IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

United States Court of Appeals
Fifth Circuit
FILED
August 17, 2018
Lyle W. Cayce
Clerk

No. 17-41116

UNITED STATES OF AMERICA,

Plaintiff - Appellee

v.

HENRY FRANKLIN REDDICK,

Defendant - Appellant

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

Before KING, SOUTHWICK, and HO, Circuit Judges.

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 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 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.

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.

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]

The Supreme Court's decision in *United States v. Jacobsen*, 466 U.S. 109 (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.

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. Any expectation of privacy the recipients

[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.

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.

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*, 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 (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. 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.

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-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.