SMU | Dedman School of Law

SMU Law Review

Volume 72 | Issue 2 Article 14

2019

"Hashing" in the Cloud: The Private Search Defense is Active and Potent

Tri T. Truong
Southern Methodist University, Dedman School of Law, tttruong@smu.edu

"HASHING" IN THE CLOUD: THE PRIVATE SEARCH DEFENSE IS ACTIVE AND POTENT

*Tri Truong**

THE touchstone of the Fourth Amendment is reasonableness, for it concerns the realm of individual liberty, not expediency in law enforcement.[1] And it is in this light that the Supreme Court has recognized a person's constitutionally protected "reasonable expectation of privacy."[2] The private search doctrine evolved in response to contemporary developments to enable the government to repeat a search previously executed by a private party without violating the Fourth Amendment insofar as the latter search does not exceed the scope of the private conduct.[3] The rationale is that once information is unveiled by a private search, the expectation of privacy is defeated.[4] This note will examine the Fifth Circuit's application of the private search doctrine to searches of electronic files, and briefly discuss an alternative analysis under the single-purpose container doctrine.

The rise of the private search defense is a troubling development, particularly in the electronic era, as third parties have become indispensable surrogates, allowing the police to eschew violating Fourth Amendment protections in ways that they themselves could not perform absent a search warrant. A common example is hash value or "hashing" technology used by private entities to track digital images and compare them to known child pornography in certain national libraries.[5] The hash function utilizes an algorithm to trawl large amounts of electronic information indiscriminately and assign "unique identifiers" to the files.[6] A fundamental principle of hashing is that the hash itself must not reveal any

* J.D. Candidate, SMU Dedman School of Law, May 2019; B.S., Texas A&M, May 2008. I would like to thank my family for their support. I am also grateful to Professor Jenia Turner, Professor Cassie DuBay, and my colleagues for their helpful comments.

1. United States v. Reddick, 900 F.3d 636, 637 (5th Cir. 2018), *petition for cert. filed*, (U.S. Nov. 19, 2018) (No. 18-6734).

2. United States v. Jones, 565 U.S. 400, 406 (2012) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

3. *See* United States v. Jacobsen, 466 U.S. 109, 115–16 (1984).

4. *Id.* at 117.

5. *See Reddick*, 900 F.3d at 636–37.

6. *See id.* at 637; Alexandra L. Mitter, *Deputizing Internet Service Providers: How the Government Avoids Fourth Amendment Protections*, 67 N.Y.U. ANN. SURV. AM. L. 235, 260 (2011).

information about the input data.[7] Facing an unending distribution of online child pornography and the dilemma that the private search doctrine would place police activities beyond the reach of the Fourth Amendment, courts struggle to resolve the tension between an individual's privacy in the digital sphere and the utility of the government search. In attempting to strike the proper balance, the Fifth Circuit understandably erred.

In *United States v. Reddick*, the Fifth Circuit was presented with a novel question: whether the user had any remaining expectation of privacy after a private party's hash value analysis of the uploaded files revealed a match of child pornography such that a warrant was necessary to permit police to view the images.[8] The Fifth Circuit erroneously held that the Fourth Amendment was not implicated when the officer viewed the images reported by the third-party as matching the hash values of known images of child pornography.[9] By oversimplifying and expanding the scope of the private search exception in this narrow context, the Fifth Circuit radically altered Fourth Amendment jurisprudence. In effect, *Reddick* not only erodes Fourth Amendment protections, but also invites practical mischief and creates a significant disincentive for police to seek a warrant. *Reddick* is further exacerbated by a potential split with the Tenth Circuit.

