Akron Law Review

Volume 53 | Issue 1 Article 7

2019

Hash It Out: Fourth Amendment Protection of Electronically Stored Child Exploitation

Rebekah A. Branham

HASH IT OUT: FOURTH AMENDMENT PROTECTION OF ELECTRONICALLY STORED CHILD EXPLOITATION

*Rebekah A. Branham**

I. INTRODUCTION

The globalization of the internet and technology has caused "child pornography being traded over the Internet [to] rise exponentially."[1] It has allowed images to be transferred from the computer of one individual to that of millions through just the click of a button. Robert S. Mueller, of the Federal Bureau of Investigations, imputes the rise in child exploitation

* Rebekah A. Branham, J.D. candidate at The University of Akron School of Law, May 2020. I express my gratitude to the editors and associate editors of the *Akron Law Review* for their valuable feedback and assistance. A special thanks also to my family and fiancé for their unwavering encouragement and support.

1. Daniel S. Armagh, *Virtual Child Pornography: Criminal Conduct or Protected Speech?*, 23 CARDOZO L. REV. 1993, 1994 (2002).

to the readily available Internet, stating that "An increasing amount of this exploitation takes place in the dark shadows of the Internet . . . ."[2] In attempts to reverse this incredulous crime, private computer programs are taking steps to identify shared child exploitation on the internet—in some instances, in the absence of adequate warrants.[3] Their efforts involve a method known as hash-based evaluation ("hashing"). Hashing allows private computer programs "to identify suspect material from enormous masses of online data, through the use of specialized software programs—and to do so rapidly and automatically without the need for human searches."[4] Richard Salgado, former senior counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice, explains: "The concept behind hashing is quite elegant: take a large amount of data, such as a file or all the bits on a hard drive, and use a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data."[5] Today, hash-based examination is used throughout the forensics process to "[combat] the online distribution of unlawful aberrant content."[6] Hashing assists private computer programs in "assess[ing] whether a suspect's computer contains files . . . known to be contraband"[7] and is authorized under 18 U.S.C. § 2258(C) to screen images to detect child sexual abuse.[8] Internet service providers ("ISP") do this by comparing the unique algorithm generated from the hash to databases containing hash values associated with known child pornography, such as the images stored by the National Center for Missing and Exploited Children (NCMEC).[9] These distinctive identifiers, recently dubbed the "digital fingerprint,"[10] are the seeds of

2. Robert S. Mueller III, *Child Exploitation on the Internet: The Dark Side of the Web*, FED. BUREAU OF INVESTIGATION (Dec. 6, 2006), https://archives.fbi.gov/archives/news/speeches/child-exploitation-on-the-internet-the-dark-side-of-the-web [https://perma.cc/AV3A-GNVY].

3. Dennis Martin, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 700 (2018) ("And [law enforcement officers] might sometimes use hash values to identify evidence of crimes outside the scope of their warrant.").

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

5. Richard P. Salgado, *Fourth Amendment Search and* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38 (2005) *Power of the Hash*, 119 HARV. L. REV. F. 38 (2005).

6. *Reddick*, 900 F.3d at 637.

7. Marcia Hofmann, *Arguing for Suppression of 'Hash' Evidence*, CHAMPION, May 2009, at 20.

8. 18 U.S.C. § 2258(C).

9. Hofmann, *supra* note 7, at 20. ("A hash may also help to assess whether a suspect's computer contains files already known to be contraband. For instance, the National Center for Missing and Exploited Children maintains a database of hash values of child pornography files, which can be compared to files on other computers to see if there are any matches.").

10. Martin, *supra* note 3, at 695.

controversy within the realm of the Fourth Amendment. Advocates of hash-based examination argue that, because the tool only reveals the presence or absence of illicit material while "exposing little, if any, ancillary information," the Fourth Amendment is not violated.[11] Adversaries, however, argue that hashing has unconstitutionally extended police investigative powers, allowing them to discover criminal material "outside the scope of a search warrant."[12] So long as there remains no clear, definitive standard for searches of data on computer hard drives, hashing will continue to be of controversy among lower courts.

One particular computer software program developed in 2010, Microsoft PhotoDNA ("PhotoDNA"), has the ability to scan and identify large numbers of explicit photos in a matter of seconds using the hashing method.[13] When new images are uploaded onto the internet, social media sites, or email service providers, the program can automatically run that photo against its own database of digital markers "without the need for human searchers."[14] Computer software programs that perform hash-based evaluations operate at a high degree of accuracy.[15] Common hash-value algorithms have the ability to "generate numerical identifiers so distinctive that the chance that any two data sets will have the same [hash value], no matter how similar they appear, is less than one in one billion."[16] If a hash value match is found, "PhotoDNA creates a 'CyberTip,' sending the file and the uploader's IP address to NCMEC."[17]

NCMEC is a "private, non-profit . . . corporation whose mission is to help find missing children, reduce child sexual exploitation, and

11. Salgado, *supra* note 5, at 41; *see also* Martin, *supra* note 3, at 693.

12. Martin, *supra* note 3, at 693 ("For many years, government investigators have used digital forensic software to conduct hash searches: a very accurate, very computationally efficient type of search that can be used not just for legitimate purposes but also to identify evidence of crimes outside the scope of a search warrant.").

13. United States v. Reddick, 900 F.3d 635, 637–38 (5th Cir. 2018).

14. *Id. See also* United States v. Coyne, 387 F. Supp. 3d 387, 392 (D. Vt. 2018) ("A large and sophisticated [ISP] such as Microsoft employs its own human reviewers before forwarding the tip [to NCMEC]. Small [ISPs] such as Chatstep may choose to forward tips automatically without reviewing any images themselves.").

15. Martin, *supra* note 3, at 716 ("And even though accuracy is relevant not to whether a given technique is a search but only to whether it's sufficient to establish probable cause, it's also true that hash searches are highly accurate. The odds of two files producing the same hash value are 'infinitesimally small'. . . .").

16. Ronald J. Hedges et al., Managing Discovery of Electronic Information, Third Edition, Federal Judicial Center, at 52 (2017), available at https://www.fjc.gov/sites/default/files/2017/Managing_Discovery_of_Electronic_Information_3d_ed.pdf [https://perma.cc/9FYL-QRFL].

17. United States v. Reddick, 900 F.3d 636, 638 (5th Cir. 2018).

prevent child victimization."[18] It works in conjunction with ISPs and law enforcement in discovering child sexual abuse and trafficking on the internet. NCMEC operates a "national 24-hour toll-free hotline by which individuals may report information regarding the location of any missing child" known as the Cyber Tipline ("Tipline").[19] The Tipline has seen much prosperity. Since 1998 when the Tipline was developed, more than 25 million instances of child pornography images have been reported.[20] In 2008, Congress imposed obligations *requiring* ISP's to report "actual knowledge of any facts or circumstances" of a violation of any child pornography statute to the NCMEC.[21] While providers are required to report hash value matches, they are not, however, required to engage in affirmative monitoring or investigating alleged perpetrators.[22]

Few courts have addressed whether the use of hash values by ISPs violate an individual's Fourth Amendment rights. Courts that have addressed the issue focus their attention on whether NCMEC is a governmental entity.[23] However, the Fifth Circuit has very recently addressed this issue in *United States v. Reddick.*[24] After the defendant uploaded files to the cloud-sharing server SkyDrive,[25] PhotoDNA, a software program that uses hash-based examination, automatically reviewed the hash values of those files and compared them against its database of known child pornography hash values.[26] It proceeded to report the files to law enforcement.[27]

This note will examine the Fifth Circuit's reasoning in the *Reddick* decision. While it ultimately agrees with the outcome, it attempts to reconcile the oversimplified analysis the Fifth Circuit used in arriving at its decision. It is increasingly important that future defendants are afforded a thoughtful, balanced, and definitive legal analysis. This note

18. *About Us*, NAT'L CTR. FOR MISSING & EXPLOITED CHILDREN, http://www.missingkids.com/footer/about [https://perma.cc/KP35-S5V6].

