DISTRICT COURT OF APPEAL OF FLORIDA
SECOND DISTRICT

LAWRENCE YOUNGMAN,

Appellant,

v.

STATE OF FLORIDA,

Appellee.

No. 2D21-2472

July 1, 2022

Appeal from the Circuit Court for Polk County; Michael P. McDaniel, Judge.

Howard L. Dimmig, II, Public Defender, and Richard J. Sanders, Assistant Public Defender, Bartow, for Appellant.

Ashley Moody, Attorney General, Tallahassee, and Jonathan S. Tannen, Assistant Attorney General, Tampa, for Appellee.

LaROSE, Judge.

Lawrence Youngman appeals his judgment and sentences related to child pornography. Specifically, he challenges the trial court's denial of his motion to suppress numerous child

pornography files seized from his personal computer. We have jurisdiction. *See* Fla. R. App. P. 9.030(b)(1)(A). Mr. Youngman lacked a reasonable expectation of privacy in the alphanumeric identification codes unique to each file he shared and otherwise made available to the public over a peer-to-peer file sharing network. Therefore, we affirm.

Background

The Polk County Sheriff's Office (PCSO) commenced an online investigation of child pornography on BitTorrent, a peer-to-peer file sharing network. BitTorrent is publicly available. It allows users to share their computer's selected content over the BitTorrent network with other users and to search other users' shared content.

PCSO utilized a software program, Torrential Downpour, to scour BitTorrent's astronomical amount of shared content. Torrential Downpour is a Child Protection System (CPS) software available only to law enforcement. It searches for the "hash values" of known child pornographic content. *See generally United States v. Hoeffener*, 950 F.3d 1037, 1040-41 (8th Cir. 2020) ("Torrential Downpour is a law enforcement software program configured to search the BitTorrent network for Internet Protocol ('IP') addresses

associated with individuals offering to share or possess files known to law enforcement to contain images or videos of child pornography. . . . [T]he program logs the date, time, and [hash values] of the activity occurring during the investigation; the path and file name investigated; and the investigated computer's IP address, port identifier, and BitTorrent software."). A "hash value" is a thirty-two-digit alphanumeric code, a "unique digital fingerprint" for each piece of digital media; no two pieces have the same value. *United States v. Sosa-Pintor*, 741 F. App'x 207, 208 (5th Cir. 2018).

To facilitate file searching and sharing among BitTorrent's users, BitTorrent users manually search by hash value for a particular file. However, Torrential Downpour is an automated program allowing for a much more efficient search of the users' catalogue of shared files. Importantly, Torrential Downpour does not allow law enforcement to access a BitTorrent user's hard drive, or the files stored thereon, only the hash value for the files shared by the user on the BitTorrent network. Torrential Downpour lacks the capacity to breach a device's firewall; instead, it searches BitTorrent for files with hash values known to be associated with

child pornography. *See Hoeffener*, 950 F.3d at 1041 ("Torrential Downpour cannot access non-public areas or unshared portions of an investigated computer, nor can it override settings on a suspect's computer.").

Mr. Youngman installed BitTorrent and shared his computer's selected content with the public. Through its use of Torrential Downpour, PCSO identified two hash values for known child pornography shared from a device associated with Mr. Youngman's IP address. *See Knight v. State*, 154 So. 3d 1157, 1159 (Fla. 1st DCA 2014) (describing an "IP address" as "the number identifying the location where the computer [i]s hooked up to the Internet"). Based upon the hash value comparison, Torrential Downpour "asked" Mr. Youngman's computer if it still had the media associated with those hash values; his computer automatically responded in the affirmative. *See Morales v. State*, 274 So. 3d 1213, 1218 (Fla. 1st DCA 2019) ("[H]ash 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.' " (quoting *United States v. Larman*, 547 F. App'x 475, 477 (5th Cir. 2013))). PCSO was unable to complete the

download of the media from Mr. Youngman's computer. Nonetheless, because PCSO knew that the hash values were associated with child pornography, it obtained a search warrant for Mr. Youngman's home and the electronic devices therein.

