NO._____

IN THE SUPREME COURT OF THE UNITED STATES

HENRY FRANKLIN REDDICK,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Petition for Writ of Certiorari to the United States
Court of Appeals for the Fifth Circuit

PETITION FOR WRIT OF CERTIORARI

MARJORIE A. MEYERS
Federal Public Defender
Southern District of Texas
Attorney of Record

H. MICHAEL SOKOLOW
First Assistant Federal Public Defender
Attorneys for Petitioner
440 Louisiana Street, Suite 1350
Houston, Texas 77002-1056
Telephone: (713) 718-4600

QUESTION PRESENTED

I. Does a police officer violate the Fourth Amendment by opening a digital file and viewing an image in it without a warrant to confirm a private company's statement that the image is child pornography based solely on the company's comparison of the hash value of the image and the hash value in a digital database said to contain known child pornography when there is no evidence that the database actually contains images of child pornography, how the images in it were selected, or who selected them?

II. Does a police officer go beyond a private company's search, which merely compared the hash value of a digital file to hash values in a digital database said to contain known child pornography, by opening the file and viewing an image in it without a warrant to confirm that the image is child pornography?

III. Has this Court's holding in United States v. Jacobsen, 466 U.S. 109, 123-25 (1984) – that it was not a search for the government to field test white powder revealed to private employees when a package was damaged – been abrogated by the property rights analysis of the Fourth Amendment in United States v. Jones, 565 U.S. 400 (2012)? See United States v. Ackerman, 831 F.3d 1292, 1307 (10th Cir. 2016) (per Gorsuch, J.).

PARTIES TO THE PROCEEDINGS

The parties to the proceedings are named in the caption of the case before this Court.

TABLE OF CONTENTS

TABLE OF CONTENTS – (Cont'd)

Page

TABLE OF CITATIONS

Page

CASES

CONSTITUTIONAL PROVISION

TABLE OF CITATIONS – (Cont'd)

Page

STATUTES AND RULES

MISCELLANEOUS

PRAYER

Petitioner Henry Franklin Reddick respectfully prays that a writ of certiorari be granted to review the judgment of the United States Court of Appeals for the Fifth Circuit issued on August 17, 2018.

OPINIONS BELOW

On August 17, 2018, the United States Court of Appeals for the Fifth Circuit entered its judgment and opinion affirming Mr. Reddick's judgment of conviction. See United States v. Reddick, 900 F.3d 636 (5th Cir. 2018). The Fifth Circuit's opinion is reproduced as Appendix A to this petition. The district court entered its opinion on April 13, 2017, see United States v. Reddick, No. 2:16-CR-928, 2017 WL 1353803 (S.D. Tex. Apr. 13, 2017), and that opinion is reproduced as Appendix B to this petition.

JURISDICTION

On August 17, 2018, the United States Court of Appeals for the Fifth Circuit entered its opinion and judgment in this case. This petition is filed within 90 days after that date and thus is timely. See Sup. Ct. R. 13.1. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment to the United States Constitution provides:

> The 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.

U.S. Const. amend. IV.

STATEMENT OF THE CASE

On November 6, 2016, the petitioner, HENRY FRANKLIN REDDICK, was charged by indictment with four counts of possessing child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). ROA.16-19. On February 7, 2017, Mr. Reddick filed a motion to suppress evidence alleging the following. ROA.64-69.

Images that had been uploaded to and were located on Mr. Reddick's Microsoft SkyDrive online storage service were sent by Microsoft to the National Center for Missing and Exploited Children ("NCMEC") based on the belief that the hash values of the images indicated that they might contain child pornography. ROA.64-65. On March 10, 2015, NCMEC sent the images to Corpus Christi Police Department ("CCPD") Detective Michael Ilse, who received and opened the images on that same day. ROA.65. Based on his review of the images, on April 9, 2016, Detective Ilse obtained a warrant to search Mr. Reddick's residence and, on April 10, 2016, seized a number of items from the residence, including a laptop computer, a tower computer, CDs, and flash drives. ROA.264. The motion requested suppression of the evidence seized because Microsoft had not opened the images on Mr. Reddick's SkyDrive and because either NCMEC (as a government entity) or Detective Ilse had violated the Fourth Amendment by going beyond the scope of Microsoft's search by opening and viewing the images without a warrant or Mr. Reddick's consent. ROA.64-65.

On March 2, 2017, the district court held a hearing on the motion to suppress at which the government introduced the testimony of Detective Ilse and Kenneth E. Patterson,

a computer forensics specialist for the CCPD Internet Crimes Against Children Unit ("ICAC"). See ROA.291, 331. The evidence was as follows.

Detective Ilse works at the CCPD ICAC and investigates crimes involving child exploitation and the like. ROA.291-92. Microsoft SkyDrive, now called OneDrive, is an online cloud drive that can be used to store and backup data and images. ROA.294-95. Microsoft, like other electronic service providers ("ESPs"), uses PhotoDNA to monitor data and images uploaded to SkyDrive by comparing the hash values of the images with the hash values of images that have been determined by NCMEC to be child pornography. ROA.299-301.

According to Detective Ilse, PhotoDNA breaks images down to smaller sizes, grayscales them, analyzes them with an algorithm, and gives each image a hash value. ROA.300-01. According to Mr. Patterson, a hash value is a hexadecimal, which is a series of letters from A though F and a series of numbers from 0 through 9, and uses an algorithm that records the number of 0s and 1s in the digital image and their position. ROA.339-40. However, to compare the hash value of the unknown images to hash values of the images that have been determined to be child pornography, a human being must initially look at the so-called known images and make the judgment that they are child pornography. ROA.340-41.

If Microsoft determines that the hash value of an image matches the hash value of an image that NCMEC says is an image of child pornography, Microsoft will create a CyberTip and forward that image to NCMEC, but Microsoft does not open any files or view any images. ROA.301-02. Microsoft also forwards to NCMEC a hash value, an IP

address, and a provider address. ROA.302. NCMEC then determines what company the IP address belongs to. ROA.302. For example, in this case the IP address belonged to the provider Grande. ROA.302.

In the present case, Microsoft sent NCMEC a CyberTip on February 10, 2015, and two additional CyberTips on March 2, 2015. ROA.322. Detective Ilse received the CyberTips on March 10, 2015, after he was assigned to this case. ROA.323. In his testimony at the suppression hearing, Detective Ilse confirmed that no one at Microsoft or NCMEC had opened the images and looked at them. ROA.319; see also ROA.302, 319. In fact, the CyberTips themselves contained a notice stating the following: "Please be advised that NCMEC has not opened or viewed any uploaded files submitted with this report and has no information concerning the content of the uploaded files other than information provided in the report by the ESP." ROA.306 (internal quotation marks omitted).

On March 10, 2015, the same day that he received the three CyberTips, Detective Ilse opened them and all 79 images included with them and determined that the images were child pornography. ROA.323; see also ROA.303-08. Detective Ilse then used an administrative subpoena to Grande Communications for the IP address related to the images, learned that Mr. Reddick was the subscriber of the internet account, and learned the address of Mr. Reddick's residence from an investigation of public utility service records and Texas driver's license records. ROA.308-10. On April 9, 2015, Detective Ilse obtained a search warrant for Mr. Reddick's residence from a state district court judge. ROA.310-11.

At the suppression hearing in this case, Detective Ilse stated that he opens the files in a CyberTip "[t]o verify the suspected images are in fact child pornography" and that this

was "what I do as far as investigat[ing] cases involving child pornography" because he "need[ed] to determine if it is child pornography" and "an offense," and "to follow up with that investigation." ROA.320. At the hearing, Detective Ilse was asked the following question: "Do you ever generate a search warrant affidavit to search somebody's personal effects and house based solely on the hash values that you receive from NCMEC." Detective Ilse answered as follows: "I don't base it on hash values. I actually look at the image to determine if it's child pornography." ROA.320-21. In fact, Detective Ilse did not think any investigator on a similar case would do otherwise. ROA.329-30.

On April 10, 2015, Detective Ilse executed the search warrant for Mr. Reddick's residence. ROA.310-12. Mr. Reddick was present during the search, and, after being warned of his rights, denied possessing child pornography, but said that this must be related to a letter he had received from Microsoft stating that he had violated the terms of his service and blocking him from using Microsoft. ROA.312-13.

