NOT FINAL UNTIL TIME EXPIRES TO FILE REHEARING MOTION AND, IF FILED, DETERMINED

IN THE DISTRICT COURT OF APPEAL
OF FLORIDA
SECOND DISTRICT

TRAVIS MORGAN JEROR,)
Appellant,))
V.) Case No. 2D19-3308
STATE OF FLORIDA,)
Appellee.)))

Opinion filed February 12, 2021.

Appeal from the Circuit Court for Sarasota County; Debra Johnes Riva, Judge.

Tim Bower Rodriguez of Tim Bower Rodriguez, P.A., Tampa, for Appellant.

Ashley Moody, Attorney General, Tallahassee, and Jonathan P. Hurley, Assistant Attorney General, Tampa, for Appellee.

SILBERMAN, Judge.

Travis Morgan Jeror appeals his judgment and sentence of eleven months and twenty-nine days in jail, to be followed by three years of probation, for transmission of child pornography by electronic device or equipment. He contends that the trial court should have granted his motion for judgment of acquittal because the State failed to prove that he knew or reasonably should have known that he transmitted the

pornography by using a peer-to-peer file-sharing program. In reviewing the evidence in the light most favorable to the State, as we must, we conclude that the trial court did not err in denying the motion for judgment of acquittal and allowing the case to go to the jury. Accordingly, we affirm.

FACTS

At trial, Detective James Klay was the State's primary witness. His job is to forensically analyze electronic evidence, and he is trained in how to investigate peer-to-peer software, including the "BitTorrent network." The detective explained that a peer-to-peer network is "a program that reaches out and obtains data" by communicating with other computers. Users get data from each other all over the world. Peer-to-peer network users are like a phone directory, but he acknowledged users "may not know in the background that they are being the phone directory."

The detective's work involves trying to download child pornography from throughout Florida. He searched for known "hash values" or "torrents" of child pornography. Jeror's computer had the peer-to-peer file-sharing program called wTorrent installed on it. The detective's computer communicated with Jeror's Internet Protocol (IP) address seventeen times. This meant that the user of the target IP address was actively running the program during those times. The prosecutor asked the detective if "that person was sort of advertising child pornography." The defense objected to the reference "that person" if the prosecutor was referring to a computer. The trial court sustained the objection. The detective clarified that when the peer-to-peer file-sharing program was actively running, "[t]he computer was indicating" that it

had child pornography. The computers communicate by what is known as "handshakes," with "one computer talking to another computer."

The detective was able to download a video of child pornography from Jeror's IP address in Sarasota County on November 12, 2017. On February 17, 2018, he was able to download two more videos that contained child pornography from Jeror's IP address. They were "obtained via peer-to-peer." The detective did not have direct communication with Jeror and did not search Jeror's computer to get the videos. Rather, he asked the router for videos while the user was on the network. He explained that the "whole purpose" of a file-sharing peer-to-peer network such as wTorrent is to share information, and if a person is using the network, he is "seeding the network." The detective acknowledged that sometimes a user, referred to as a leech, wants to use a torrent program to look at something but does not want to share it. However, he was not aware of an opt-out function to sharing on wTorrent. Instead, the application (app) can access anything in the video folder on the computer.

After a search warrant was obtained and Jeror's computer was seized on February 28, 2018, the detective conducted a forensic examination of the computer. In his experience, an "advanced computer user" would download the types of programs found on Jeror's computer. Among Jeror's programs were three that create a virtual private network (VPN) and scramble information to hide what the user is doing, including on the internet. Some of the programs allow internet searches that are not recorded and access to the "dark web." Jeror's computer also had programs designed to erase data from the computer. Another program was Easy Tether which allows a

person to tether his Android phone to his computer. Jeror's computer also had a solidstate hard drive which, at the time, the detective did not see very often.