During its search, PCSO located a multitude of electronic files containing child pornography. Ultimately, the State charged Mr. Youngman with one count of promoting a sexual performance by a child and one hundred counts of possession of child pornography (enhanced). *See* § 827.071(3), (4), Fla. Stat. (2016).

Mr. Youngman filed a motion to suppress "[a]ny and all . . . files that were stored on [Mr. Youngman]'s personal computing devices." He asserted that the search warrant should never have issued because the "[hash value] evidence was obtained as a result of an illegal search without a warrant." He contended that the hash values themselves were protected, private information and that this "information was obtained by means of [Torrential Downpour,] a software search program available only to law enforcement and not to the general public." Thus, he claimed, the illicit images must be suppressed as "fruit of the poisonous tree." *See generally Hatcher v. State*, 834 So. 2d 314, 317 n.4 (Fla. 5th DCA 2003) ("The fruit of the

poisonous tree doctrine is a court-made exclusionary rule 'which forbids the use of evidence in court if it is the product or fruit of a search or seizure or interrogation carried out in violation of constitutional rights.' " (first quoting *Craig v. State*, 510 So. 2d 857, 862 (Fla. 1987); and then citing *United States v. Cruz*, 581 F. 2d 535, 537 (5th Cir. 1978) (en banc), *overruled on other grounds by United States v. Causey*, 834 F.2d 1179, 1184-85 (5th Cir. 1987))).

The trial court denied the motion. It reasoned that Mr. Youngman lacked a reasonable expectation of privacy in his electronic files publicly stored and shared on a peer-to-peer file-sharing network. After Mr. Youngman entered a nolo plea, the trial court sentenced him to thirty years' imprisonment.

Reiterating many of the arguments made below, Mr. Youngman continues to claim that the trial court erred in denying his suppression motion, arguing that the hash value was obtained as part of an illegal search. He likens his case to *Kyllo v. United States*, 533 U.S. 27, 34 (2001), in which the Supreme Court "held that use of a thermal imager to scan for heat signals within a person's home constituted a search because that information[-]i.e., the heat signals[-]could not have been obtained without the use of a

'sense-enhancing technology' that intruded into the interior of a home, a 'constitutionally protected area.' " *McClelland v. State*, 255 So. 3d 929, 932 (Fla. 2d DCA 2018) (quoting *Kyllo*, 533 U.S. at 34); *see Kyllo*, 533 U.S. at 29, 40 (concluding that "the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment" as the device, which "[wa]s not in general public use, . . . explore[d] details of the home that would previously have been unknowable without physical intrusion").

Standard of Review

"[I]n reviewing a trial court's ruling on a motion to suppress, this court must give deference to the trial court's factual findings if those findings are supported by competent, substantial evidence, but this court must review the trial court's ruling of law de novo." *State v. Roman*, 103 So. 3d 922, 924 (Fla. 2d DCA 2012) (citing *Jardines v. State*, 73 So. 3d 34, 54 (Fla. 2011)).

Analysis

"Technological advancement often collides with the Fourth Amendment." *State v. Sylvestre*, 254 So. 3d 986, 990 (Fla. 4th DCA

2018); *cf. NetChoice, LLC v. Att'y Gen.*, No. 21-12355, 2022 WL 1613291, at *1 (11th Cir. May 23, 2022) ("Not in their wildest dreams could anyone in the Founding generation have imagined Facebook, Twitter, YouTube, or TikTok."). And yet, "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, [the United States Supreme Court] has sought to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' " *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (third alteration in original) (quoting *Kyllo*, 533 U.S. at 34).

