FIFTH CIRCUIT HOLDS NO FOURTH AMENDMENT VIOLATION WHEN DETECTIVE VIEWED CHILD PORN DISCOVERED BY PRIVATE COMPANY

February 2019

Article Source: http://llrmi.com/articles/legal_updates/2019_us_v_reddick/

On August 17, 2018, the Fifth Circuit Court of Appeals decided *the United States v. Reddick*[i], in which the Fifth Circuit decided a case of first impression that stemmed from a detective viewing images from Reddick's computer files that were downloaded to Microsoft SkyDrive and sent to law enforcement via a tip line. The relevant facts of *Reddick,* taken directly from the case, are as follows:

> 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).[ii]

Reddick filed a motion to suppress and argued that opening the files from CyberTips without a warrant violated his rights under the Fourth Amendment, and any evidence obtained from the subsequent

search warrant should be excluded as "fruit of the poisonous tree." The district court denied the motion and Reddick pled guilty with the right to appeal the denial of the motion to suppress. He then appealed the denial of the motion to the Fifth Circuit Court of Appeals.

On appeal, the Fifth Circuit noted that a private company used private software to identify the hash values of known child pornographic images and then passed that information, and image file along to law enforcement. The court noted that this is considered a "private search" for Fourth Amendment purposes. However, they also noted that the "private search" doctrine has not previously been applied in similar factual circumstances by any other federal circuit. As such, the Fifth Circuit stated

> This case therefore presents an opportunity to apply established Fourth Amendment principles in this new context.[iii]

The court of appeals then examined the case of the *United States v. Jacobsen*[iv], which is the Supreme Court case in which the Court first established "private search" or "frustration of privacy" concept. In that case, Federal Express employees noticed that a package had been damaged during shipping. They opened the package and observed that it contained white powder. The DEA was called and agents used a field test kit to test the powder, which tested positive for cocaine. The agents used this information to then obtain warrants to arrest intended recipients of the package. The Supreme Court held that the agents did not violate the Fourth Amendment by testing the white powder because once a person's expectation of privacy is frustrated by a private person, that information is no longer private (or subject to a reasonable expectation of privacy).

The Supreme Court articulated the rule regarding private searches (or frustration of privacy) as follows:

> **Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-non-private information**.[v] [emphasis added]

The court then identified the issue before them as follows:

> [*W]hether, 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*.[vi]

In other words, the court set out to determine if Reddick's expectation of privacy had already been frustrated by CyberTips and the use of the PhotoDNA software when the files and hash values were sent to the detective.

The court examined the relevant facts of the case and stated

> **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**.[vii] [emphasis added]

The court then set out to examine if opening the files exceeded the scope of private search. First, the court noted that hash values "allow law enforcement to identify child pornography with almost absolute certainty."[viii] Therefore, when the detective opened the files, there was no significant expansion of the private search. In other words, opening the file to dispel any doubt regarding the nature of the images was analogous to the DEA agents in *Jacobsen*, testing the powder. The court stated

> **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.[ix] [emphasis added]

The court also contrasted Reddick's case with the Tenth Circuit case of *the United States v. Ackerman*[x], in which an investigator conducted a warrantless search of an email and three attachments that did **not** have hash values that corresponded to child pornography. The Tenth Circuit held that this was a Fourth Amendment violation. However, in Reddick's case, the hash values did match known child pornography, thus, *Ackerman* was not relevant to Reddick's case.

The court then held that the detective in Reddick did not violate the Fourth Amendment by opening the files. The court stated

> **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**.[xi]

---

[i] No. 17-41116 (5th Cir. Decided August 17, 2018 Unpublished)
[ii] Id. at 3-4
[iii] Id. at 2
[iv] 466 U.S. 109 (1984)
[v] Id. at 117
[vi] Id. at 5
[vii] Reddick, No. 17-15294 at 6
[viii] Id.
[ix] Id. at 7
[x] 831 F. 3d 1292 (10th Cir. 2016)
[xi] Reddick, No. 17-15294 at 7