19. 34 U.S.C. § 11293(b)(1)(M)(i) (2018).

20. United States v. Coyne, 387 F. Supp. 3d 387, 392 (D. Vt. 2018).

21. 18 U.S.C. § 2258(A) (2018).

22. *See* 18 U.S.C. §2258A(f) (2018) ("Nothing in this section shall be construed to require a provider to (1) monitor any user, subscriber, or customer of that provider . . . (3) affirmatively search, screen, or scan for facts or circumstances . . . ."); *see also* Alexandra L. Mitter, Alexandra L. Mitter, *Deputizing Internet Service Providers: How the Government Avoids Fourth Amendment Protections*, 67 N.Y.U. ANN. SURV. AM. L. 235, 245 (2011).

23. *See, e.g.*, *Coyne*, 387 F. Supp. 3d at 397; United States v. Ackerman, 831 F.3d. 1292, 1300–04 (10th Cir. 2016); United States v. Cameron, 699 F.3d 621, 644 (1st Cir. 2012); United States v. Richardson, 607 F.3d 357, 364–68 (4th Cir. 2010).

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

25. Presently referred to as "OneDrive."

26. *Reddick*, 900 F.3d at 637–38.

27. *Id.*

proceeds in three parts. Part I catalogs the constitutional and statutory requirements for searches and seizures under the Fourth Amendment. Part II analyzes the reasoning for the outcome in *Reddick.* Part III concludes with a proposed analysis for all cases involving the use of the hash value, child exploitation, and Fourth Amendment violations.

II. BACKGROUND

A. Constitutional Requirements for Search and Seizure

The Fourth Amendment of the United States Constitution establishes that: "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[28] It safeguards individual liberties by prohibiting two unreasonable intrusions by the government: searches and seizures.[29] "A search occurs when the government infringes upon an expectation of privacy that society is prepared to consider reasonable."[30] "Seizure of a person occurs when the government meaningfully interferes with his liberty; seizure of property occurs when the government meaningfully interferes with an individual's possessory interests in property."[31] Both of these protections extend to "computer[s] or its peripheral equipment."[32] Customarily, the Fourth Amendment is only implicated by searches carried out by the government.[33] However, Section IV of this note discusses a caveat to that general rule—the private search doctrine.

While considerable dialogue about specific warrant requirements exceeds the scope of this note, it is important to highlight the three categories of searches of electronically stored information as recognized in three separate Supreme Court cases:[34] (1) searches that require warrants

28. U.S. CONST. amend. IV.

29. Nat'l Treasury Emps. Union v. Von Raab, 816 F.2d 170, 174–75 (5th Cir. 1987).

30. *Id.* at 175.

31. *Id.*

32. Robin Cheryl Miller, Annotation, *Validity of Search or Seizure of Computer, Computer Disk, or Computer Peripheral Equipment*, 84 A.L.R. 5th 1, 2a (2000). In addition to the exceptions to the warrant requirement discussed in this note, computers and other personal electronic or digital storage devices are also subject to additional, unrelated exceptions, including but not limited to the "border search doctrine." See, e.g., Claudia G. Catalano, *Border Search or Seizure of Traveler's Laptop Computer, or Other Personal Electronic or Digital Storage Device*, 45 A.L.R. Fed. 2d 1.

33. U.S. CONST. amend. IV.

34. Mitter, *supra* note 22, at 246.

supported by probable cause;[35] (2) searches conducted without a warrant but with "reasonable suspicion" that criminal activity "may be afoot";[36] and (3) searches conducted without a warrant or particularized suspicion.[37] Unfortunately, as a result of the ever changing technological advancements, digital media does not securely fit into the framework of the Fourth Amendment.[38] While the Supreme Court readily continues to develop new tests in an attempt to withstand our contemporary use of technology,[39] it has yet to develop a standardized analysis for the use of hash-based examination in criminal investigations.

B. The Use of The Hash Value and The Fourth Amendment

Hash value algorithms are "powerful and pervasive" tools used by law enforcement for digital forensics purposes.[40] The properties of hash values have been equated to a human's DNA, meaning that it is virtually impossible for two images or videos to possess the same hash value.[41] Salgado notes four different properties of hashing that make it such a valuable and reliable tool. First, every file has only one hash value, and editing just one pixel of that file will generate a new hash value.[42] A hash value is generated in a way that "[t]he chance of two different inputs 'colliding,' . . . is astronomically small."[43] Thus, they produce highly definitive results that can be relied upon by law enforcement officers. Second, hashing offers law enforcement officers a method to examine only important digital files, weeding out any ancillary information and preserving the privacy interests of the subject.[44] Third, once the hash value has been generated, it "cannot be 'reversed' to generate the photo itself."[45]

35. *See generally* Katz v. United States, 389 U.S. 347 (1967).

36. Terry v. Ohio, 392 U.S. 1, 20 (1968).

37. *See generally* Indianapolis v. Edmond, 531 U.S. 32, 37 (2000).

38. Mitter, *supra* note 22, at 246 ("The Supreme Court has often struggled to fit rapidly changing technologies into this framework.").

39. *Id.* ("The Supreme Court has often struggled to fit rapidly changing technologies into [the Fourth Amendment] framework. The Court often tries to develop unique tests that will allow the Fourth Amendment to keep pace with technological change.").

40. Salgado, *supra* note 5, at 38.

41. *Id.* at 42 ("There is essentially no chance that any other hard drive would have the same hash value.").

42. *Id.* at 39 ("First, the hash value will be, for all practical purposes, uniquely associated with the input. No other file will have the same hash value as the . . . photo, except a file that is identical.").

43. *Id.*

44. *Id.* at 46 ("It . . . provides a means to discard from the examination the irrelevant, and focus on the important, while exposing little, if any, ancillary information.").

45. *Id.* at 40 ("A second property is that the hash algorithm works only in one direction. One can calculate a hash value from input, but cannot derive the input from the hash value.").

Lastly, hashing does not require a file to be physically opened and therefore is *seemingly* non-intrusive.[46] However, confusion about whether to categorize hashing as a Fourth Amendment violation stems from this very non-intrusive nature of it. Because the file is never physically opened, adversaries dwell on the *de minimis* risk of a false hash value match.

C. Statutory Protection of Internet Activity

In the interest of Americans' significant value of their individual privacy, Congress protects their reasonable expectation of privacy and regulates internet activity through the Electronic Communications Privacy Act (ECPA).[47] Without clear application of the Fourth Amendment to electronically stored information ("ESI"), Congress set out to "balance the government's need to obtain evidence with the public's desire to maintain privacy of electronic communication and electronically stored information." [48] The goal of the ECPA is to "'fill the gaps' left by the uncertain application of the Fourth Amendment protections to Internet communications."[49] The ECPA includes three federal statutes: the Stored Communications Act;[50] the Pen Register statute;[51] and the Wiretap Act.[52]

Congress enacted the Stored Communications Act (SCA) in 1986 to "protect individuals' private communications held in electronic storage . . . ."[53] The SCA provides circumstances in which the government can *compel* ISPs to disclose records.[54] Section 2702 of the SCA also provides circumstances in which an ISP can voluntarily disclose records.[55] An ISP is generally prohibited from voluntarily disclosing customer communications and subscriber records to a governmental entity, subject to just a few limited exceptions.[56] Section 2702(b)(6)

46. Salgado, *supra* note 5, at 42.

47. Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat.1848.