To that end, whether it be the virtual reality crafted by technological innovation or our own corporeal reality, a court's analysis of any search and seizure remains the same; it is guided by article I, section 12, of the Florida Constitution and the Fourth Amendment to the United States Constitution. *See Morales*, 274 So. 3d at 1215 ("Under article I, section 12 of the Florida Constitution, the right of individuals to be free from unreasonable searches and seizures must be construed in conformity with the Fourth Amendment to the United States Constitution as interpreted

by the United States Supreme Court." (citing *Clayton v. State*, 252 So. 3d 827, 829 (Fla. 1st DCA 2018))).

More specifically, "[t]he touchstone of any Fourth Amendment analysis is whether the defendant had a reasonable expectation of privacy in the place searched." *State v. M.B.W.*, 276 So. 3d 501, 506 (Fla. 2d DCA 2019).

> "For purposes of the Fourth Amendment, a 'search' occurs only when an individual's reasonable expectation of privacy is infringed by an agent of the government." *Duke v. State*, 255 So. 3d 478, 480 (Fla. 1st DCA 2018) (citing *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). Thus, "a Fourth Amendment search does not occur . . . unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that expectation as reasonable.' " *Kyllo*[, 533 U.S. at 33] (quoting *California v. Ciraolo*, 476 U.S. 207, 211 (1986)). "Before a defendant may invoke the protections of the Fourth Amendment, he must establish standing by showing that he has a legitimate expectation of privacy in the area searched or the item seized." *State v. Williams*, 184 So. 3d 1205, 1208-09 (Fla. 1st DCA 2016).

Morales, 274 So. 3d at 1215-16 (first alteration and omission in original); *see Bond v. United States*, 529 U.S. 334, 338 (2000) ("Our Fourth Amendment analysis embraces two questions. First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that 'he

[sought] to preserve [something] as private.' . . . Second, we inquire whether the individual's expectation of privacy is 'one that society is prepared to recognize as reasonable.' " (alterations in original) (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979))); *Hicks v. State*, 929 So. 2d 13, 16 (Fla. 2d DCA 2006) ("A search violates a defendant's Fourth Amendment rights only if (1) a defendant demonstrates that he or she had an actual, subjective expectation of privacy in the property searched and (2) a defendant establishes that society would recognize that subjective expectation as objectively reasonable." (first citing *Minnesota v. Olson*, 495 U.S. 91, 95 (1990); and then citing *Smith*, 442 U.S. at 740-41)).

In *Smith*, 442 U.S. at 743-44, the Court reiterated that it had "consistently . . . held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." In the age of peer-to-peer electronic file sharing, "[federal] courts have consistently held that Fourth Amendment protections do not extend to data shared through peer-to-peer networks." *United States v. Weast*, 811 F.3d 743, 747 (5th Cir. 2016); *see United States v. Conner*, 521 F. App'x 493, 497 (6th Cir. 2013) ("[P]eer-to-peer file sharing is different in kind from e-mail, letters, and telephone calls.

Unlike these forms of communication, in which third parties have incidental access to the content of messages, [peer-to-peer file sharing] programs . . . are expressly designed to make files on a computer available for download by the public, including law enforcement. Peer-to-peer software users are not mere intermediaries, but the intended recipients of these files. Public exposure of information in this manner defeats an objectively reasonable expectation of privacy under the Fourth Amendment." (citing *Katz v. United States*, 389 U.S. 347, 351 (1967))).

Florida courts, too, have rejected Fourth Amendment challenges to information shared over peer-to-peer networks. *See, e.g.*, *Mardosas v. State*, 257 So. 3d 540, 540 (Fla. 1st DCA 2018). For instance, in *Frazier v. State*, 180 So. 3d 1067, 1068 (Fla. 5th DCA 2015), the court concluded "that a person who shares files over a peer-to-peer network has no expectation of privacy in those files" and, therefore, "the State did not violate Appellant's Fourth Amendment rights by using [CPS software] to obtain information to form the basis for its search warrant." That is because "CPS software does not infiltrate any computers when searching peer-to-peer networks for child exploitation material. Rather, the software

gathers only public information made available by the user sharing files over the network." *Id.* In other words, "CPS software does not 'search any areas of [defendant's] computer, download any files, or otherwise reveal any information . . . unavailable to ordinary internet users." *Id.* (alteration and omission in original) (quoting *United States v. Gabel*, No. 10-60168, 2010 WL 3927697, at *7 (S.D. Fla. 2010)).