Following the suppression hearing, the court permitted the parties to submit additional briefing in which Mr. Reddick argued that the good faith exception did not apply in this case because Detective Ilse's initial search was unconstitutional and was based on his subjective belief that it was proper and relied on no rule, statute, precedent, or other objective factor. ROA.81-83. The district court issued an opinion denying the motion to suppress on April 13, 2017. ROA.91-104; see also United States v. Reddick, No. 2:16-CR-928, 2017 WL 1353803, at *8 (S.D. Tex. Apr. 13, 2017). The court "decline[d] to wade into the myriad of issues regarding Reddick's expectation of privacy" either because the record did not allow for that or because there was not sufficient case law from this Court

addressing such issues. ROA.99-100; see also Reddick, 2017 WL 1353803, at *5-*6. The district court thus "assume[d] without deciding that Officer Ilse's viewing of the file images (Phase I search)[ ] invaded a constitutional expectation of privacy, exceeded the scope of Microsoft Skydrive's hash value search, and did not fall into any exception to the warrant requirement." ROA.100; see also Reddick, 2017 WL 1353803, at *6.

The district court held that Detective Ilse's viewing of the images in the CyberTip was "close enough to the line of validity so as to warrant application of the good faith exception." ROA.102 (footnote, citation, and internal quotation marks omitted); see also Reddick, 2017 WL 1353803, at *7. The court relied on the unclear boundaries of electronic data privacy interests, the significance of the prior matching of hash values, and the fact that Detective Ilse's actions were detailed in the warrant application without any misleading or dishonest information. ROA.102-03; see also Reddick, 2017 WL 1353803, at *7.

On April 28, 2017, Mr. Reddick entered a conditional plea of guilty to the first count of the indictment pursuant to a plea agreement that expressly preserved his right to appeal the district court's denial of his motion to suppress and also provided, in relevant part, that the government would dismiss the remaining counts of the indictment. ROA.355-56, 362-65, 393; see also ROA.109-14 (plea agreement).

On October 19, 2017, the district court sentenced Mr. Reddick to serve 36 months in the custody of the Bureau of Prisons and to a 10-year term of supervised release. ROA.464. The court imposed a $100 special assessment, but did not impose a fine. ROA.464. The court granted the government's motion to dismiss the remaining counts of the indictment. ROA.466.

Mr. Reddick timely filed notice of appeal on October 26, 2017. ROA.148. In his opening brief, he argued that the district court's assumption that the Fourth Amendment had been violated was well founded in light of the opinions of this Court and the lower courts, but that the district court had erred by finding that the good faith exception, rather than the independent source doctrine, applied, that the independent source doctrine required reversal of the district court's ruling, and, in the alternative, that the district court had misapplied the good faith exception. App. Br. 13-41. In response, the government argued that the Fourth Amendment had not been violated because Microsoft had effectively opened the digital files by comparing hash values and that Detective Ilse thus had learned nothing new by actually opening them and viewing the images. Gov't Br. 21-38. The government alternatively argued that, assuming Detective Ilse had learned something new, the good faith exception applied. Gov't Br. 38-48.

Mr. Reddick's reply brief responded that Detective Ilse had violated the Fourth Amendment by opening and viewing the images and that the good faith exception did not apply in this case. Reply Br. 2-19. In his argument concerning the Fourth Amendment violation, he contended that Walter v. United States, 447 U.S. 649 (1980), as opposed to United States v. Jacobsen, 466 U.S. 109 (1984), applied because Microsoft was like the employees in Walter who had only viewed the labels on the film boxes, and Detective Ilse was like the FBI agents who had searched the contents of the films inside. Reply Br. 13-15. He also pointed out that the government's forensic computer expert admitted that a human being has to look at images and make judgments whether they are child pornography before they are included in the database of so-called known child

pornography, but "the government presented no witness from NCMEC on the process by which it is determined that database images are child pornography or the reliability or any other statistics concerning that determination, and defense counsel even provided the court with examples where federal agents and police officers had made a mistake by charging or accusing people with possessing child pornography." Reply Br. 16-17.

On August 17, 2018, the United States Court of Appeals for the Fifth Circuit affirmed Mr. Reddick's conviction. See United States v. Reddick, 900 F.3d 636 (5th Cir. 2018). The Fifth Circuit relied on the concept that, if "two identical files are inputted, . . . the hash function will generate identical output," id. at 637 (internal quotation marks and citation omitted), despite the fact that there was no evidence in the record showing what was in the database of so-called known child pornography or how the decision was made to include an image in it. Relying on the holding in United States v. Jacobsen, 466 U.S. 109 (1984), that the government's drug test of white powder found by Federal Express employees when a package had been torn "infringed no expectation of privacy that had not already been infringed," Reddick, 900 F.3d at 639, the Fifth Circuit held that, under the private search doctrine, Detective Ilse had not violated the Fourth Amendment because he "reviewed *only* those files whose hash values corresponded to the hash values of known child pornography images, as ascertained by the PhotoDNA program." Id. at 640. It thus affirmed the district court's denial of the motion to suppress on an alternative ground not addressed by the district court. See id. at 638, 640.

BASIS OF FEDERAL JURISDICTION IN THE UNITED STATES DISTRICT COURT

The district court had jurisdiction pursuant to 18 U.S.C. § 3231.

REASONS FOR GRANTING THE WRIT

I. As to the first and second questions presented, this Court should grant certiorari to address how the private search doctrine under the Fourth Amendment, as articulated in Walter v. United States, 447 U.S. 649 (1980), and United States v. Jacobsen, 466 U.S. 109 (1984), applies to searches of digital files using hash values, which is an important federal question that has not been, but should be, settled by the Court given the widespread use of this technology by federal, state, and local law enforcement.

A. Introduction.

In Riley v. California, 134 S. Ct. 2473 (2014), this Court recognized that stored digital data and images are protected by the Fourth Amendment. See id. at 2485 (holding that data stored on cell phones cannot be searched without a warrant). Almost a decade before that holding, however, it had become clear that "[h]ashing is a powerful and pervasive technique used in nearly every examination of seized digital equipment media" and that "hashing has become an important fixture in forensic examinations." Richard P. Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38, 38 (2005). The lower courts have entered a number of opinions addressing whether the use of hash values in searches of digital files violates the Fourth Amendment and some are contrary to others. Compare Reddick, 900 F.3d at 637-640 (holding that private match of hash values meant that officer's subsequent opening of digital images revealed nothing new and thus did not violate the Fourth Amendment), with United States v. Keith, 980 F. Supp. 2d 33, 43 (D. Mass. 2013) (holding that match of image's hash value with image in database only reveals that the two images are identical but conveys nothing about the provenance of the image in the database). And, in fact, an opinion written by Justice

Gorsuch when he was a Tenth Circuit Judge presaged the questions presented here. See United States v. Ackerman, 831 F.3d 1292, 1306 (10th Cir. 2016). Because this appeal presents two important questions that involve the nature and extent of the protections under Riley and the intersection of this Court's Fourth Amendment precedent with technology used by law enforcement across the country, it presents important questions of federal law that have not been, but should be, answered by the Court. This Court, therefore, should grant certiorari in this case.

B. This Court Should Grant Certiorari Because the United States Court of Appeals Has Decided Important Questions of Federal Law that Have Not Been, but Should Be, Settled by this Court.

As set out in more detail above,[1] the facts of this case are straightforward. Microsoft used a computer program to compare the hash values of digital files in Mr. Reddick's SkyDrive account to a database of images said to contain child pornography, and it found that some of the hash values matched. Microsoft then sent CyberTips with the digital files to NCMEC, which forwarded the Cybertips to Detective Ilse in Corpus Christi. No one at Microsoft or NCMEC opened the digital images before Detective Ilse received them. Detective Ilse opened the digital files and viewed the images in them without a warrant because, as he testified, he opens the files in a CyberTip "[t]o verify the suspected images are in fact child pornography," because "that's what [he] do[es] as far as investigat[ing] cases involving child pornography," and because he "need[s] to determine if it is child pornography" and "an offense." ROA.320. He confirmed that he never generates a search

[1] See supra text, at 3-7.

warrant affidavit based solely on the hash values he receives from NCMEC and that he did not think any investigator on a similar case would do otherwise. ROA.320-21, 329-30. Moreover, the government's forensic computer expert admitted at the suppression hearing that a human being has to look at images and make judgments whether they are child pornography before they are included in the database of so-called known child pornography. And, the government presented no witness on the process by which it is determined that database images are child pornography or the reliability or any other statistics concerning that determination. Defense counsel also provided the court with examples where federal agents and police officers had made a mistake by charging or accusing people with possessing child pornography.