The wTorrent program on Jeror's computer was installed and used from November 12, 2017, to February 25, 2018. That is the program from which the detective obtained the contraband through Jeror's IP address. The detective used one of his investigative computers to download wTorrent. After he hit the "get-button" a "splash screen" popped up, and the detective did a screen capture of the splash screen. The splash screen stated, "This app can access your internet connection and act as a server." The detective explained that on peer-to-peer networks "the users are the users and the servers." He did not install the wTorrent app because he did not want to expose everything on the sheriff's office network to the world.

The detective was unaware of any user license agreement for wTorrent.

He explained that the app can access anything in the video folder on the computer and share it with everyone on the program. It also accesses music, pictures, and other information. The wTorrent program only shares video files after the files have been moved from the download folder to a video folder. The detective testified that "Windows creates a file so it can find it later, saying, 'This is where it's at. It's in videos.' "

Information on Jeror's computer showed that one afternoon, Jeror's bank statements were downloaded. About an hour and a half later, one of the child pornography videos was viewed in Jeror's downloads folder. Less than two hours later, the video was viewed again in the video folder. The detective testified that the videos were moved by "user interaction" from the downloads folder into the video folder. Had they remained in the downloads folder the app would not have shared them.

The detective was asked "if a person doesn't do anything in the world but use this program to go and get something and look at it, okay, and five minutes later" you extract it, has the user "affirmatively done anything with you other than use the BitTorrent program?" The detective responded, "Well, tacitly, yes, because that's how the program works." He agreed that by using the program, the user has "tacitly agreed to share." The detective was later asked:

- Q. Did he affirmatively do anything to further that, other than simply use the BitTorrent program himself?
- A. No, he did not.
- Q. So, this is all done automatically?
- A. Correct.

The detective said that "the only thing the human being has to do in this case is have the program running at the time." But "the way to not have sent it is not to have put it in the videos folder."

As to whether Jeror was intentionally trying to share files, the detective testified without objection that "just from using the program, you should reasonably know, in my opinion, stress that again, my opinion, that you are sharing it." (Emphasis added.) He acknowledged that Jeror did not communicate with him, and he saw no indication that Jeror had offered to share child pornography with anyone else.

There was no contraband on Jeror's computer when it was searched. But there was evidence that contraband had been on the computer at some point and had been deleted. The forensic examination revealed that cleaning programs had been used to clean the computer before it was seized.

In his motion for judgment of acquittal, Jeror argued that he did nothing other than use a torrent program to download something from the internet. He argued that there has to be some affirmative act on the part of a defendant to send the image to meet the element of transmitting. He did not dispute that he downloaded and looked at the images but contended that there was no evidence "he did something that caused [the videos] to be sent."

The State argued that it met its burden in that Jeror "move[d] these files from the original download location to the videos location where the defendant, as an advanced computer user, as testified to by Detective Klay, would know that that is where the videos would be sent." Moving a file from the download folder to the video folder "caused it to be able to be downloaded by other members of that network" when Jeror was running the network. The State also argued that Jeror "saw that splash screen which indicates that is where the files will be shared from." Jeror responded that there was no evidence that he saw the splash screen, signed a user agreement, or "did anything affirmatively to acknowledge the fact that he knew he would be sharing."

In denying the motion for judgment of acquittal, the trial court noted the programs on Jeror's computer, "his knowledge of the use of these specialized programs, and what the—what flashes up once the torrent is placed on to the computer." The trial judge ruled as follows:

When I look at the evidence that the State elicited through Detective Klay and the fact that this was a publicly accessible website that the items were moved to, I am going to find that the State has met its burden to allow the case to go to the jury, and I'll deny the motion for judgment of acquittal.

ANALYSIS

In reviewing the sufficiency of the evidence, we consider " 'the evidence in the light most favorable to the State' and, maintaining this perspective, ask whether 'a rational trier of fact could have found the existence of the elements of the crime beyond a reasonable doubt.' " Bush v. State, 295 So. 3d 179, 200 (Fla. 2020) (quoting Rogers v. State, 285 So. 3d 872, 891 (Fla. 2019), receded from on other grounds by Lawrence v. State, 45 Fla. L. Weekly S277, S278 (Fla. Oct. 29, 2020)). The State must present competent, substantial evidence to sustain the verdict, and conflicts in the evidence and reasonable inferences from that evidence are resolved in favor of the verdict. Id. at 200-01.