48. Laura J. Tyson, *A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content to Discover an Internet User's Identity*, 40 SETON HALL L. REV. 1257, 1268 (2010).

49. *Id.*

50. 18 U.S.C. §§ 2701–10 (2018).

51. 18 U.S.C. §§ 3121–27 (2018).

52. 18 U.S.C. §§ 2510–22 (2018).

53. Denae Kassotis, *The Fourth Amendment and Technological Exceptionalism After* Carpenter*: A Case Study on Hash-Value Matching*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1243, 1259 (2019).

54. 18 U.S.C § 2703(a) (2018).

55. 18 U.S.C § 2702 .

56. *Id.*

allows an ISP to "divulge the contents of a communication to the [NCMEC]" in order to report child sexual exploitation.[57]

Importantly, an individual alleging a violation of the SCA has a narrow list of remedies, and suppression of the evidence is not one of them.[58] Remedies based solely on a violation of the SCA include "preliminary and other equitable or declaratory relief as may be appropriate," "damages," and "reasonable attorney's fees and other litigation costs reasonably incurred."[59] Only when an individual can prove a violation of the Fourth Amendment in conjunction with a violation of the SCA is suppression of the evidence a remedy.[60]

III. STATEMENT OF THE CASE

The recent developments in hash-based examination have not gone uncontested. Advocates for hash-based examination firmly believe it is the sheathing against the war on child pornography.[61] Defendants, however, have attempted to challenge evidence seized through hash-based contraband detection on two grounds.[62] First, on the grounds that the "law enforcement officers [have conducted an] impermissible Fourth Amendment search[]," and second, that the "hash value match . . . [was] an inadequate basis for probable cause."[63] Both arguments have proved to fail.[64] This note focuses on a recent case in which this challenge was made: *United States v. Reddick*.[65] *Reddick* concerned one of the most controversial and contentious issues in today's society driven by technology—governmental intrusion into personal computer content. The Fifth Circuit Court of Appeals' decision directly addressed this conflict and has the potential to change the direction of the Fourth Amendment

57. *Id.* at § 2702(b)(6).

58. Kassotis, *supra* note 53, at 1260.

59. 18 U.S.C. § 2707(b)(1–3) (LexisNexis 2018).

60. United States v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014) ("For [a defendant] to suppress the . . . data, he therefore must show that the cell site location data was obtained not just in violation of the [SCA], but also in violation of the Fourth Amendment.").

61. Thorn Staff, *Eliminating Child Sexual Abuse Material: The Role and Impact of Hash Values*, THORN, https://www.thorn.org/blog/eliminating-child-sexual-abuse-material-hash-values/ [https://perma.cc/8Z6N-V7CS] (John Shehan, Vice President of NCMEC, states: "In the 16 years that I've devoted my career towards child protection at NCMEC, I can confidently say that hash values are the way forward. Together, we have made a huge difference in the lives of children around the world, and I am proud to have been a part of making these tools a reality.").

62. Martin, *supra* note 3, at 703.

63. *Id.*

64. *Id.*

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

jurisprudence. The Fifth Circuit decided *Reddick* on August 17, 2018.[66] The defendant, Henry Reddick, uploaded digital files onto a cloud hosting service known as Microsoft SkyDrive.[67] SkyDrive then used a proprietary technology called PhotoDNA to "scan the hash values of the uploaded files and compare them to the hash values of known images of child pornography."[68] PhotoDNA detected a hash value match between Reddick's photos and the database, and SkyDrive created a "CyberTip," sending the files and users' IP address to the NCMEC.[69] NCMEC then forwarded the same information to the Corpus Christi Police Department in Corpus Christi, Texas.[70] Corpus Christi Police Department Detective, Michael Ilse, opened the files to confirm they contained child pornography.[71] Thereafter, Ilse received a warrant, searched Reddick's home, seized his computer, and found "additional evidence of child pornography in [his] possession."[72] Reddick was indicted for possession of child pornography. He asserted that "Officer Ilse's review of the files . . . was a warrantless search in violation of the Fourth Amendment," and therefore, all the evidence obtained as a result must be suppressed pursuant to the exclusionary rule.[73] In denying his motion, the district court relied on the good faith exception to the exclusionary rule, finding that the law enforcement officers' reliance on the warrant was objectively reasonable.[74]

The U.S. Supreme Court created the exclusionary rule to bar prosecution from introducing evidence obtained by way of an "illegal search."[75] The Supreme Court recognized the good faith reliance on search warrants that are later found to be invalid in *United States v. Leon* when it stated: "the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial

66. *Id.*
67. *Id.* at 637.
68. *Id.* at 639.
69. *Id.* at 638.
70. *Id*.
71. United States v. Reddick, 900 F.3d 636, 638 (5th Cir. 2018).
72. *Id.*
73. United States v. Reddick, No. 2:16-CR-928, 2017 U.S. Dist. LEXIS 56577, at *8 (S.D. Tex. Apr. 13, 2017).
74. *Id.* at *15. ("Officer Ilse fully recited the circumstances by which he came into possession of the Phase I files and the fact that he opened them and viewed them. This exhibits a firmly held conviction that his Phase I investigation, including viewing of the files, was appropriate and lawful.").
75. *Id.* at *13 (citing United States v. Leon, 468 U.S. 897, 906 (1984)).

costs of exclusion."[76] In *Reddick*, the district court, relying on *Leon*, chose to honor the detective's good faith reliance on the search warrant used to enter and search Reddick's residence and his computer.[77]

The district court decision recognized five relevant factors for demonstration of a reasonable expectation of privacy. These five factors include:

> (1) whether the defendant has a property or possessory interest in the thing being searched; (2) whether the defendant has a right to exclude others from the place; (3) whether he has exhibited a subjective expectation of privacy; (4) whether he took normal precautions to maintain privacy; and (5) whether he was legitimately on the premises.[78]

The privacy issue, according to the district court, does not end there.[79] The answer to the overarching issue of whether hash-based evaluations constitute a search for Fourth Amendment purposes requires an exhaustive analysis in the context of each independent case. The district court recommended a series of additional "technology-specific determinations involving undeveloped facts and law" beginning with a review of the scope of the private search, the significance of the hash value "view," and any expectation of privacy that remains and including: Whether a subsequent search by law enforcement provide any additional information that was not already known?[80] Will viewing the file expose additional images that do not contain contraband?[81] Is law enforcement's view of the files after NCMEC a new search?[82] Is a hash value match reliable enough to equate it to an image of contraband?[83]

The Fifth Circuit affirmed the district court's denial on a much broader basis, giving limited attention to scope of the law enforcement officer's "search." It relied on the private search doctrine to guide its reasoning and found that the viewing by Detective Ilse did not violate the Fourth Amendment.[84] In general, regardless of whether invasions of privacy by a private individual "[are] accidental or deliberate and whether

76. *Leon*, 468 U.S. at 922 (1984) ("[S]uppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purpose of the exclusionary rule.").

77. *Reddick*, 2017 U.S. Dist. LEXIS 56577, at *16.

78. *Id.* at *9–10. *See also* United States v. Runyan, 275 F.3d 449, 457 (2001) (quoting United States v. Cardoza-Hinojosa, 140 F.3d 610, 615 (5th Cir. 1998)).

79. *Reddick*, 2017 U.S. Dist. LEXIS 56577, at *11.