On these facts, the Fifth Circuit relied on the concept that, if "two identical files are inputted, . . . the hash function will generate identical output," id. at 637 (internal quotation marks and citation omitted), despite the fact that there was no evidence in the record showing what was in NCMEC's database of so-called known child pornography or how the decision was made to include any particular image in it. The Fifth Circuit held that there was no violation of the Fourth Amendment because "Detective Ilse reviewed *only* those files whose hash values corresponded to the hash values of known child pornography images, as ascertained by the PhotoDNA program." Id. at 640 (italics in original). This appeal thus raises two important federal questions: (1) Does a police officer violate the Fourth Amendment by opening a digital file and viewing an image in it without a warrant to confirm a private company's statement that the image is child pornography based solely on the company's comparison of the hash value of the image and the hash value in a digital

database said to contain known child pornography when there is no evidence that the database actually contains images of child pornography, how the images in it were selected, or who selected them?; and (2) Does a police officer go beyond a private company's search, which merely compared the hash value of a digital file to hash values in a digital database said to contain known child pornography, by opening the file and viewing an image in it without a warrant to confirm that the image is child pornography?

The first question presented applies not only in the warrantless search context in the present case, but also in the context in which a law enforcement officer obtains a search warrant based upon a comparison of a digital file's hash value to a hash value in a database said to contain child pornography. See, e.g., United States v. Henderson, 595 F.3d 1198, 1202 (10th Cir. 2010) (holding that affidavit for search warrant was sufficient because it alleged that computer had downloaded videos with hash values associated with child pornography and contained the computer's IP address). Thus, whether the issue concerns probable cause to support a warrant or the application of the private search doctrine when an officer opens a file based on a private company's prior comparison of hash values, the crucial question is the provenance of the database to which a digital file's hash values are being compared:

> In this regard it is worth noting that matching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file. What the match says is that the two files are identical; it does not itself convey any information about the contents of the file. It does say that the suspect file is identical to a file that someone, sometime, identified as containing child pornography, but the provenance of that designation is unknown. So a match alone indicts a file as contraband but cannot alone

> convict it. That is surely why a CyberTipline analyst[2] opens the file to view it, because the actual viewing of the contents provides information additional to the information provided by the hash match. This is unlike what the Court found the case to be in Jacobsen, where the subsequent DEA search provided no more information than had already been exposed by the initial FedEx search. Jacobsen is inapposite.

Keith, 980 F. Supp. 2d at 43.

In fact, legal scholars have recognized that the provenance of the designation that a database contains child pornography is a critical question for Fourth Amendment jurisprudence as "[i]t is one thing to conclude that child pornography is contraband; it is quite another to conclude that a particular image to be included in a hash value set is child pornography." Richard P. Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38, 45-46 (2005). In other words, it is not a mechanical endeavor to determine whether an image fits the definition of child pornography:

> These issues are compounded further when considering a type of contraband like child pornography, which cannot be defined by any chemical formula. The forensic tools currently in existence use databases maintained by the NCMEC, a private organization. It is up to courts to determine whether a database of that kind is sufficient to guarantee that a purported image of child pornography is in fact contraband.
>
> These databases, however, may not always be perfect. If the set of known child pornography images contains files other than child pornography--in other words, if the known file set contains items that are not contraband--then the use of a hash runs the same risk as employing a dog that can detect the presence of both street drugs and Tylenol. An alert might indicate the presence of contraband, but it might also indicate some noncontraband file in which the owner of the drive has a right to privacy.

Ben Adams, What is Fourth Amendment Contraband?, 69 Stan. L. Rev. 1137, 1192-93 (2017).

---

[2] In Keith, a NCMEC CyberTip analyst opened the digital file to determine if it contained child pornography, just as Detective Ilse did in the present case. See Keith 980 F. Supp. 2d at 37.

This important issue is raised by this case because the Fifth Circuit was so impressed by the fact that the hash values of two digital files matched that it ignored the fact that the nature and provenance of what a digital file is being matched to is the critical question for the application of the private search doctrine in this context. See Reddick, 900 F.3d at 637, 640 (relying on match of hash values without even addressing the lack of evidence concerning the matching database). The import with regard to the application of the Fourth Amendment's private search doctrine is that an officer's viewing of the digital file reveals more to him than the referring private company knew because the evidence only shows that the private company knew that the hash value of the digital file matched an image in a digital database but not what the image in the database was or whether it was the kind of image it was purported to be.

In terms of this Court's case law, this means that Detective Ilse's opening and viewing of the digital files and images violated the Fourth Amendment because his actions went beyond the scope of the private search by the internet service provider, which consisted of a comparison of only the hash values of the digital files on Mr. Reddick's drive and the database provided by NCMEC. In other words, this Court's opinion in Walter v. United States, 447 U.S. 649 (1980), rather than its opinion in United States v. Jacobsen, 466 U.S. 109 (1984),[3] governs this case, and the evidence should have been suppressed.

---

[3] In Jacobsen, the Court held that there was no Fourth Amendment violation where Federal Express employees opened a damaged package, found a concealed tube that contained plastic bags of white powder, and notified federal agents who also removed the tube and the bags from the damaged package, removed a trace of the white substance from each bag, and discovered from a field test that the white powder was cocaine. See Jacobsen, 466 U.S. at 111-12. The Court noted that "privacy interests in the contents of the package had been largely compromised" because

The opinion in Walter involved a company employee who examined boxes that had labels indicative of explicit content and who opened some boxes and unsuccessfully attempted to view film inside of them by holding it up to the light. See Walter, 447 U.S. 651-52. Without a warrant, the FBI then viewed the films using a projector. See id. at 652. The Court held that the FBI's viewing of the films was unlawful because it exceeded the scope of the private search. See id. at 654-56.

The opinion in Walter described the crux of the decision in the following way:

> It is perfectly obvious that the agents' reason for viewing the films was to determine whether their owner was guilty of a federal offense. To be sure, the labels on the film boxes gave them probable cause to believe that the films were obscene and that their shipment in interstate commerce had offended the federal criminal code. But the labels were not sufficient to support a conviction and were not mentioned in the indictment. Further investigation—that is to say, a search of the contents of the films—was necessary in order to obtain the evidence which was to be used at trial.

Id. at 654.

Under Walter, the search in this case was illegal because the private parties had not viewed the contents of the "packages" in their possession and only had looked at the labels on them, which consisted of verbal labels and the hash values. And, as in Walter, "[i]t is perfectly obvious that the [investigator's] reason for viewing the [digital files and images] was to determine whether the owner was guilty of a federal offense." Id. Although the

---

"[t]he agents had already learned a great deal about the contents of the package from the Federal Express employees, all of which was consistent with what they could see." Jacobsen, 466 U.S. at 120. Moreover, "[t]he package itself, which had previously been opened, remained unsealed, and the Federal Express employees had invited the agents to examine its contents." Id. Since the distinctive character of the contents of the package was readily recognizable to the agents as contraband, the temporary seizure of the package and its contents by the agents was reasonable. Id. at 121-22.

labels and hash values might have given Detective Ilse probable cause to believe that the digital files were illegal, they "were not sufficient to support a conviction" and "[f]urther investigation—that is to say, a search of the contents of the [digital files]—was necessary in order to obtain the evidence which was to be used at trial." Id. And, Detective Ilse confirmed this exact point when he testified that he would never seek a search warrant based on the hash values alone and that no investigator in such a case as this would do so. ROA.320-21, 329-30. In other words, to proceed with a prosecution, just as the agents in Walter, he would need more evidence and that necessitated opening the digital files and looking at the images. See Walter, 447 U.S. at 654. Moreover, that the holding of Walter applies here is reinforced by the fact that the box in Jacobsen had been opened and the contents had been revealed, which allowed the agents to view the exact contents that the Federal Express employees had seen, and not just labels indicating the contents. That exposure of the actual contents of the "package" to law enforcement did not occur here especially because the private party compared only the hash values of files, where there was no evidence of who selected the images of the database that was being used for comparison or what criteria were used in that selection.