The defendant, Henry Reddick (Reddick), uploaded his computer files to a cloud storage system operated by Microsoft.[10] Microsoft utilized a proprietary software to automatically detect the hash values of Reddick's electronic files and compared the results with the hash values of known images of child pornography.[11] This software allows the identification of illicit content (such as child pornography) without actually exposing the images to viewers.[12]

When the software intercepted Reddick's files based on the corresponding hash values of apparent child pornography in the National Center for Missing and Exploited Children (NCMEC) database, Microsoft copied the unopened electronic files and sent them together with Reddick's subscriber information to NCMEC.[13] NCMEC, without opening the files, confirmed the hash value match and forwarded that information to local law enforcement for further investigation.[14] Upon receiving the reports, the detective visually confirmed that the images depicted child pornography prior to securing a warrant.[15] After the police executed a warrant and searched Reddick's residence, they found addi-

7. Stephen Hoffman, *An Illustration of Hashing and Its Effect on Illegal File Content in the Digital Age*, 22 INTELL. PROP. & TECH. L. J. 6, 7 (2010).
8. *See Reddick*, 900 F.3d at 638.
9. *Id.* at 639–40.
10. *Id.* at 637.
11. *Id.* at 637–38.
12. United States v. Reddick, No. 2:16-CR-928, 2017 WL 1353803, at *2 (S.D. Tex. Apr. 13, 2017), *aff'd*, 900 F.3d 636 (5th Cir. 2018).
13. *Id.* at *3.
14. *Id.*
15. *Reddick*, 900 F.3d at 638.

tional evidence of child pornography in Reddick's possession.[16]

Reddick was charged with possession of child pornography.[17] He moved to suppress the evidence on the basis that the officer's viewing of the images exceeded the scope of the private search, and therefore, the exclusionary rule barred the admission of any additional evidence of child pornography found in his home.[18] On that record, the district court nevertheless found that, even assuming that the officer's viewing of the images exceeded the private party's search, the police acted in good faith when they relied upon the warrant's apparent validity to search Reddick's residence.[19] The district court therefore denied his motion.[20]

On appeal, the Fifth Circuit upheld the district court's decision under the private search doctrine.[21] The Supreme Court articulated the private search doctrine in *Walter v. United States*,[22] and further elaborated in *United States v. Jacobsen*.[23] *Walter* involved the FBI's warrantless viewing of obscene filmstrips which had been mistakenly delivered to a private party who then turned them over to the agency.[24] The labels on the exteriors of the boxes indicated that the films contained pornographic activities.[25] Prior to contacting the FBI, an employee attempted, without success, to view the film by holding it up to the light.[26] In a plurality opinion, the Supreme Court held that the subsequent warrantless screening of the films by federal agents was an unlawful extension of the private search because the agents' inquiry was more intrusive than the private party's original visual inspection of the labels. [27] The Court reasoned that the projection of the films was a "significant expansion" of the private party's search because, prior to the screening of the films, agents could only draw inferences about the contents of the films based on their labels.[28] Put simply, the sender's expectation of privacy was not wholly stripped when the employees opened the packages to reveal the labels on the boxes because the unfrustrated portion of the encroachment would nonetheless remain.[29] Thus, the additional search by the FBI breached the remaining portion of the sender's expectation of privacy that had not been frustrated by the private search.[30]

---

16. *Id.*
17. *Id.*
18. *Id.*
19. *Id.* The good faith exception is available when law enforcement reasonably relied on a warrant, but it is later found to be defective. *See* United States v. Leon, 468 U.S. 897, 926 (1984).
20. *Reddick*, 900 F.3d at 638.
21. *Id.*
22. 447 U.S. 649, 658–59 (1980).
23. 466 U.S. 109, 115 (1984).
24. *Walter*, 447 U.S. at 651–52.
25. *Id.* at 652.
26. *Id.*
27. *Id.* at 657–58.
28. *Id.*
29. *See id.* at 658–59.
30. *See id.*

In *Jacobsen*, the Court clarified that the "additional invasions of . . . privacy by the government agent must be *tested by the degree* to which they exceeded the scope of the private search."[31] There, employees of Federal Express opened a damaged package and found several plastic bags of a white, powdery substance concealed in layers of crumpled newspaper.[32] They then notified the Drug Enforcement Administration, who conducted a visual inspection as well as chemical field tests on the white powder and determined the powder was cocaine.[33] The Court held that the agents did not run afoul of the Fourth Amendment by physically examining the powder because any expectation of privacy had already been thwarted when the employees examined the package and discovered the white powder.[34] The Court reasoned that the field tests, which determined whether a particular substance is cocaine, did not infringe the defendants' privacy interest because the field tests could reveal "no other arguably 'private' fact."[35]