Section 847.0137(2), Florida Statutes (2017), provides that "any person in this state who knew or reasonably should have known that he or she was transmitting child pornography, as defined in s. 847.001, to another person in this state or in another jurisdiction commits a felony of the third degree." (Emphasis added.) Transmit is defined as "the act of sending and causing to be delivered any image, information, or data from one or more persons or places to one or more other persons or places over or through any medium, including the Internet, by use of any electronic equipment or device." § 847.0137(1)(b).

The Florida Supreme Court addressed section 847.0137 in Smith v. State, 204 So. 3d 18 (Fla. 2016) (Smith II), and whether the State had proven a transmission. The Florida Supreme Court approved the Fourth District's decision in Smith v. State, 190 So. 3d 94 (Fla. 4th DCA 2015) (Smith I). Smith II, 204 So. 3d at 22. The facts in Smith II revealed the following:

Smith sent child pornography images to an electronic "place" by loading them into a specific computer file and, through his

use of the file-sharing program, made those images accessible to third parties for whom access was authorized. Smith then sent a "friend" request to a third party which authorized the third party—through the file-sharing program—to obtain access to the place to which the images had been sent.

<u>Id.</u> Smith sent the friend request to undercover detectives. After he was arrested, Smith had admitted to "trading in child pornography." <u>Id.</u> at 20 (quoting <u>Smith I</u>, 190 So. 3d at 95).

When the computer user creates a "shared file folder and specifically authorizes others to download the contents of that folder, he is 'sending' information in the form of the 'friend' request and is 'causing' the pornographic images to be delivered to another. It is reasonably foreseeable that the pornographic images will be accessed and downloaded." Id. at 20-21 (quoting Smith I, 190 So. 3d at 97). The user need not personally deliver the files to a third party, "such as by attaching them to an email." Id. at 21 (quoting Smith I, 190 So. 3d at 97). The user could reasonably foresee that another party "would access the folder and download the images, thus 'causing' them to be delivered to another." Id. (quoting Smith I, 190 So. 3d at 97).

In a case where a "statute is clear and unambiguous, courts will not look behind the statute's plain language for legislative intent or resort to rules of statutory construction to ascertain intent." Id. at 21 (quoting Borden v. E.—European Ins. Co., 921 So. 2d 587, 595 (Fla. 2006)). The Smith II court determined that the definition of transmit was unambiguous and that "Smith sent child pornography images to an electronic 'place' by loading them into a specific computer file," and via the file-sharing program he "made those images accessible to third parties for whom access was authorized." Id. at 22. The court concluded that "the use of a file-sharing program,

where the originator affirmatively grants the receiver access to the originator's child pornography files, constitutes the transmission of child pornography under the plain meaning of section 847.0137." <u>Id.</u> at 22.

Here, the wTorrent program Jeror used did not require him to individually grant access to a specific person by sending a friend request. Unlike in <u>Smith II</u>, Jeror did not send a friend request authorizing someone else to access his video folder. But the evidence established that by using the wTorrent program, anything moved into Jeror's video folder would be shared automatically as long as his computer was running the program. Because section 847.0137 applies to conduct where the person "knew or reasonably should have known that he or she was transmitting child pornography," the question before us is whether the evidence, viewed most favorably to the State, was sufficient to support the denial of Jeror's motion for judgment of acquittal and to allow the case to go to the jury.

Jeror cites to <u>United States v. Carroll</u>, 886 F. 3d 1347, 1353 (11th Cir. 2018), regarding the knowledge element. <u>Carroll</u> involved a federal statute that prohibited "knowingly" distributing child pornography. <u>Id.</u> (citing 18 U.S.C. § 2252(a)(2) (2012)). Carroll had used the Ares peer-to-peer network which, when the user downloads the program, "sets up a shared folder on the computer where, by default, it automatically places all subsequent downloads." <u>Id.</u> at 1350. A file is immediately accessible to other Ares users when the file is placed in the shared folder. Id.