The previous discussion also encompasses the second question presented, which asks whether a police officer goes beyond a private company's comparison of the hash value of a digital file to hash values in a digital database said to contain known child pornography by opening the digital file and viewing an image in it without a warrant to confirm that the image is child pornography. As previously discussed, child pornography cannot be defined by any mechanical formula, and forensic tools use databases maintained

by the NCMEC, a private organization, and may not always be perfect and thus may contain images other than known child pornography. See supra text, at 16-17 (quoting Ben Adams, What is Fourth Amendment Contraband?, 69 Stan. L. Rev. 1137, 1192-93 (2017)). In other words, "unlike drug contraband, . . . no legislative body has declared particular images to be contraband, must less a blessed set of hash values," and "[i]t would seem that populating a hash set requires exercise of discretion that is not required when teaching a dog to detect cocaine or developing a chemical test to react to particular narcotics." Richard P. Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38, 46 (2005). This raises the question of whether a police officer who opens a digital file and views an image discovers information beyond what a private company has learned by a comparison of hash values.

And the answer to that question is "yes" because the officer actually confirms whether the image in the file is in fact child pornography. Indeed, Detective Ilse's candor in this regard is striking as he flatly stated that he opened the digital files and viewed the images in them without a warrant "[t]o verify the suspected images are in fact child pornography," and that this was "what I do as far as investigat[ing] cases involving child pornography" because he "need[ed] to determine if it is child pornography" and "an offense," and "to follow up with that investigation." ROA.320. He also confirmed that he never generates a search warrant affidavit based solely on the hash values he receives from NCMEC and that he did not think any investigator on a similar case would do otherwise. ROA.320-21, 329-30. Given the unknown provenance of the images in the database said to be child pornography, a private company may have suspicions raised that a digital file

contains child pornography, but an officer can only know that by opening the file and looking at it. See, e.g., Walter, 447 U.S. at 654.

In sum, because this appeal raises two an important federal questions that have not been, but should be, settled by this Court, this Court should grant certiorari.

II. As to the third question presented, this Court should grant certiorari to decide whether the holding in United States v. Jacobsen, 466 U.S. 109, 123-25 (1984) – that it was not a search for the government to field test white powder revealed to private employees when a package was damaged – has been abrogated by the property rights analysis of the Fourth Amendment in United States v. Jones, 565 U.S. 400 (2012). See United States v. Ackerman, 831 F.3d 1292, 1307 (10th Cir. 2016) (per Gorsuch, J.).

In the Fifth Circuit, Mr. Reddick argued that this Court's opinion in Walter v. United States, 447 U.S. 649 (1980), rather than its opinion in United States v. Jacobsen, 466 U.S. 109 (1984), governed this case. See Reply Br. 12-15. In his discussion of Walter and Jacobsen, Mr. Reddick warned the Fifth Circuit that the viability of Jacobsen's holding that the field test of the cocaine did not violate the Fourth Amendment was suspect following this Court's decision in Florida v. Jardines, 569 U.S. 1, 10-11 (2013). See Reply Br. 13 n.2, He pointed out that this portion of Jacobsen relied heavily on the holding of United States v. Place, 462 U.S. 696 (1983), see Reply Br. 13 n.2 (citing Jacobsen, 466 U.S. at 123-26), and that Jardines had noted, but declined to reconsider, the expectation-of-privacy issue as determined by Place, choosing instead to rely on the property-rights prong of the Fourth Amendment. See Reply Br. 13 n.2 (citing Jardines, 569 U.S. at 10-11).

The Fifth Circuit paid no attention to this warning, however, and instead emphasized that Jacobsen had held that the government's drug test of white powder found by Federal Express employees when a package had been torn "infringed no expectation of privacy that had not already been infringed," Reddick, 900 F.3d at 639. Relying on Jacobsen's holding, the Fifth Circuit concluded that, under the private search doctrine, Detective Ilse had not violated the Fourth Amendment because he "reviewed *only* those files whose hash values

corresponded to the hash values of known child pornography images, as ascertained by the PhotoDNA program." Id. at 640.

As pointed out by Justice Gorsuch in an opinion he wrote when he was a Tenth Circuit Judge, this Court's case law issued subsequent to Jacobsen, including United States v. Jones, 565 U.S. 400 (2012), calls into question whether this holding of Jacobsen is still good law:

> Our conclusion about this is confirmed by yet another and distinct line of authority. Jacobsen said no "search" implicating the Fourth Amendment took place even when officers exceeded the scope of the search previously performed by the private party and removed and destroyed a small amount of powder to conduct a drug test. In doing so, Jacobsen invoked Katz[4] and held there was no "reasonable expectation of privacy" in concealing whether something is or isn't contraband. See 466 U.S. at 122–23. But after United States v. Jones, [565] U.S. [400], 132 S. Ct. 945 (2012), there's reason to wonder about that conclusion. After all, Jones held that the Katz formula is but one way to determine if a constitutionally qualifying "search" has taken place. Id. at 949–51. In light of the Fourth Amendment's original meaning, Jones explained that government conduct can constitute a Fourth Amendment search either when it infringes on a reasonable expectation of privacy or when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing ("persons, houses, papers, and effects") for the purpose of obtaining information. So the fact the government's conduct doesn't trigger Katz doesn't mean it doesn't trigger the Fourth Amendment. Id. at 950 ("Fourth Amendment rights do not rise or fall with the Katz formulation. . . . [F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas . . . it enumerates. Katz did not repudiate that understanding.").
>
> Reexamining the facts of Jacobsen in light of Jones, it seems at least possible the Court today would find that a "search" did take place there. After all, the DEA agent who performed the drug test in Jacobsen took and destroyed a "trace amount" of private property, 466 U.S. at 125, a seeming trespass to chattels. Neither is there any question that the purpose and effect of the agent's action was to obtain information. See id. at 122–23. And while

[4] Katz v. United States, 389 U.S. 347 (1967).

> the destruction of only a "trace amount" of private property might not amount to a trespass under modern tort law, even less was required to establish a claim of trespass to chattels at the time of the founding—and we know the Fourth Amendment is no less protective of persons and property against governmental invasions than the common law was at the time of the founding. Jones, 132 S. Ct. at 950, 953; id. at 957 n.2 (Alito, J., concurring in the judgment) ("At common law, a suit for trespass to chattels could be maintained if there was a violation of 'the dignitary interest in the inviolability of chattels,' but today there must be 'some actual damage to the chattel before the action can be maintained.' " (quoting W. Keeton et al., Prosser & Keeton on Law of Torts § 14, at 87 (5th ed. 1984))).

United States v. Ackerman, 831 F.3d 1292, 1307 (10th Cir. 2016) (parallel citations omitted).

Whether this portion of Jacobsen remains good law following this Court's property rights analysis of the Fourth Amendment in Jones is of the utmost importance in this case and in similar cases. Based on Jacobsen's privacy analysis, the Fifth Circuit held that Detective Ilse did not violate the Fourth Amendment by opening the digital files that belonged to Mr. Reddick. However, it never considered whether opening the digital files violated Mr. Reddick's property rights under the Fourth Amendment. And, given the widespread use by law enforcement of hash values to justify opening and viewing digital files, see supra text, at 12, whether this holding of Jacobsen remains good law is an important Fourth Amendment question, that has not been, but should be addressed by this Court. This Court, therefore, should grant certiorari in this case.

CONCLUSION

For the foregoing reasons, petitioner Henry Franklin Reddick prays that this Court grant certiorari to review the judgment of the Fifth Circuit in his case.

