 2019. This Note is dedicated to my biggest supporter and cheerleader in heaven, my mom, Lisa. I also owe a great deal of appreciation to my friend Kim for inspiring me to join Law Review; Professor Flannery and Professor Reese for their advisement and time spent editing this Note; my sister, Helen for supporting me through everything; my friends for encouraging me throughout this entire writing process; and my colleagues in the Law Review for the countless hours spent editing and publishing this Note, I could not have done it without each of you.