80. *Id.*

81. *Id.*

82. *Id.*

83. *Id.*

84. United States v. Reddick, 900 F.3d 636, 639 (5th Cir. 2018).

they [are] reasonable or unreasonable, they [do] not violate the Fourth Amendment, because of their private character."[85] Subsequent and additional invasions of privacy by the government, beyond those committed by a private party, "must be tested by the degree to which they exceeded the scope of the private search."[86] Notably stated by the Fifth Circuit:

> The exact issues presented by this case may be novel. But the governing constitutional principles set forth by the Supreme Court are not. The government effectively learned nothing from Detective Ilse's viewing of the files that it had not already learned from the private search. Accordingly, under the private search doctrine, the government did not violate Reddick's Fourth Amendment rights.[87]

When PhotoDNA detected a hash value match, created a CyberTip, and sent the file to NCMEC, the Fifth Circuit interpreted it as a private search by Microsoft that frustrated whatever expectation of privacy the defendant had.[88]

The Fifth Circuit's oversimplified analysis leaves significant tension between balancing an individual's right to privacy and the utility of hash-based examination. To prevent future misapplication of the law, it is time for a thoughtful, balanced, and definitive legal analysis. Given the sensitivity of the Fourth Amendment, as well as the need to develop new procedures to abolish child exploitation, courts should afford each factor thorough analysis to avoid eroding constitutional protections of the accused.

A. Private Search Doctrine

Although the Supreme Court stated that "searches conducted outside the judicial process, without prior approval by [a] judge or magistrate, are *per se* unreasonable under the Fourth Amendment, subject only to a few specifically established and well-delineated exceptions,"[89] one of those exceptions is the private search doctrine. The private search doctrine presents a caveat to the Fourth Amendment that allows the government to "receive and utilize[] information uncovered by a search conducted by a private party."[90] The contemporary developments in technology,

85. United States v. Jacobsen, 466 U.S. 109, 115 (1984).
86. *Id*.
87. *Reddick*, 900 F.3d at 640.
88. *Id.* at 639.
89. Katz v. United States, 389 U.S. 347, 357 (1967).
90. United States v. Reddick, 900 F.3d 636, 637 (5th Cir. 2018).

including the developments in hash-based examination have, however, given purported surrogates of the government room to circumvent Fourth Amendment protections. The Fourth Amendment is only implicated when private parties conduct searches "with both the knowledge of law enforcement authorities and with the intent to assist those authorities."[91] Thus, it would follow that when law enforcement agencies utilize information volunteered by third parties who lack the intent to assist law enforcement agencies *at the time they conducted the initial search*, it is beyond the reach of the Fourth Amendment.[92]

In *Reddick*, the Fifth Circuit reasoned that, "the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant's expectation of privacy has not already been frustrated."[93] The court turned its attention to whether the defendant's "expectation of privacy in his computer files had already been thwarted" by PhotoDNA prior to the subsequent examination by Detective Isle.[94] The court's analysis was guided by a United States Supreme Court case decided in 1984 regarding contraband in a shipping package.[95] In *United States v. Jacobsen*, Federal Express ("FedEx") employees opened a damaged package and found a suspicious white powder beneath "layers of wrappings" and concealed in a tube.[96] FedEx put the contents of the tube back in the package and reported their discovery to the Drug Enforcement Administration (DEA).[97] The DEA reopened the package and conducted both a visual examination as well as a chemical field test, and determined that the white powder inside the tube was in fact cocaine.[98] Additional agents arrived, conducted another search, and then obtained a warrant to search the return address listed on the package.[99] The Court held that the DEA did not infringe on any privacy interest of the defendant that had not already been frustrated by the

91. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 79 (1994).

92. In United States v. Walther, the Ninth Circuit articulated a "critical factor test" to distinguish between private and government action. The court looked at the government's role in the search, the government's control of the searcher, and most relevant here, the private party's intent in conducting the search. The latter of the three entails an analysis of whether the private party had some legitimate independent motivation for the search, separate and apart from aiding the police in a successful prosecution of the suspect. United States v. Walther, 652 F.2d 788 (9th Cir. 1981).

93. *Reddick*, 900 F.3d at 638 (quoting United States v. Runyan, 275 F.3d 449, 461 (2001)).

94. *Id.*

95. *Id.* at 639 (citing United States v. Jacobsen, 466 U.S. 109 (1984)).

96. *Jacobson*, 466 U.S. at 111.

97. *Id.*

98. *Id.*

99. *Id.* at 112.

FedEx.[100] Warrantless searches of effects are "presumptively unreasonable" when conducted by a *governmental entity*, not when conducted by a private party.[101] Therefore, the Supreme Court ruled that the subsequent search conducted by the DEA infringed no legitimate expectation of privacy, simply because that expectation had already been frustrated by a private party.[102]

Once the Court established that FedEx had not infringed on the defendant's constitutionally protected "reasonable expectation of privacy," it held that the proper test is one that tests "the degree to which [the latter governmental search] exceeds the scope of the private search."[103] The *Jacobsen* Court relied on a standard adopted by a majority of the Court set forth by two Justices in *Walter v. United States*.[104] Justice Stevens, joined by Justice Stewart, stated: "[S]urely the Government may not exceed the scope of the private search unless it has the right to make an independent search."[105] The Court proceeded to describe how, in *Walter*, the private actor was only able to draw inferences about the contents of the package and, therefore, the latter governmental search was a "significant expansion of the search that had been conducted previously by a private party. . . ."[106] However, the distinction in *Jacobsen* came down to the availability of the contraband. The DEA did not have to draw inferences about the contents of the package, as it was in plain view when it was turned over to the government and was freely made available for their inspection. Removing the tube from the package after the FedEx employee had already done so did not reveal anything that had not been previously learned during the private search.[107]

Similarly, in *Reddick*, when law enforcement officers viewed the files, they were doing so to simply to "dispel[] any residual doubt about

100. United States v. Jacobsen, 466 U.S. 109, 126 (1984).

101. *Id.* at 130 (noting that the Fourth Amendment is "wholly inapplicable" to searches conducted by a private individual not acting as an agent of the Government).

102. *Id.* at 126.

103. *Id.* at 115.

104. *Id.* (citing Walter v. United States, 447 U.S. 649 (1980) ("Even though some circumstances—for example, if the results of the private search are in plain view when materials are turned over to the Government—may justify the Government's reexamination of the materials, surely the Government may not exceed the scope of the private search unless it has the right to make an independent search. In these cases, the private party had not actually viewed the films. Prior to the Government's screening one could only draw inferences about what was on the films. The projection of the films was a significant expansion of the previous search that had been conducted previously by a private party . . . .").

105. *Walter*, 447 U.S. at 657.

106. *Id.*

107. United States v. Jacobsen, 466 U.S. 109, 115 (1984).

the contents of the files."[108] After the automatic review by PhotoDNA of the package of digital files, law enforcement officers learned nothing from their examination that had not already been examined.[109] Moreover, Detective Ilse did not conduct a search of any files other than those previously, and reliably, flagged as child pornography.[110]

IV. A PROPOSAL

Fourth Amendment jurisprudence governing child pornography on the internet has not been subject to rigorous judicial analysis. The "tremendous growth" of the internet offers advantages to child pornography sharing outlets: "(1) the rapid transfer of files/images; (2) relatively high security; and of course (3) almost complete anonymity, all of which significantly lower the risk of arrest to the child pornographer."[111] Meanwhile, the limited remedies for violations of the Stored Communications Act "provide[] little incentive for a defendant to make a Fourth Amendment challenge."[112] Unfortunately, the lack of lucid foundation for Fourth Amendment challenges against search and seizures of electronically stored child pornography resulted in the Fifth Circuit failing to establish thoughtful precedent for future courts presented with the same issue. Combining the variation of analysis proffered by the circuit courts, this note proposes that, on a case-by-case basis and paying close attention to the circumstances surrounding the search, courts should answer the following questions: (1) Was the individual that conducted the initial search in fact acting as a private individual? (2) Was the defendant's reasonable expectation of privacy thwarted by the third-party doctrine? (3) Was there probable cause for the warrantless search? (4) Was the subsequent state actor acting within the scope of the private party search? If the answer to any of the preceding questions is no, the defendant should be entitled to challenge the admission of the evidence gained during the unconstitutional search. The contemporary technological advancements create ideal circumstances for the Supreme Court to craft a new test for lower courts to consider.