Date: November 14, 2018

Respectfully submitted,

MARJORIE A. MEYERS
Federal Public Defender
Southern District of Texas
Attorney of Record

By H. Michael Sokolow
H. MICHAEL SOKOLOW
First Assistant Federal Public Defender
Attorneys for Petitioner
440 Louisiana Street, Suite 1350
Houston, Texas 77002-1056
Telephone: (713) 718-4600

900 F.3d 636
United States Court of Appeals, Fifth Circuit.

UNITED STATES of America, Plaintiff-Appellee
v.
Henry Franklin REDDICK, Defendant-Appellant

No. 17-41116
|
August 17, 2018

Synopsis

Background: Following the denial of his suppression motion, 2017 WL 1353803, defendant was convicted on a conditional guilty plea in the United States District Court for the Southern District of Texas, Nelva Gonzales Ramos, J., of possession of child pornography. Defendant appealed.

[Holding:] The Court of Appeals, James C. Ho, Circuit Judge, held that as a matter of first impression, police detective did not violate defendant's Fourth Amendment rights by reviewing image files that had been flagged by private hosting service as matching known child pornography files.

Affirmed.

West Headnotes (4)

[1] **Criminal Law**
Theory and Grounds of Decision in Lower Court

As a general rule, the Court of Appeals may affirm the district court's ruling on a motion to suppress based on any rationale supported by the record.

Cases that cite this headnote

[2] **Searches and Seizures**
Private persons

Under the private search doctrine, 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. U.S. Const. Amend. 4.

Cases that cite this headnote

[3] **Searches and Seizures**
Private persons

Under the private search doctrine, once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information. U.S. Const. Amend. 4.

Cases that cite this headnote

[4] **Searches and Seizures**
Carriers and communication companies

Under the private search doctrine, police detective did not violate defendant's Fourth Amendment rights by reviewing digital image files uploaded by defendant to cloud hosting service, which alerted law enforcement that the hash values of the files corresponded to hash values of known child pornography images; whatever expectation of privacy defendant might have had in the hash values of his files was frustrated by service's private search, detective's visual review of the files merely dispelled any residual doubt about contents of files, and there was no indication that detective searched any of defendant's files other than those flagged as child pornography. U.S. Const. Amend. 4.

Cases that cite this headnote

Appeal from the United States District Court for the Southern District of Texas

Attorneys and Law Firms

Andrew R. Gould, Assistant U.S. Attorney, Carmen Castillo Mitchell, Assistant U.S. Attorney, U.S. Attorney's Office, Houston, TX, for Plaintiff-Appellee.

Marjorie A. Meyers, Federal Public Defender, H. Michael Sokolow, Assistant Federal Public Defender, Federal Public Defender's Office, Houston, TX, for Defendant-Appellant.

Before KING, SOUTHWICK, and HO, Circuit Judges.

Opinion

JAMES C. HO, Circuit Judge:

Private businesses and police investigators rely regularly on "hash values" to fight the online distribution of child pornography. Hash values are short, distinctive identifiers that enable computer users to quickly compare the contents of one file to another. They allow investigators to identify suspect material from enormous ***637** masses of online data, through the use of specialized software programs—and to do so rapidly and automatically, without the need for human searchers.

Hash values have thus become a powerful tool for combating the online distribution of unlawful aberrant content. The question in this appeal is whether and when the use of hash values by law enforcement is consistent with the Fourth Amendment. For the Fourth Amendment concerns not efficiency, but the liberty of the people "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." There is no precedent in our circuit concerning the validity of these investigative tools under the Fourth Amendment, and to our knowledge no other circuit has confronted the precise question before us. This case therefore presents an opportunity to apply established Fourth Amendment principles in this new context.

One touchstone of our Fourth Amendment jurisprudence is that the Constitution secures the right of the people against unreasonable searches and seizures conducted by the government—not searches and seizures conducted by private parties. Under the private search doctrine, 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.

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 effect an intrusion on Mr. Reddick's privacy that he did not already experience as a result of the private search. Accordingly, we affirm the judgment of the district court.

I.

In technical terms, a hash value is "an algorithmic calculation that yields an alphanumeric value for a file." *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013). More simply, a hash value is a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file's contents. In the words of one commentator, "[t]he 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." Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38 (2005).

Hash values are regularly used to compare the contents of two files against each other. "If two nonidentical files are inputted into the hash program, the computer will output different results. If the two identical files are inputted, however, the hash function will generate identical output." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 541 (2005). Hash values have been used to fight child pornography distribution, by comparing the hash values of suspect files against a list of the hash values of known child pornography images currently in circulation. This process allows potential child pornography images to be identified rapidly, without the need to involve human investigators at every stage.

II.

Henry Reddick uploaded digital image files to Microsoft SkyDrive, a cloud hosting service. SkyDrive uses a program called PhotoDNA to automatically scan the *638 hash values of user-uploaded files and compare them against the hash values of known images of child pornography. When PhotoDNA detects a match between the hash value of a user-uploaded file and a known child pornography hash value, it creates a "CyberTip" and sends the file—along with the uploader's IP address information—to the National Center for Missing and Exploited Children (NCMEC).

In early 2015, Microsoft sent CyberTips to NCMEC based on the hash values of files that Reddick had uploaded to SkyDrive. Based on location data derived from the IP address information accompanying the files, NCMEC subsequently forwarded the CyberTips to the Corpus Christi Police Department. Upon receiving the CyberTips, police detective Michael Ilse opened each of the suspect files and confirmed that each contained child pornography. Shortly thereafter, Detective Ilse applied for and received a warrant to search Reddick's home and seize his computer and related materials. This search uncovered additional evidence of child pornography in Reddick's possession.

Reddick was indicted for possession of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). Following his indictment, Reddick initially pled not guilty and moved to suppress all the evidence of child pornography. He alleged that Detective Ilse's warrantless opening of the files associated with the CyberTips was an unlawful search. He further claimed that any evidence of child pornography found in his home should be suppressed under the exclusionary rule, since the initial review of the suspect files was improper.

The district court denied his motion. Reddick subsequently pled guilty, while retaining the right to appeal the denial of his suppression motion. In denying Reddick's motion, the district court "assume[d] without deciding that Officer Ilse's viewing of the file images ... invaded a constitutional expectation of privacy, exceeded the scope of Microsoft Skydrive's hash value search, and did not fall into any exception to the warrant requirement." The court nevertheless concluded that "the evidence here support[ed] the good faith exception to the exclusionary rule." Accordingly, the court found no justification to suppress the evidence of child pornography found in Reddick's home.

[1] As a general rule, "[w]e may affirm the district court's ruling on a motion to suppress 'based on any rationale supported by the record.' " *United States v. Wise*, 877 F.3d 209, 215 (5th Cir. 2017) (citation omitted). Consistent with this rule, we affirm the denial of the motion to suppress on a ground broader than the one invoked by the district court—namely, that under the private search doctrine, Officer Ilse's viewing of the file images did not violate the Fourth Amendment.

III.

[2] Under the private search doctrine, "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." *United States v. Runyan*, 275 F.3d 449, 461 (5th Cir. 2001). The question presented here, then, is whether, by the time Detective Ilse viewed the suspect image files, Reddick's expectation of privacy in his computer files had already been thwarted by a private third party. [1]

*639 The Supreme Court's decision in *United States v. Jacobsen*, 466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984), guides our analysis. In *Jacobsen*, employees of Federal Express observed that one of its packages had been damaged in transit. They opened the package and discovered a white powder. In response, the employees contacted the Drug Enforcement Administration. DEA agents conducted chemical field tests on the white powder and determined that the power was cocaine. The government then used the test results to obtain a warrant and arrest the package's intended recipients, who subsequently challenged the government's actions as unconstitutional.

[3] The Court held that the agents' actions did not violate the Fourth Amendment. "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id.* at 117, 104 S.Ct. 1652. Any expectation of privacy the recipients might have

had in the package's contents was abrogated when the Federal Express employees opened and searched the package and discovered the white powder. The government's subsequent use of that information—its test to discern the powder's chemical composition—infringed no expectation of privacy that had not already been infringed.

[4] So too here. When Reddick uploaded files to SkyDrive, Microsoft's PhotoDNA program automatically reviewed the hash values of those files and compared them against an existing database of known child pornography hash values. In other words, his "package" (that is, his set of computer files) was inspected and deemed suspicious by a private actor. Accordingly, whatever expectation of privacy Reddick might have had in the hash values of his files was frustrated by Microsoft's private search.