The *Reddick* court, relying on *Jacobsen*, curiously held that when the detective opened and viewed the images, that was not a significant expansion of the private search sufficient to constitute a separate search.[36] The court reasoned that, like *Jacobsen*, when Reddick uploaded the "package" of digital files, it "was inspected and deemed suspicious by a private actor."[37] It follows that Reddick had no reasonable expectation that the contents of his files would remain free from inspection by the government following Microsoft's search.[38] Thus, when the government opened and viewed the files—"akin to the government agents' decision to conduct chemical tests on the white powder in *Jacobsen*"—that was a step taken merely to "dispel[ ] any residual doubt about the contents of the files."[39] Consequently, the court concluded that the government learned nothing from the viewing of the files to the extent that those files had already been examined by a private party.[40]

The problem with the court's analysis is that it incorrectly treated the hash identification of the files as the equivalent of evidence of contraband and permitted hindsight to color the evaluation of the reasonableness of the search. Here, the private search could only disclose whether there was a positive match of child pornography. While hashing has been a powerful tool for detecting known images of child exploitation, the district court explained that "one cannot recreate an image or determine its con-

31. United States v. Jacobsen, 466 U.S. 109, 115 (1984) (emphasis added).
32. *Id.* at 111.
33. *Id.* at 111–12.
34. *Id.* at 120, 126.
35. *Id.* at 123.
36. United States v. Reddick, 900 F.3d 636, 639 (5th Cir. 2018), *petition for cert. filed*, (U.S. Nov. 19, 2018) (No. 18-6734).
37. *Id.*
38. *Id.*
39. *Id.*
40. *Id.*

tent *solely* from its hash value."[41] This observation is consistent with the basic properties of a hash function. It is one thing to say that "hash value comparison 'allows law enforcement to identify child pornography with almost absolute certainty,'"[42] and another that the electronic file is, in fact, contraband, without viewing the electronic images or the corresponding source materials. In a similar vein, to say that "[t]he government effectively learned nothing from [the detective's] viewing of the files"[43] after a private search is to accept the shortcomings of hindsight judgment and ignore the fact that the Fourth Amendment not only protects against unreasonable searches, but also prevents police abuses.

Moreover, the court erroneously analogized the detective's viewing of the electronic files to the chemical tests in *Jacobsen* for two reasons. First, his visual inspection, unlike hashing or a chemical test, could reveal not only a binary response, but also the potential discovery of non-contraband or other incriminating information.[44] Indeed, the *Jacobsen* Court stated that "[the chemical tests] could tell him nothing more, not even whether the substance was sugar or talcum powder."[45] Thus, the court's conclusion that subsequent review of the files was not an expansion of the private search ignores its multiplying effect. In this respect, Professor Orin Kerr's observation is apt: "The opener of the file sees the full image, and then, after seeing the image, makes a judgment about whether the file is child pornography."[46] Second, the holding of the *Jacobsen* opinion is premised, in part, on the proposition that, like a chemical test, a "canine sniff" test is not entitled to Fourth Amendment protection because "the sniff discloses only the presence or absence of narcotics."[47] And, because the field test could reveal "no other arguably 'private' fact," the test "compromise[d] no legitimate privacy interest."[48] Far from a "sniff test" (or a chemical test), an "investigative technique [that] is much less intrusive than a typical search" as exemplified in *Jacobsen*, a visual search significantly jeopardizes the sense of security that is distinct from the hash analysis because more is learned than the mere presence or absence of child pornography.[49] A visual confirmation, for example, could help determine the identity, gender, location, time, and possibly the approximate

41. United States v. Reddick, No. 2:16-CR-928, 2017 WL 1353803, at *2 (S.D. Tex. Apr. 13, 2017), *aff'd*, 900 F.3d 636 (5th Cir. 2018) (emphasis added).

42. *Reddick*, 900 F.3d at 639 (quoting United States v. Larman, 547 F. App'x 475, 477 (5th Cir. 2013)).

43. *Id.* at 640.

44. *See* Orin S. Kerr, *Opening a File Whose Hash Matched Known Child Pornography Is Not a 'Search,' Fifth Circuit Rules*, LAWFARE (Aug. 18, 2018, 10:09 AM), https://www.lawfareblog.com/opening-file-whose-hash-matched-known-child-pornography-not-search-fifth-circuit-rules [https://perma.cc/Q8QL-BAFW].