---

108. United States v. Reddick, 900 F.3d 636, 639 (5th Cir. 2018).

109. *Id*.

110. *Id.* ("Significantly, there is no allegation that Detective Ilse conducted a search of any of Mr. Reddick's files other than those flagged as child pornography.").

111. William R. Graham, Jr., *Uncovering and Eliminating Child Pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Enforcement's Access to 'Wonderland'*, 2000 L. REV. MICH. ST. U. DET. C.L. 457, 465 (2000).

112. Mitter, *supra* note 22, at 236.

A. Private Party or Governmental Agency?

As discussed in the preceding section, Fourth Amendment protections only apply to searches conducted by governmental entities or agents.[113] Thus, an unreasonable search or seizure conducted by a *private party* is exempt from those same constraints.[114] When presented with the novel question of whether an individual's Fourth Amendment safeguards were violated as a result of modern "hashing" technology, the first step in the proposed four-part analysis is to determine whether the entity acted as a private party or an indispensable "surrogate of the government."[115] While this certainty requires consideration of ISP's statutory requirements under 18 U.S.C. § 2258A(a), the analysis does not stop there. This note proposes a "totality of the circumstances" based approach when determining whether the actual function and motivating purpose of the ISP transformed it into an agent of the government. The Supreme Court has reasoned that whether a private party is constrained by the Fourth Amendment as an agent of the government "necessarily turns on the degree of the government's participation in the private party's activities, a question that can be resolved only 'in light of all the circumstances . . . .'"[116] An ISP is statutorily required to report *discovered* files involving child pornography,[117] but that does not necessarily mean it was required to affirmatively *monitor* its users or affirmatively search for violations.[118] The operation of the hash-based examination rests in the private hands of the ISP. But does an ISP lose its private nature simply because it is engaged in work of social importance?

The circuit courts have considered the fine line between private entity and governmental agent, but there is no universal test employed. Rather, courts are divided between employing a two-part test and a similar three-part test. The Fifth, Ninth, and Tenth Circuits devised a two-part

113. U.S. CONST. amend. IV.

114. *See Jacobsen*, 466 U.S. at 113 (explaining that protections afforded by the Fourth Amendment do not apply to searches conducted by private parties).

115. Michael J. Woods, *Data Retention Requirements and Outsourced Analysis: Should Private Entities Become Government Surrogates in the Collection of Intelligence?*, 4 AM. U. BUS. L. REV. 49, 55 (2015) (proposing that when a private party is serving the government's purpose, and not for business purposes, it becomes a functional surrogate of the government).

116. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)).

117. 18 U.S.C. § 2258A(a) (LexisNexis 2018) (providing that where company has "actual knowledge" of child pornographic pictures they must report this to the NCMEC).

118. § 2258A(f) (stating that "nothing in this section shall be construed" to require an ISP to monitor any user or affirmatively seek facts).

test.[119] The foundation behind this two-part test stems from a well-articulated proposition established in *United States v. Souza*, stating that "A search by a private person becomes a government search if the government coerces, dominates, or directs the actions of the private person conducting the search."[120] The court in *Souza* determined whether the characteristics of a private party transformed it into a governmental agent by asking two questions: "(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."[121]

The First Circuit has identified an additional important factor when determining whether a private party's actions transform it into a governmental agent. The First Circuit analyzed: (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."[122]

Regardless of the test employed, Fourth Amendment protections must not be circumvented by permitting a governmental agent to operate under the disguise of a private party. When applying these tests to the technological realm, courts must look at the totality of the circumstances in each particular case to determine first whether the "search" by the ISP, not the subsequent "search" by NCMEC, triggers Fourth Amendment protections. This begins with a consideration of the reporting requirements of providers under 18 U.S.C. § 2258A(a). Moreover, many courts agree that a reporting requirement alone does not transform an ISP into a governmental agent when it scans users' files by choice.[123] Namely, the Eighth Circuit in *United States v. Stevenson* held that an ISP was not

119. *See generally* United States v. Paige, 136 F.3d 1012 (5th Cir. 1998); United States v. Miller, 688 F.2d 652 (9th Cir. 1982); United States v. Souza, 223 F.3d 1197 (10th Cir. 2000).

120. *Saouza*, 223 F.3d at 1201 (quoting Pleasant v. Lovell, 876 F.2d 787, 796 (10th Cir. 1989)).

121. *Id.*; *see also* United States v. Ackerman, 831 F.3d 1292, 1301 (10th Cir. 2016).

122. United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009) (quoting United States v. Pervaz, 118 F.3d 1, 6 (1st Cir. 1997)).

123. *See, e.g.*, United States v. Cameron, 699 F.3d 621, 637–38 (1st Cir. 2012) (stating that while 42 U.S.C. § 13032(b)(1) required the ISP to report child pornography, it was not obligated to search for the files, and therefore, was not controlled by the government); United States v. Richardson, 607 F.3d 357, 364–67 (4th Cir. 2010) (stating that the statutory provisions requiring AOL to report known child pornography did not convert AOL into a governmental agent for Fourth Amendment purposes); United States v. Stevenson, 727 F.3d 826, 830 (8th Cir. 2013) (holding that a duty to report does not transform an ISP into a government agent when it is not affirmatively obligated to search an individual's computer but does so by choice).

transformed into a governmental agent because the ISP had no affirmative duty to discover files containing child pornography.[124]

The analysis does not end there, however. It should also require courts to explore any internal policies and procedures of the specific internet service as well as the terms of service governing the client relationship to determine whether the private party was acting as an "agent[] or instrument[] of the government."[125] The defendant in *Stevenson* argued that even if the ISP was "not transformed into a government agent by operation of law,"[126] a look at the particular circumstances could prove that the ISP was acting as an instrument of the government—affirmatively conducting hash-based evaluations in attempts to assist the government in discovering files containing child pornography, or developing its scanning program for its own business reasons.[127]

The developments in hashing technology have raised unforeseen difficulties in the application of the private search doctrine. In *Reddick*, the Fifth Circuit correctly noted that "the Fourth Amendment is not implicated where the government does not conduct the search itself, but only receives and utilizes information uncovered by a search conducted by a private party."[128] Unfortunately, that was the extent of the analysis afforded to the defendant. The court stated:

> The private search doctrine decides this case. A private company determined that the hash values of files uploaded by Mr. Reddick corresponded to the hash values of known child pornography images. The company then passed this information on to law enforcement. This qualifies as a "private search" for Fourth Amendment purposes. And the government's subsequent law enforcement actions in reviewing the images did not affect an intrusion on [the defendant's] privacy . . . .[129]

Not only are there splintered decisions among federal circuit courts regarding which test to use, but there is also a circuit split regarding the scope of the search. The split makes the time ripe for the Supreme Court

124. *Stevenson*, 727 F.3d at 830. AOL used its automatic hash-based evaluation too to identify files on Defendant's computer containing child pornography. The hash value match automatically alerted the National Center of Missing and Exploited Children, who then reported the tip to the Iowa Department of Criminal Investigation. The law enforcement officers obtained a warrant and searched Defendant's home where they found 721 images of child pornography. Stevenson moved to suppress the images arguing that his rights were violated under the Fourth Amendment.