When Detective Ilse first received Reddick's files, he already knew that their hash values matched the hash values of child pornography images known to NCMEC. As our court has previously noted, hash value comparison "allows law enforcement to identify child pornography with almost absolute certainty," since hash values are "specific to the makeup of a particular image's data." *United States v. Larman*, 547 F. App'x 475, 477 (5th Cir. 2013) (unpublished). *See also United States v. Sosa-Pintor*, —— Fed.Appx. ——, ——, 2018 WL 3409657, at *1 (5th Cir. July 11, 2018) (unpublished) (describing a file's hash value as its "unique digital fingerprint").

Accordingly, when Detective Ilse opened the files, there was no "significant expansion of the search that had been conducted previously by a private party" sufficient to constitute "a separate search." *Walter v. United States*, 447 U.S. 649, 657, 100 S.Ct. 2395, 65 L.Ed.2d 410 (1980). His visual review of the suspect images—a step which merely dispelled any residual doubt about the contents of the files—was akin to the government agents' decision to conduct chemical tests on the white powder in *Jacobsen*. "A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy." 466 U.S. at 123, 104 S.Ct. 1652. This principle readily applies here—opening the file merely confirmed that the flagged file was indeed child pornography, as suspected. As in *Jacobsen*, "the suspicious nature of the material made it virtually certain that the substance tested was in fact contraband." *Id.* at 125, 104 S.Ct. 1652.

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. Contrast a Tenth Circuit decision authored by then ***640** Judge Gorsuch. *See United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016). In *Ackerman*, an investigator conducted a search of an email and three attachments whose hash values did *not* correspond to known child pornography images. 831 F.3d at 1306. The Tenth Circuit reversed the district court's denial of a motion to suppress accordingly. *Id.* at 1309. Here, by contrast, Detective Ilse reviewed *only* those files whose hash values corresponded to the hash values of known child pornography images, as ascertained by the PhotoDNA program. So his review did not sweep in any "(presumptively) private correspondence that could have contained much besides potential contraband." *Id.* at 1307.

* * *

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. We affirm the judgment of the district court.

All Citations

900 F.3d 636

Footnotes

1 We assume without deciding that Reddick indeed had a legitimate expectation of privacy in the computer files at issue. As the district court correctly noted, "the most useful evidence on which to make the determination" of whether Reddick's expectation of privacy was reasonable—"the end user agreement governing Reddick's use of Microsoft Skydrive"—is not in the record.

End of Document

2017 WL 1353803
Only the Westlaw citation is currently available.
United States District Court, S.D.
Texas, Corpus Christi Division.

UNITED STATES of America
v.
Henry Franklin REDDICK

CRIMINAL ACTION NO. 2:16-CR-928
|
Signed 04/13/2017

Attorneys and Law Firms

Hugo Ricardo Martinez, United States Attorneys Office, Corpus Christi, TX, Financial Litigation, U.S. Attorney's Office, Houston, TX, for United States of America.

ORDER ON MOTION TO SUPPRESS

NELVA GONZALES RAMOS, UNITED STATES DISTRICT JUDGE

***1** Defendant Henry Franklin Reddick (Reddick) is charged by indictment with four counts of possession of child pornography. D.E. 1. Before the Court is his motion to suppress evidence (D.E. 34). First, he seeks to exclude all of the alleged images of child pornography that a private party referred—in unopened electronic files—to law enforcement. His reasoning is that the officer engaged in a search beyond the scope of the private party's investigation by opening and viewing the contents of those electronic files without a warrant (Phase I search). Second, he seeks to exclude all evidence found in his home and on his computer because the search warrant used to search his property (Phase II search) was based, in part, on the information gleaned from the initial warrantless viewing.

The Government argues that it did not engage in an unreasonable search and seizure because its Phase I search did not exceed the scope of the private investigation and referral. Alternatively, the Government argues that if it exceeded the scope of the private search, the good faith exception to the exclusionary rule permits admission of the evidence the officers found when executing what they believed was a valid search warrant. D.E. 36, 41. Reddick responds that the Phase I search exceeded the scope of any private search and the officer's conduct in securing the Phase II search warrant takes it outside the good faith exception to the exclusionary rule. D.E. 40.[1] For the reasons set out below, the Court DENIES the motion to suppress.

FACTS

PhotoDNA is a software program using an algorithm by which still and video digital images are converted to grayscale, broken down into grids of data, and assigned certain alphanumeric values associated with the hue gradient of the target material, arriving at what is called a "hash value." The hash value has been described as an electronic equivalent of a fingerprint[2] in that two iterations of the same image will, to an over 99% level of accuracy, produce the same hash value.[3] Conversely, the chances of two different images generating the same hash value is nearly non-existent.

***2** Some of the advantages to using the PhotoDNA software include the ability to scan large numbers of electronic files for their hash values in very little time, and doing so without exposing the images to viewers. The software thus ferrets out child pornography and protects children from additional exploitation. While hash values are useful and reliable for identifying matches to known images, one cannot recreate an image or determine its content solely from its hash value. Therefore, 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. The high likelihood that it is contraband stems from the integrity of the database of offending hash values used to test for matches.

With the imprimatur of the federal government,[4] the National Center for Missing and Exploited Children (NCMEC) established a database containing the hash values of known images that contain confirmed or suspected child pornography. There are multiple contributors to the database and, on this record, it is uncertain what criteria govern and whose judgment is used when a particular hash value result is included in the NCMEC database. And, because the original images from which offending hash values were generated are destroyed,

there is no readily available matching image to view to confirm the illegal nature of a matched hash value image.

Reddick submits that the judgment call used to populate the NCMEC database may lead to adult pornography being submitted erroneously as child pornography or there may be contributions that cause other false positives in searching for contraband. D.E. 40, p. 2 n.1 (citing a New York Post article regarding one such misidentification of an adult as a child). However, there is no evidence that such over-inclusiveness has occurred in the NCMEC database or is widespread, impugning the overall integrity of the database. Instead, law enforcement regularly relies on a hash value match with the NCMEC database results to successfully identify images that are, indeed, images of child pornography.

Many internet service providers, desiring to avoid any reputation for aiding those who possess or transmit child pornography, use PhotoDNA to scan files that customers upload through the service providers' browsers, applications, or cloud storage facilities. They then compare the hash value results with the hash values in the NCMEC database. When they get a match, they refer the files, along with subscriber information, to NCMEC as required by law. NCMEC, without opening the electronic file, generates a report and conducts an initial investigation, limited to confirming the hash value match and identifying the location of the internet user whose equipment uploaded the matching file. NCMEC then forwards the report (CyberTipline report) to the appropriate law enforcement agency with geographic jurisdiction over the internet user for further investigation.

Reddick made use of software systems that stored his electronic files in a cloud maintained by Microsoft Corporation and referred to as Skydrive. At the suppression hearing, Reddick did not offer evidence of any terms on which his files were so maintained. The Government offered the standard end user agreement of Microsoft OneDrive for that purpose. While OneDrive is the current electronic system formerly referred to as Skydrive, the Government's witnesses could not testify that the current OneDrive agreement stated the same terms that were in place when the events of this case transpired—during the Skydrive period. The Court therefore excluded the OneDrive agreement from evidence. While the Government's witnesses then testified that there is a standard in the industry by which privacy rights are waived in cloud storage agreements, permitting PhotoDNA scans and law enforcement referrals, they were not able to opine that the specific agreement governing Reddick's account met that standard.

*3 At any rate, Microsoft Skydrive conducted a hash value examination of electronic files on its system, including those related to Reddick. Several of Reddick's files generated hash values that matched hash values in the NCMEC database. As required by law, Microsoft Skydrive copied the electronic files and referred them to NCMEC, along with Reddick's subscriber information and other metadata that identified when and how the files were uploaded. NCMEC determined that Reddick was within the jurisdiction of Corpus Christi, Texas.