Any member of the public could access Mr. Youngman's shared files by simply downloading BitTorrent and asking for the desired files, a request that the suspect computer automatically fulfills. It follows then, that because the hash value for each digital media stored on BitTorrent is publicly available, any claimed expectation of privacy in the hash value withers under the scrutiny of a Fourth Amendment analysis. Torrential Downpour neither searched for nor obtained any information that was not already publicly available. Quite simply, Mr. Youngman lacked a reasonable expectation of privacy in publicly available information. *See Hicks*, 929 So. 2d at 16 ("Whether a defendant has a reasonable expectation of privacy is a threshold inquiry." (footnote omitted) (citing *Rakas v. Illinois*, 439 U.S. 128, 143 (1978))).

Moreover, to our knowledge "[a]ll reported state court decisions considering this issue have likewise held that law enforcement may use CPS software to obtain information to form probable cause for a search warrant without violating the defendant's expectation of privacy." *Frazier*, 180 So. 3d at 1068-69 (citing several foreign state cases). Thus, we echo the *Frazier* court's sentiment; Mr. Youngman "knew or should have known that sharing files over the [peer-to-peer file sharing] network would 'allow the public at large to access files in his shared folder unless he took steps to avoid it.' " *Id.* at 1069 (quoting *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010)).

We reject Mr. Youngman's argument that *Kyllo* applies. There, the Court was especially offended by law enforcement's utilization of a heat-seeking technology ("a device that is not in general public use") to invade the physical boundaries of someone's home. *Kyllo*, 533 U.S. at 40. The Court easily concluded that the use of such technology constituted "a 'search' and is presumptively unreasonable without a warrant." *Id.* ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been

unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

PCSO did not intrude into the sanctity of Mr. Youngman's home. It only searched his shared publicly available files. Unlike *Kyllo*, 533 U.S. at 40, where the "details of the home" were otherwise "unknowable without physical intrusion," Torrential Downpour did not afford PCSO access to the digital equivalent of Mr. Youngman's home, that is, his hard drive or the files stored thereon.

Additionally, the Torrential Downpour technology used by PCSO "merely automates the aggregation of public information[-]a task that could otherwise be performed manually by law enforcement, albeit at a slower and less efficient pace." *Frazier*, 180 So. 3d at 1068 (quoting *United States v. Thomas*, 788 F.3d 345, 352 (2d Cir. 2015)). "CPS software operates 'simply as a sorting mechanism to prevent the government from having to sift, one by one, through [an individual's] already publicly exposed files." *Id.* (alteration in original) (quoting *Borowy*, 595 F.3d at 1048). Thus, Torrential Downpour is not akin to the thermal imager in *Kyllo* that law enforcement utilized to search inside one's home. Torrential

Downpour merely affords the government a more efficient means of sifting publicly available data.

In light of the foregoing, the trial court properly concluded that Mr. Youngman lacked a reasonable expectation of privacy in the publicly available electronic files, and the corresponding hash values, shared over BitTorrent. The evidence from the suppression hearing demonstrated that PCSO's CPS software only searched for information that Mr. Youngman's computer made publicly available over the network. *Cf. United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009) ("One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking."). PCSO could have conducted the same search for hash values of known child pornography using publicly available BitTorrent software. The Torrential Downpour program simply automates the process, allowing law enforcement to conduct thousands of searches at a time. Law enforcement's use of such technology to ascertain the hash values tied to Mr. Youngman's computer does not offend the Fourth Amendment.

Conclusion

The trial court properly denied Mr. Youngman's motion to suppress. We affirm his judgment and sentences.

Affirmed.

MORRIS, C.J., and BLACK, J., Concur.

Opinion subject to revision prior to official publication.