125. *Id.* at 829 (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

126. *Id.* at 830.

127. *Id.*

128. United States v. Reddick, 900 F.3d 636, 637 (5th Cir. 2018).

129. *Id.*

to articulate a more clear, operable and consistent framework for analyzing the private search doctrine as applied to ISPs.

B. Expectation of Privacy

In order to constitute a search or seizure under the confines of the Fourth Amendment, the search or seizure must reasonably "intrude[] upon a reasonable expectation of privacy in . . . a significant way."[130] In *Katz v. United State*s, the Supreme Court changed the understanding of the "reasonable expectation of privacy" analysis into a more nuanced understanding of the privacy protected by the Fourth Amendment:

> For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his home or office, is not subject to the Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[131]

In Justice Harlan's concurrence, he articulated a two-prong test to determine when a search is unreasonable: "[F]irst that a person exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[132] Only activities that "intrude[] upon a reasonable expectation of privacy in . . . a significant way" constitute a search under the Fourth Amendment's reasonableness requirement.[133] The rationale behind the "reasonable expectation of privacy" standard is that, once confidential information is revealed by a private party, the expectation of privacy is thwarted. The second inquiry of this four-part proposal requires courts to consider whether the defendant had a subjective expectation that the thing seized would "remain free from governmental intrusion."[134]

---

130. United States v. Paige, 136 F. 3d 1012, 1017 (5th Cir. 1998) (quoting United States v. York, 895 F.2d 1026, 1028 (5th Cir. 1990)).

131. Katz v. United States, 389 U.S. 347, 351 (1967) (holding that the government's attachment of an electronic listening device in the telephone booth where defendant made a call violated the defendant's justified reliance on his right to privacy and thus, the government's actions constituted a "search and seizure" within the meaning of the Fourth Amendment).

132. *Id.* at 361 (Harlan, J., concurring).

133. *Paige*, 136 F.3d at 1017 (quoting *York*, 895 F.2d at 1028).

134. United States v. Ibarra, 948 F.2d 903, 906 (5th Cir. 1991) (quoting United States v. Haydel, 649 F.2d 1152, 1155 (5th Cir. 1981)) ("In assessing whether a legitimate expectation of privacy exists, we examine several factors including 'whether the defendant has a possessory interest in the thing seized or the place searched, whether he has the right to exclude others from that place, whether he has exhibited a subjective expectation of privacy that it would remain free from governmental intrusion, whether he took normal precautions to maintain privacy and whether he was legitimately on the premises.").

The principles of the third-party doctrine are straightforward: the government may obtain information from third parties without first procuring a search warrant. The long-standing third-party doctrine, recognized in *United States v. Miller* in 1976, has endured for more than 40 years.[135] It "applies specifically when an individual voluntarily conveys the information to a *third-party* that the government later obtains."[136] Under the third-party doctrine, individuals who entrust confidential information in a third party relinquish any Fourth Amendment protection of that information—even if it is later revealed to government authorities.[137] This is true even when an individual reveals information to a third party "on the assumption that it will be used only for a limited purpose and the confidence placed in a third party will not be betrayed."[138] For example, generally, when an individual saves files to a personal hard drive, they have demonstrated a "reasonable expectation of privacy in the contents of those files."[139] However, "[a] computer owner or user may lose her expectation of privacy in the contents of the computer's memory if she makes the computer generally accessible to others."[140] When the same individual places the files on a cloud server, such as Microsoft SkyDrive, he creates a reasonably foreseeable risk of intrusion, and it cannot be said that he has manifested that same expectation of privacy.[141]

The third-party doctrine is regularly raised as a defense to the notion that a defendant possessed a reasonable expectation of privacy in ESI. In *United States v. Miller*, the Supreme court held that a bank customer had "no protectible Fourth Amendment interest" in the copies of checks and other bank records retained by the bank.[142] It articulated a clear rule stating that the information revealed to a third party is not afforded Fourth Amendment protection even when revealed on the assumption that "it will be used only for a limited purpose and the confidence placed in the third

135. United States v. Miller, 425 U.S. 435, 443 (1976).

136. In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1027 (N.D. Cal. 2015).

137. Stephen E. Henderson, *After* United States v. Jones, *After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 437 (2013) ("[We] have held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party] to the Government authorities. . . .").

138. *Id*.

139. United States v. Barth, 26 F. Supp. 2d 929, 937 (W.D. Tex. 1998).

140. Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. && TECH. 75, 84 (1994).

141. *Barth*, 26 F. Supp. 2d at 937.

142. United States v. Miller, 425 U.S. 435, 437 (1976).

party will not be betrayed."[143] The justifications for the third-party doctrine stem from the reasonable expectation of privacy test established by the Supreme Court in 1967 in *Katz*. In *Katz*, the defendant made telephone calls from a public telephone booth to make gambling wagers.[144] FBI agents attached an electronic recording device to the outside of the booth.[145] The United States District Court for the Southern District of California convicted Katz for transmitting wagering information by telephone.[146] The government introduced evidence of the recorded telephone conversations, and the defendant objected.[147] The Court discarded the previous notion that there are "constitutionally protected areas" and constitutionally unprotected areas, stating that "[T]he court has never suggested that this concept can serve as a talismanic solution to every Fourth Amendment problem."[148] It emphasized that "the Fourth Amendment protects people, not places"; therefore, "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[149]

As *Katz* suggests, if a court were to categorically define what digital media is protected under the reasonable expectation of privacy theory, it would essentially undermine the logical reasoning behind the Supreme Court's third-party doctrine. There is no magical line drawn to determine what forms of electronic communication are and are not protected. Based on a subjective standard, it would be reasonable to assume that an individual has an expectation of privacy in an email sent to a family member via his private email. Conversely, when a person uploads illicit files to a cloud sharing server operated by Microsoft, does he really have an expectation that those contents will remain free from inspection by the government? Or does he assume the risk that the information could be reported to authorities? To enlist a categorical rule providing all criminal defendants with a reasonable expectation of privacy in images they upload to cloud sharing software would be a misguided application of Fourth Amendment principles. Therefore, the second inquiry under this proposed analysis requires courts to step into the defendant's mind to determine his actual expectations at the time he or she engaged in the illegal act.

143. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 752 (1971)).
144. Katz v. United States, 389 U.S. 347, 348 (1967).
145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.* at 351 n.9.
149. Katz v. United States, 389 U.S. 347, 351 (1967).

C. Are Hash Value Matches an Adequate Basis for Probable Cause?

Courts use hash-based examination as a trustworthy procedure to establish that the results are an "authentic product of the evidence seized."[150] Some courts even compare the hash value to digital fingerprints.[151] How reliable do these digital fingerprints have to be? The Fourth Amendment requires a showing of probable cause before a search warrant may be issued.[152] The Supreme Court defined probable cause as "a fair probability that contraband or evidence of a crime will be found in a particular place."[153] When presented with issues involving hash-based searches, the third prong of the test requires courts to determine whether the hash value match serves as an adequate basis for probable cause. Although there is always a small risk of mistake that could lead to a violation of constitutional rights, all courts that have addressed the use of hash searches as they pertain to illicit material generally "[find] them legal and reliable."[154] However, the district court in *Reddick* noted that "without viewing the electronic image or the material from which the matching hash value was sourced, one cannot say with certainty that the electronic file is, in fact, contraband." [155]

An alteration of even a single pixel of a digital file will result in a different alphanumeric value.[156] Thus, once a hash value match occurs, the "suspected copy can be determined to be identical to the original file" that is stored in a database.[157] Reddick argued that, because law enforcement officers conducted the subsequent search pursuant to a warrant based on information accessed through a warrantless search, the evidence must be suppressed.[158] The Fifth Circuit failed to determine

150. Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y 2, 9 (2007).