On March 10, 2015, the Corpus Christi Police Department (CCPD) Organized Crime Unit–Internet Crimes Against Children (ICAC) Task Force received three CyberTipline reports from NCMEC, containing 13, 50, and 16 electronic files, respectively. The NCMEC transmission of the files to CCPD-ICAC included the assertion that the files had been hash value matched, but had not been opened or viewed. Officer Michael Ilse, a CCPD-ICAC member, received the reports and opened and viewed the contents of the files (Phase I search) to confirm that the images depicted child pornography. He testified that he always visually confirms that the files contain child pornography before seeking a search warrant and that this is the established practice of all detectives he knows who investigate these crimes.

Officer Ilse then submitted an affidavit with a request for a search warrant to search and seize Reddick's computer and related materials (Phase II search). In his affidavit, among other things, he recounts the NCMEC CyberTipline reports, describes the matching of hash values, lists some of the file names, [5] and recites that he opened and viewed the files, stating why they appear to contain child pornography. A state district judge issued the warrant on April 9, 2015. CCPD searched Reddick's residence, including several digital devices, and found evidence of child pornography, including 456 still images and 13 videos. Nine of those files matched those transmitted to CCPD in the NCMEC CyberTipline reports. Reddick was later arrested on November 10, 2016.

DISCUSSION

A. Burden of Proof

Reddick asserts that Officer Ilse's review of the files uploaded to Skydrive (Phase I search) was a warrantless search in violation of the Fourth Amendment. And because the subsequent Phase II search was conducted pursuant to a warrant that was based on information accessed through the Phase I warrantless search, the evidence obtained is fruit of the poisonous tree. Accordingly, all evidence obtained as a result of the Phase I warrantless search of the files uploaded to Skydrive must be suppressed. D.E. 34, p. 2.

Unconstitutional Search. It is the defendant's burden to prove a Fourth Amendment violation by a preponderance of the evidence. *United States v. Riazco*, 91 F.3d 752, 754 (5th Cir. 1996). To show a Fourth Amendment violation, a defendant must first establish that the search invaded a legitimate expectation of privacy that society recognizes as reasonable. *See generally, Minnesota v. Olson*, 495 U.S. 91, 95-96 (1990) (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)). Whether the search was a reasonable intrusion into that privacy interest depends on whether the government acted pursuant to a warrant. A warrantless search is presumed unreasonable and shifts the burden of proof to the government to establish an exception to the warrant requirement. *United States v. Castro*, 166 F.3d 728, 733 n. 7 (5th Cir. 1999) (en banc); *United States v. Waldrop*, 404 F.3d 365, 368 (5th Cir. 2005). Such exceptions include special law enforcement needs, exigent circumstances, diminished expectations of privacy, and minimal intrusions. *See generally, Illinois v. McArthur*, 531 U.S. 326, 330 (2001).

***4 Exclusionary Rule**. If the evidence supports a finding of an unconstitutional search, there is a presumption that the resulting evidence should be excluded from the trial. Thus, the burden is on the government to demonstrate why the exclusionary rule should not apply to the fruits of the illegal search or seizure. *United States v. Houltin*, 566 F.2d 1027, 1031 (5th Cir. 1978). *See also, United States v. Runyan*, 275 F.3d 449, 456 (5th Cir. 2001). One such reason is that the search was conducted in good faith reliance on a warrant thought to be valid. *United States v. Leon*, 468 U.S. 897, 926 (1984).

B. On this Record, the Court Assumes an Unlawful Search

According to the Fifth Circuit, the relevant factors for a determination of a reasonable expectation of privacy are: (1) whether the defendant has a property or possessory interest in the thing seized or the place searched; (2) whether he has the right to exclude others from the place; (3) whether he has exhibited a subjective expectation of privacy that it would remain free from governmental intrusion; (4) whether he took normal precautions to maintain privacy; and (5) whether he was legitimately on the premises. *United States v. Runyan*, 275 F.3d 449, 457 (2001) (*quoting United States v. Cardoza-Hinojosa*, 140 F.3d 610, 615 (5th Cir. 1998)). "[T]he *Cardoza-Hinojosa* factors, 'while appropriate to determine the expectation of privacy in the context of searches of physical real property,' cannot necessarily be applied to other types of searches without modification." *Id.* (*quoting Kee v. City of Rowlett, Texas*, 247 F.3d 206, 212-13 (5th Cir. 2001)).

The expectation of privacy in this digital age is fraught with varying levels of confidence in the ability to protect electronic data as well as specialized needs to monitor data systems for electronic viruses, hacking attempts, phishing efforts, malware, illegal content, international security, and other threats. One's expectation of privacy is no easy issue in the abstract and the parties have deprived the Court of the most useful evidence on which to make the determination in this case—the end user agreement governing Reddick's use of Microsoft Skydrive. That agreement, by which the user's electronic data is stored on a private system, ordinarily specifies who may access the data, how that data may be accessed, and for what purposes. Only with that information could the Court reliably begin to address whether Reddick had a constitutional expectation of privacy or had waived any such expectation by contractually permitting searches for contraband images.

The privacy issue, while starting with an end user agreement, would not necessarily end there. The Court would have to make other technology-specific determinations involving undeveloped facts and law with respect to the issues of the scope of the private search, the significance of the algorithmic "view" of the file, and any remaining expectation of privacy after a NCMEC database match is discovered. For instance:

- Is an electronic file already searched if its contents are invaded for the purpose of determining its hash value? [6]

- Does law enforcement gain any material information it did not already know by opening an electronic file that has already been hashed and matched? [7]

- Is the slight possibility that viewing the file will expose an image that is not contraband within social tolerances?

- Is viewing a file a new search when an exact copy of the file was opened by someone else and reported to NCMEC as child pornography, causing its hash value to be added to the NCMEC database? [8]

*5 • Would it make a difference if the government used the hash value only for purposes of matching and viewed only a separate copy of the matched image that had been stored or was located elsewhere outside of the defendant's possession?

- Is the NCMEC database of hash values sufficiently reliable to equate a match with a contraband image?

- If there is no constitutional expectation of privacy in contraband, does opening an isolated electronic file implicate anything more than what the hash value has indicated to be contraband, akin to a field test of controlled substances? [9]

There are cases that have addressed some of these issues, but they are not all consistent. And the Fifth Circuit has not yet issued opinions to provide this Court with guidance regarding these very specific technology-and policy-intense matters.

*6 As will be demonstrated below, the evidence here supports the good faith exception to the exclusionary rule. For this reason, the Court declines to wade into the myriad of issues regarding Reddick's expectation of privacy. The Court will assume without deciding that Officer Ilse's viewing of the file images (Phase I search) invaded a constitutional expectation of privacy, exceeded the scope of Microsoft Skydrive's hash value search, and did not fall into any exception to the warrant requirement.

C. The Good Faith Exception to the Exclusionary Rule Applies

The exclusionary rule is a remedy imposed to protect the Fourth Amendment by suppressing evidence obtained through an illegal search. (*United States v. Leon*, 468 U.S. 897, 906 (1984)). The derivative evidence rule, also known as the fruit of the poisonous tree doctrine, further requires suppression of evidence that is discovered as an indirect result of police misconduct. *United States v. Tedford*, 875 F.2d 446, 450 (5th Cir. 1989). There are four recognized exceptions [10] to these rules. The Government relies only upon the good faith exception, allowing admission of evidence obtained in good faith reliance upon a warrant that is found invalid after its execution.

In *Leon*, the Court reasoned that excluding evidence when law enforcement acted in good faith on a warrant would not further the purpose of the exclusionary rule: to deter unconstitutional conduct. "Penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of the Fourth Amendment violations." *Leon*, 468 U.S. at 921. Thus, "In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause." [11] *Id.* at 926. "[T]he analysis 'is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization.' " *United States v. Massi*, 761 F.3d 512, 530 (5th Cir. 2014) (citing *United States v. Payne*, 341 F.3d 393, 400 (5th Cir. 2003)).