45. United States v. Jacobsen, 466 U.S. 109, 122 (1984).

46. Kerr, *supra* note 44. Professor Kerr is a learned scholar of criminal procedure and computer crime law.

47. *Jacobsen*, 466 U.S. at 124 (quoting United States v. Place, 462 U.S. 696, 707 (1983)).

48. *Id.* at 123.

49. *Id.* at 124; *see also* Kerr, *supra* note 44.

age of the victim. It may also disclose incriminating information such as the presence of the accused in those images. The consequent legal question, then, is whether a positive identification of one or more victims in the pictures following the detective's viewing of the files is consistent with the Fourth Amendment.[50] *Reddick* suggests the answer is yes.

In concluding that the detective's viewing was not a "significant expansion" of the private search, the *Reddick* opinion can be read as taking the position that the officer did not exceed the prior private search when he examined these files perhaps more thoroughly or in a different manner. However, the proper test concerning additional invasions of privacy by the government, as announced in *Jacobsen*, "must be tested by the degree to which they exceeded the scope of the private search," not whether the government exceeds the scope of a private search when it examines the same materials as the private party in a more thorough or different manner.[51] The *Jacobsen* formulation made clear that the government's ability to conduct a warrantless follow-up search is expressly circumscribed by the scope of the private search because the detective's authority to duplicate a private search is distinct from his authority to conduct an independent search.[52] The test of degree is subtle but significant, for it recognizes any residual privacy must not be unduly infringed. The *Reddick* framework, on the other hand, would effectively and impermissibly subsume the government search and eliminate any privacy interests altogether following a private search. Accordingly, unlike *Jacobsen*, the revelation of intimate information by a visual confirmation should not obviate the warrant requirement because it could reveal other "private" facts, thereby compromising the owner's privacy interest associated with that search.

Although *Reddick* was not analyzed under *Walter*, that case involved facts significantly analogous to those present in *Reddick*.[53] Like *Walter*, Microsoft's conclusion that the files were child pornography was based solely on the hash labels.[54] The detective had possession of Reddick's files for nearly a month before a warrant was issued.[55] Despite the court's view that the detective's viewing of the images was merely to confirm his suspicion, it was obvious that his reason for opening the files was an effort to search for evidence of a federal crime. Indeed, prior to the detective's viewing, police could only draw inferences about the contents of the files based on the hash values. The fact that the police might have probable cause, borne out by the private search, to believe the image files were child pornography and that the user had committed an offense would not alter the need to comply with the warrant requirement because the hash

50. *See* United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001) (leaving this issue open).

51. *Jacobsen*, 466 U.S. at 115.

52. *See id.* at 117–18.

53. *See* Walter v. United States, 447 U.S. 649, 651–52 (1980).

54. United States v. Reddick, No. 2:16-CR-928, 2017 WL 1353803, at *3 (S.D. Tex. Apr. 13, 2017), *aff'd*, 900 F.3d 636 (5th Cir. 2018).

55. *See id.*

values alone were not sufficient to support a conviction. Thus, the officer's subsequent viewing of the files made clear that further investigation of the contents of the files was necessary to obtain the evidence which was to be used at trial. Therefore, whatever expectation of privacy *in the hash values* of Reddick's files was frustrated as a result of a private search does not automatically negate the warrant requirement and justify a complete invasion of privacy in his files.[56]

Notably, the Fifth Circuit attempted to contrast its holding with *United States v. Ackerman*.[57] *Ackerman* involved the NCMEC's warrantless viewing of an email and three images of child pornography whose hash values did not correspond to known images of child pornography.[58] Although the Tenth Circuit overruled the district court's denial of the motion to suppress for reasons not at issue in *Reddick*, the *Ackerman* court signaled its stance that when a government agent opened an email after a private party had run a hash on the email, it exceeded rather than simply repeated the private party's search.[59]

To be sure, Professor Kerr has posited that the same result could be reached in *Reddick* under the single-purpose container doctrine.[60] Professor Kerr explains:

> It seems at least plausible that this could apply to opening a file with a known hash. If you know that a particular image has a particular hash, and you then have a file with that hash, then the information you have before you open the file "clearly announce[s] its contents . . . by its distinctive configuration" so that "its contents are obvious to an observer." The contents "can be inferred by [the file's] outward appearance," at least if you take "appearance" to include the hash value of the file.[61]

Ordinarily, police officers must secure a warrant before they may open a closed container because a person maintains a reasonable expectation of privacy by concealing the contents from plain view.[62] The single-purpose container exception permits the pre-warrant search of a container that is "so distinctive that its contents are a foregone conclusion and can therefore be said to be in plain view."[63] The Fifth Circuit has adopted a narrow view of this exception.[64] In *United States v. Villarreal*, the court affirmed the suppression of evidence when custom agents, without a war-

56. *See Walter*, 447 U.S. at 659.
57. 831 F.3d 1292, 1295 (10th Cir. 2016).
58. *Id.* at 1294, 1308 (finding NCMEC was a governmental entity or agent).
59. *Id.* at 1306 (quoting United States v. Jacobsen, 466 U.S. 109, 122 (1984)) ("NCMEC's search of the email itself quite easily 'could [have] disclose[d]' information previously unknown to the government besides whether the one attachment contained contraband.").
60. Kerr, *supra* note 44.
61. *Id.*
62. *See* United States v. Villarreal, 963 F.2d 770, 773 (5th Cir. 1992).
63. Allison M. Lucier, Comment, *You Can Judge a Container by Its Cover: The Single-Purpose Container Exception and the Fourth Amendment*, 76 U. CHI. L. REV. 1809, 1809 (2009).
64. *Villarreal*, 963 F.2d at 776 (citing *Walter*, 447 U.S. at 649).

rant, opened one of the containers labeled as phosphoric acid and discovered marijuana inside after their drug-sniffing canine alerted them to the containers. [65] The court rejected the government's view that the contents of the containers could be inferred from the description on the labels.[66] The court held that the owners did not surrender their expectations of privacy simply because the exterior descriptions on a container may reveal some information about its contents.[67] Citing *Walter*, the court stated, "If the government seeks to learn more than the label reveals by opening the container, it generally must obtain a search warrant."[68] In effect, the court's analysis removed any doubt that the label on the container was not part of the "outward appearance" of the container.[69]

Similarly here, application of the *Villareal* analysis militates for the finding that the hash value of each file is excluded from the "appearance" of the electronic file. Like *Villareal*, the individual computer files concealed their contents from plain view. In this context, the hash values themselves, albeit exposed to plain view, did not remove the owner's expectation that those contents would remain free from inspection by the government. Thus, their contents could not be inferred simply by looking at files, unless the hash value of each file is to be considered as part of the "appearance" of the file. To read "appearance" broadly is to contravene *Villareal*.

In sum, child pornography makes a difficult case. The Fifth Circuit's broad construction of the private search doctrine in *Reddick* is a vexing development, incompatible with *Walter* and *Jacobsen*, and hostile to the Framers' aim "'to place obstacles in the way of a too permeating police surveillance.'"[70] *Reddick* further implicates a potential split with the Tenth Circuit on whether the opening of a file after a private party's hash analysis exceeds the scope of the private search. The *Reddick* court certainly could have achieved the same result by affirming the district court's decision on a narrower ground—that is to say, the good-faith exception applied. Even if the good-faith doctrine did not apply, the detective's affidavit gave the district court a substantial basis for concluding that there was probable cause to search Reddick's residence. Instead, the Fifth Circuit legitimizes unreasonable police tactics and gives the police greater rein to search, despite existing probable cause sufficient to secure a warrant.

---

65. *Id.* at 772–73, 777.

66. *Id.* at 776.

67. *See* Walter v. United States, 447 U.S. 649, 654 (1980) (stating despite the fact that the incriminating nature of the contents of the films was depicted on the individual containers, the unauthorized viewing of the films constituted a Fourth Amendment violation). *Compare id.*, *with* United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001) ("The defendant's expectation of privacy in the contents of the container has already been frustrated because the contents were rendered obvious by the [private party's viewing of the images].").

68. *Villarreal*, 963 F.2d at 776.

69. *See id.* at 775–76 ("[A] label on a container is not an invitation to search it.").

70. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).