151. *See, e.g.*, United States v. Farlow, 681 F.3d 15, 19 (1st Cir. 2012); United States v. Thomas, 788 F.3d 345, 348 n.5 (2nd Cir. 2015); United States v. Apple MacPro Comput., 851 F.3d 238, 242 n.3 (3rd Cir. 2017) ("a 'hash' is '[a] mathematical algorithm that calculates a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently ensuring the data has not been modified."); United States v. Wellman, 663 F.3d 224, 226 n.2 (4th Cir. 2011).

152. Illinois v. Gates, 462 U.S. 213, 238 (1983).

153. *Id.*

154. Martin, *supra* note 3, at 702.

155. United States v. Reddick, 2017 U.S. Dist. LEXIS 56577, at *3 (S.D. Tex. Apr. 13, 2017).

156. United States v. Keith, 980 F. Supp. 2d 33, 36–37 (D. Mass. 2013) ("Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value.").

157. *Id*.

158. *Reddick*, 2017 U.S. Dist. LEXIS 56577, at *8.

whether the hash value match established "probable cause" as to yield a "fair probability that contraband will be found in a particular place."[159]

In *United States v. Cartier*, a peer-to-peer file-sharing network used hash-based evaluation to conduct searches of shared files.[160] After receiving several tips of images depicting child pornography previously seized by law enforcement, the Spanish Guardia Civil Computer Crime Unit ("SGCCCU") notified the FBI's Innocent Images Unit.[161] The FBI obtained a search warrant for the defendant's home based on the hash match.[162] The defendant filed a motion to suppress and asserted that the search warrant lacked probable cause because the detective relied upon hash values that had not been viewed prior to the issuance of the warrant.[163] The Eighth Circuit stated that "[p]robable cause exists when a 'practical, common-sense' inquiry that considers the totality of circumstances set forth in the information before the issuing judge yields a 'fair probability that contraband and evidence of a crime will be found in a particular place.'"[164] The defendant argued that, because there was no human review of the files, there was, in fact, a possibility that two different files on a computer will "collide or overlap," generating the same hash value.[165] However, the court stated that the proper test is not whether it is *certain* that contraband will be found, but whether it is fairly probable.[166] The lack of physical examination by an individual does not undermine the reliability of hash-based examination and "does not necessitate a finding that probable cause was lacking."[167]

Considering the totality of the circumstances, courts must verify the reliability of the computer software program's hashing technology. Although some courts choose to analogize hashing to a drug-sniffing dog, this analogy actually undervalues the reliability of hashing.[168] In fact, it

159. Illinois v. Gates, 462 U.S. 213, 273 (1983) (White, J., concurring).

160. United States v. Cartier, 543 F.3d 442, 444 (8th Cir. 2008).

161. *Id.* at 445.

162. *Id.*

163. *Id.*

164. *Id.* at 446 (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

165. *Id.* at 446 ("Although Cartier correctly asserts that no one reported seeing images of child pornography on his computer prior to the execution of the search warrant, the lack of such evidence does not necessitate a finding that probable cause was lacking.").

166. United States v. Cartier, 543 F.3d 442, 446 (8th Cir. 2008).

167. *Id.*

168. Robyn Burrows, *Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files*, 19 GEO. MASON L. REV. 255, 279 (2011) ("Hashing is actually much more accurate than a dog sniff since it is almost mathematically impossible to mistake one file for another.").

has been regarded as 99.9999% reliable by law enforcement officers.[169] But that does not conclude the third prong of this analysis. It is not enough for courts to breeze over this step by simply stating that hash-based examination is reliable. It is extremely critical that they actually verify the reliability and accuracy of the computer software program itself—considering the resources, reliability, and records of each individual computer software program before determining whether the hash value match provides sufficient probable cause. The Fifth Circuit set a dangerous precedent by not engaging in the same inquiry as the Eighth Circuit.

D. Expansion of the Private Search

The last prong of the analysis requires courts to examine whether the additional intrusion by the governmental entity exceeded the scope of the private search. Dating back to 1921, the Supreme Court recognized that the scope of the Fourth Amendment extends only to protect against searches by the government:

> [T]he Fourth Amendment protects only against searches and seizures which are made under governmental authority, real or assumed, or under color of such authority. If papers have been seized, even though wrongfully, by one not acting under color of authority, and they afterwards come to the possession of the Government, they may be properly used in evidence.[170]

In 1980, the Supreme Court reiterated that there is "'nothing wrongful' about the government's examination of the contents of the packages that had been opened by private parties,"[171] so long as they do not "exceed the scope of the private search."[172] Absent an independent right to conduct the search,[173] the government must stay strictly within the realm of the third party search. So long as this standard is adhered to, and

169. United States v. Bershchansky, 958 F. Supp. 2d 354, 357 n.3 (E.D.N.Y. 2013). *See also* Martin, *supra* note 3, at 705.

170. Burdeau v. McDowell, 256 U.S. 465, 470 (1921). *See also* Boyd v. United States, 116 U.S. 616, 630 (1886) (The principles of the Fourth amendment "apply to all invasions on the part of the government and its employees to the sanctity of a man's home and the privacies of life."); Weeks v. United States, 232 U.S. 383, 386 (1914)("The Fourth Amendment is not directed to individual misconduct of state officers. Its limitations reach the Federal Government and its agencies.").

171. Walter v. United States, 447 U.S. 649, 656 (1980) (White, J., concurring in part).

172. *Id.* at 657 (majority opinion) ("Even though some circumstances—for example, if the results of the private search are in plain view when materials are turned over to the Government—may justify the Government's re-examination of the materials, surely the Government may not exceed the scope of the private search unless it has the right to make an independent search.").

173. *Id.*

the search is within the realm of the third-party search, the evidence may lawfully be used against the accused.[174] The notion behind this theory is that once the third-party search occurs, the defendant's reasonable expectation of privacy has already been thwarted, and thus, the subsequent search by the government does no harm.

To answer the question of whether the additional intrusion by the government exceeded the scope of the private search, courts must start by determining how thorough and complete the private search was.[175] *Jacobsen* is the leading Supreme Court case analyzing the "expansion of the private search" theory. It held that "governmental inspections following on the heels of private searches are not searches at all as long as police do no more than the private parties have already done."[176] The issue surrounding this last prong is that not all ISPs that use hash-based examination have resources to provide "human reviewers" to review each hash match that comes through to ensure that it is in fact illicit material.[177] Thus, if the ISP relies solely on the hash match to forward the tip to NCMEC and an employee at NCMEC then views the images, is that a categorical expansion of the private search that triggers the Fourth Amendment?

Very recently, in a case similar to *Reddick*, the Supreme Court of Vermont answered the question of whether the searches performed by NCMEC and law enforcement expanded on the initial search by the ISP.[178] The defendant in *State v. Lizotte* registered an account with AOL.[179] AOL's hash value tool, Image Detection Filtering Process, identified two emails that contained suspected child pornography.[180] Without viewing the content of the two emails, AOL submitted two reports to NCMEC.[181] An NCMEC analyst reviewed the video attachment, confirming that it was child pornography.[182] The analyst then

174. *Id.* at 656 ("It has, of course, been settled . . . that a wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and that such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully.").