*7 Reddick argues that the good faith exception does not apply because Officer Ilse knew or should have known that his Phase I search was illegal and he only perpetuated his illegal conduct by securing a Phase II search warrant based on that illegal Phase I search. The Fifth Circuit has resolved that issue in favor of law enforcement, making the test whether the illegal search was a close call: "the prior law enforcement conduct that uncovered evidence used in the affidavit for the warrant must be 'close enough to the line of validity' that an objectively reasonable officer preparing the affidavit or executing the warrant would believe that the information supporting the warrant was not tainted by unconstitutional conduct...." *Massi*, at 528. [12]

The Fifth Circuit has not had many opportunities to explain what sort of conduct is "close enough to the line of validity" so as to warrant application of the good faith exception. [13] However, given the issues in this case, the Court finds that Officer Ilse's search qualifies. As apparent from the discussion above, the Phase I search issues involve unclear boundaries on electronic data privacy interests and the significance of the prior—private—hash value invasion of files and NCMEC database matching. And this record reflects the near certainty that the electronic files were each single images that qualified as child pornography: contraband and nothing more.

Most telling on the issue of good faith is the fact that, in his affidavit seeking a search warrant, 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. Had it not been, he would have reason to expect that the judge issuing the search warrant would tell him and refuse to issue the Phase II search warrant.

The Court finds that Officer Ilse's reliance on the warrant was objectively reasonable. There was nothing in the warrant or otherwise known by him that would have made an objectively reasonable officer doubt the warrant's validity. Furthermore, there is no evidence in the record to indicate that any of the disqualifying scenarios, involving dishonest or misleading police conduct or the magistrate judge's abandonment of his or her role as independent arbiter are applicable to this case. Indeed, the NCMEC match and file names, without viewing the images, might establish sufficient probable cause to support the validity of the warrant. *See United States v. Cartier*, 543 F.3d at 446 (stating that a hash value match from a reliable source could support the issuance of a warrant under the totality of the circumstances). Thus, the good faith exception applies.

CONCLUSION

***8** Assuming without deciding that there was an unconstitutional Phase I search and that the resulting search warrant was infirm, the Court finds that the Phase II search was accomplished in good faith reliance on a warrant with apparent validity. Suppressing the evidence would not further the purposes of the exclusionary rule. Accordingly, Reddick's motion to suppress (D.E. 34) is DENIED.

ORDERED this 13th day of April, 2017.

All Citations

Not Reported in Fed. Supp., 2017 WL 1353803

Footnotes

1 Reddick also argues that there were no exigent circumstances to support a warrantless search. The Government does not rely on any exigent circumstances exception to the warrant requirement, making this issue moot.

2 *United States v. Chiaradio*, 684 F.3d 265, 271 (1st Cir. 2012). *See also United States v. Farlow*, 681 F.3d 15, 19 (1st Cir. 2012); *United States v. Cunningham*, 694 F.3d 372, 376 n.3 (3rd Cir. 2012); *United States v. Miknevich*, 638 F.3d 178, 181 n.1 (3rd Cir. 2011); *United States v. Richardson*, 607 F.3d 357, 363 (4th Cir. 2010); *United States v. Dodson*, 960 F.Supp.2d 689, 692 n.1 (W.D. Tex. 2013).

3 *See generally*, *United States v. Glassgow*, 682 F.3d 1107, 1110 (8th Cir. 2012). *See also United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008) (in challenge to probable cause supporting search warrant, rejecting argument "that it is possible for two digital files to have hash values that collide or overlap").

4 The Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701 et seq., created rules to guarantee electronic privacy. In its Title II, the Stored Communications Act (SCA), Congress prescribed the circumstances under which the government may compel disclosure or when service providers may voluntarily disclose a customer's communications or records. Under that statute, a provider must report apparent child pornography to NCMEC via its Cyber Tipline if the provider becomes aware of it. 18 U.S.C. § 2258A.

5 Along with some file names that are simply alphanumeric strings, there were files labeled: sucking mandick.jpg, very yb and dad.jpg, boy sucking boydick.jpg, boydick and mancock.jpg, boy.kiddy.pedo.Sebastian Bleisch—Das Lagerhaus—4 ET (gay preteen kidsex) 9.06.mpg. Government Exhibit 2.

6 "[A] police view subsequent to a search conducted by private citizens does not constitute a 'search' within the meaning of the Fourth Amendment so long as the view is confined to the scope and product of the initial search." *United States v. Bomengo*, 580 F.2d 173, 175 (5th Cir. 1978); *see also United States v. Paige*, 136 F.3d 1012, 1019 (5th Cir. 1998). At least one court has held that hash value analyses do constitute searches for Fourth Amendment purposes. *See United States v. Crist*, 627 F. Supp. 2d 575, 585 (2008) ("The Court rejects [the Government's] view and finds that the 'running of hash values' is a search protected by the Fourth Amendment."); *see also United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, J., concurring) ("[T]he government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves. These and similar search tools should not be used without specific authorization in [a] warrant."). However, some commentators have argued that because of the non-intrusive nature of hash value analyses and their ability to discern contraband without revealing other content, they should not be considered searches under the Fourth Amendment. These commentators have concluded that hash value comparisons are analogous to a canine sniff. *See* 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, 276-80 (2011); Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 44-46 (2005).

7 Where law enforcement's search only confirms what it already knew with substantial certainty, it does not expand the scope of a private search. *United States v. Runyan*, 275 F.3d at 463.

8 Actions that "enabled the agent to learn nothing that had not previously been learned during the private search" do not invade a legitimate expectation of privacy. *United States v. Jacobsen*, 466 U.S. 109, 127 (1984).

9 "No protected privacy interest remains in contraband in a container once government officers lawfully have opened that container and identified its contents as illegal." *Illinois v. Andreas*, 463 U.S. 765, 771 (1983). "[G]overnmental conduct that only reveals the possession of contraband 'compromises no legitimate privacy interest.' " *Illinois v. Caballes*, 543 U.S. 405, 408 (2005).

10 The exceptions are: (1) dissipated taint: when "the connection between the illegal police conduct and the discovery and seizure of the evidence is 'so attenuated as to dissipate the taint;' " (2) independent source: when the evidence was discovered by means wholly independent of the constitutional violation, even if the same evidence was also discovered during or as a consequence of illegal police conduct; (3) Inevitable discovery: when the evidence would have been discovered by lawful means had the investigation continued without the tainted evidence; and (4) good faith: when law enforcement reasonably relied in good faith upon a warrant later found to be improperly issued. While the hash value match to the NCMEC database and some of the file names might have justified using the fruits of the Phase II search under the independent source or inevitable discovery rules, the Government did not plead those exceptions. *United States v. Ceccolini*, 435 U.S. 268, 279 (1978) (first exception); *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920) (second exception); *Brewer v. Williams*, 430 U.S. 387, 406 n. 12 (1977) (third exception); *United States v. Leon*, 468 U.S. 897, 924 (1984) (fourth exception).

11 The Fifth Circuit has acknowledged that the good faith exception will not apply in four scenarios: (1) when the issuing magistrate was misled by information in an affidavit that the affiant knew or reasonably should have known was false; (2) when the issuing magistrate wholly abandoned his judicial role; (3) when the warrant affidavit is so lacking in indicia of probable cause as to render official belief in its existence unreasonable; and (4) when the warrant is so facially deficient in failing to particularize the place to be searched or the things to be seized that executing officers cannot reasonably presume it to be valid. *Massi*, 761 F.3d at 529-30 (quoting *United States v. Woerner*, 709 F.3d 527, 533-34 (5th Cir. 2013)).

12 *See also*, *United States v. McClain*, 444 F.3d 556, 566 (6th Cir. 2005). *But cf., United States v. McGough*, 412 F.3d 1232, 1239-40 (11th Cir. 2005) (good faith exception does not apply where a search warrant is issued on the basis of evidence obtained as the result of an illegal search); *United States v. Vasey*, 834 F.2d 782, 789-90 (9th Cir. 1987) (magistrate's issuance of warrant based on tainted evidence does not sanitize the taint).

13 In *Massi*, the court held that a warrant issued after a prolonged detention that was not supported by reasonable suspicion or probable cause fell within the good faith exception because of "the absence of precedent on holding suspects and their 'vehicle' in order to prepare a proper warrant request, as opposed just to searching under exigent circumstances without a warrant." *Massi*, 761 F.3d at 529. In another case, the court held that a dog sniff of the defendant's garage door was "close enough to the line of validity" for purposes of the good faith exception. *United States v. Holley*, 831 F.3d 322, 327 (5th Cir. 2016).

End of Document