The court rejected the government's argument that "it would be impossible for an individual to use a peer-to-peer file sharing program and lack a full understanding of its operations." <u>Id.</u> at 1354. The court noted that the variety of peer-to-peer

programs made the issue of knowledge a fact-sensitive inquiry, "where the mechanics of each peer-to-peer program may bear on the issue of knowledge in different ways."

Id. The court acknowledged examples, however, of when a program's design "may foreclose any possibility that the user unwittingly shared files," as follows:

It would be difficult to claim ignorance where, for example, the peer-to-peer program prompts the user during installation to choose whether or not he wants to share downloaded files, see United States v. Spriggs, 666 F.3d 1284, 1286–87 (11th Cir. 2012), requires the user to authorize file sharing for each particular peer that requests it, see United States v. McElmurry, 776 F.3d 1061, 1065 (9th Cir. 2015), or forces the user to acknowledge and accede to a licensing agreement explaining the peer-to-peer process and then involves the user in setting up a shared folder, see United States v. Shaffer, 472 F.3d 1219, 1221 (10th Cir. 2007).

<u>Id.</u> The court stated that "Carroll took none of these actions, and the government provided no other basis for his knowledge of distribution." <u>Id.</u> Thus, the court reversed his conviction for distribution of child pornography. Id.

While <u>Carroll</u> addresses a statute proscribing the knowing distribution of child pornography, the statute at issue here applies to persons "who knew or reasonably should have known" that they were transmitting such materials. § 847.0137(2). The State cites to <u>United States v. Cullen</u>, 796 F. App'x 976, 979-80 (11th Cir. 2019), in support of its argument as to the knowledge element. <u>Cullen</u> also involved a peer-to-peer sharing program. <u>Id.</u> at 977-78. Cullen testified that he had never allowed sharing of pornography from his computer. <u>Id.</u> at 978. But he acknowledged that he understood how the program's automatic file-sharing function operated, and the Eleventh Circuit affirmed his conviction for distribution of child pornography and other offenses. <u>Id.</u> at 980; <u>see also United States v. Neiheisel</u>, 771 F. App'x 935, 939 (11th

Cir. 2019) (affirming conviction for knowingly distributing child pornography when Neiheisel admitted that he stored the videos "in a shared downloads folder connected to a peer-to-peer network" and "discussed how the sharing mechanism worked"), cert. denied, 140 S. Ct. 511 (2019).

We do not find <u>Cullen</u> to be particularly helpful because here, the State presented no statements by Jeror to establish that he knew that files in his video folder are shared. Instead, the State pointed to the "splash screen" that the detective saw when he downloaded but did not install the wTorrent program during his investigation. The splash screen stated, "This app can access your internet connection and act as a server." But there was no evidence that when Jeror downloaded the program he received and saw this notice.

The State also maintains that based on the types of programs Jeror had on his computer, his action in moving the videos from the downloads folder into the video folder that is shared with other users of the wTorrent file sharing program, and the detective's testimony, the jury could reasonably determine that Jeror knew or should have known that he was transmitting child pornography through the wTorrent program. And as noted previously, when the detective was asked whether Jeror was intentionally trying to share those files, the detective testified without objection that a person using the program and moving the files into the video folder should reasonably know "you are sharing it." As to other programs that Jeror was using on his computer, the detective acknowledged that they were the types of programs which an "advanced computer user" would download.

We agree that the State presented sufficient evidence through the detective's testimony that would allow the jury to find beyond a reasonable doubt that Jeror reasonably should have known that the child pornography files would be accessible to and transmitted to others through his use of the wTorrent program and the peer-to-peer network. The trial court did not err in denying Jeror's motion for judgment of acquittal, and we affirm Jeror's judgment and sentence.

Affirmed.

CASANUEVA and BLACK, JJ., Concur.