175. JOHN WESLEY HALL, JR., SEARCH AND SEIZURE § 18.06 (5th ed. 2019).

176. United States v. Jacobsen, 466 U.S. 109, 129 (1984) (White, J. concurring).

177. United States v. Coyne, 387 F. Supp. 3d 387, 392 (D. Vt. 2018) ("A large and sophisticated [ISP] such as Microsoft employs its own human reviewers before forwarding the tip [to NCMEC]. Small [ISPs] such as Chatstep may choose to forward tips automatically without reviewing any images themselves.").

178. State v. Lizotte, 197 A.3d 362, 366 (Vt. 2018).

179. *Id.*

180. *Id.* at 368.

181. *Id.*

182. *Id.*

sent a notification to the Office of the Vermont Attorney General.[183] A detective from the Attorney General's Internet Crimes Division opened and viewed both email attachments and then applied for a warrant to search the defendant's residence.[184] The defendant was charged with possession of child pornography, promoting child pornography, aggravated sexual assault, and lewd and lascivious conduct.[185] He moved to suppress, arguing that he had a reasonable expectation of privacy in his emails and that his Fourth Amendment rights were violated because law enforcement opened the attachment to his email before obtaining a warrant.[186] The question in *Lizotte* was whether opening that attachment and email allowed the government to "learn something that had not already been discovered during the private search."[187] The court concluded that NCMEC and the law enforcement officers did not expand the search conducted by AOL by opening the video attachment, because the document was already viewed by AOL through hashing technology.[188] The hash value match confirmed the contents of the file. NCMEC and law enforcement officers already knew what the attachment contained and could not learn more than was already known by AOL.[189] The generally accepted rule is that government may utilize information that is voluntarily disclosed to a governmental entity, despite a defendant's expectation of privacy in that information.[190]

When there *is* a human examiner reviewing the images before sending the tip to NCMEC, the Supreme Court's decisions in *United States v. Jacobsen* and *Walter v. United States* govern. In *Walter*, employees of a private company opened a carton mistakenly delivered to their address.[191] Inside the box were sealed films "depicting homosexual activities."[192] The employees viewed the outside of the packages before notifying the FBI of suspected obscenity.[193] The FBI agents used a projector to confirm that the films were, in fact, obscenity.[194] In *Jacobsen*, a FedEx employee viewed the contents of a package before notifying the

183. *Id.*
184. State v. Lizotte, 197 A.3d 362, 369 (Vt. 2018).
185. *Id.*
186. *Id.*
187. *Id.* at 374.
188. *Id.* at 370.
189. *Id.* at 374.
190. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
191. Walter v. United States, 447 U.S. 649, 651–52 (1980).
192. *Id.* at 651.
193. *Id.* at 652.
194. *Id.*

DEA of suspected drugs.[195] The DEA arrived and conducted a field test to confirm that the contents were, in fact, cocaine.[196] While *Walter* held that the FBI significantly expanded on the view of the private party by running the contents through a projector to determine what the substance inside the package was, *Jacobsen* held to the contrary. In *Jacobsen*, although the field test conducted by the DEA exceeded the scope of the mere viewing by the private party, "[a] chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy."[197] *Jacobsen* removed the requirement of actual, complete identity of the substance by the private party.

When there is *not* a human examiner reviewing the images before sending the tip to NCMEC, it is more comparable to the Tenth Circuit Decision in *United States v. Ackerman*.[198] In *Ackerman*, AOL forwarded a tip to NCMEC based solely on a hash value match.[199] An NCMEC analysis then viewed the images before alerting law enforcement officers.[200] The court determined that the private search doctrine did not apply because NCMEC was the first to open and review the images.[201] Resolving this issue takes us back to the question of whether a hash value match is an adequate basis for probable cause. If the hash value match is comparable to, as it is frequently dubbed, a fingerprint, is the subsequent search by NCMEC really an expansion of the private search when the private party did not view the images? If so, this also begs the question of whether the good faith exception to the exclusionary rule applies when a governmental agent opens the files without authorization. An unconstitutional search undertaken in good faith and based on a reasonable mistaken belief gives rise to a good faith exception to the exclusionary rule.[202]

The Court in *Reddick* did not analyze whether Detective Ilse's subsequent search was an expansion of the initial private search or whether it was reasonable. Nevertheless, it is recommended that the government's search is deemed reasonable if the court used the test from *Jacobsen* to balance the nature and quality of the search on the defendant's Fourth Amendment interests against the importance of the governmental

195. United States v. Jacobsen, 466 U.S. 109, 111 (1984).
196. *Id.* at 111–12.
197. *Id.* at 123.
198. United States v. Ackerman, 831 F.3d 1292, 1292 (10th Cir. 2016).
199. *Id.* at 1294.
200. *Id.*
201. *Id.* at 1305–06.
202. *See, e.g.*, Heien v. North Carolina, 547 U.S. 54 (2014).

interest alleged to justify the intrusion.[203] Jacobsen recognizes that the exceptions to the general rule that warrantless searches are unreasonable are based on a "balancing [of] the need to search against the invasion which the search entails."[204] The government undoubtedly has an exponential interest in combating the online distribution of child sexual abuse and pornography.

V. CONCLUSION

Courts must exercise caution when admitting evidence into the record obtained through hash value algorithms. It is not, however, per se unconstitutional for private internet service providers to use hash-based examination. The precise capabilities of the hash value allow ISPs to identify identical files without examining each individual file and their content.

When used in the proper manner, its wide-reaching effect saves law enforcement officers time and money while simultaneously tapering the distribution of child pornography over our readily accessible internet and cloud sharing software. The beneficial outcomes hash-based examination can provide to society fortifies the need for a universal standard employed throughout our court system to avoid pervasive misapplication of the Fourth Amendment.

The New York Times recently published an article noting that images and videos of child pornography being shared over the internet is at a record 45 million, "which is increasingly cloaked by technology."[205] This is where ISPs can step in with surveillance of their platforms. However, ISPs must proceed with caution to avoid collaborating too closely with law enforcement officials such that they are considered governmental agents. In fact, many powerful tech companies have already begun to utilize hashing technology, including AOL, Microsoft, Facebook, Google and others.[206] With the increased surveillance by ISPs, the Supreme Court must keep up by carefully crafting a universal analysis for cases involving alleged Fourth Amendment violations related to the

203. United States v. Jacobsen, 466 U.S. 109, 125 (1984) (quoting United States v. Place, 462 U.S. 696, 703 (1983)).

204. *Id.* at 141 (Brennan, J., dissenting) (quoting Camara v. Municipal Court, 387 U.S. 523, 537 (1967)).

205. Michael H. Keller & Gabriel J.X. Dance, *The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?*, N.Y. TIMES, https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html [https://perma.cc/2HZS-YNAX]. Last year alone, there were 18.4 billion reports of child sexual abuse imagery.

206. *Id.*

use of hash values and child pornography. It is essential for our case law to evolve with society: ensuring protection of constitutional rights and preventing misinterpretation by the courts. Paying close attention to the circumstances surrounding the search, courts must determine the answer to the following questions: (1) Was the individual that conducted the initial search in fact acting as a private individual and not a state actor? (2) Was the defendant's reasonable expectation of privacy thwarted by the third-party doctrine? (3) Was there probable cause for the warrantless search? (4) Was the state actor acting within the scope of the private party search? If the answer to any of the preceding questions is no, the defendant should be entitled to suppress the evidence gained during the unconstitutional search. When courts choose to implement this standard analysis, United States citizens receive proper protection both from unreasonable search and seizure by the government, as well as protection from the crime of child exploitation.