

[DO NOT PUBLISH]

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

No. 17-13729
Non-Argument Calendar

D.C. Docket No. 6:16-cr-00170-PGB-DCI-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

DAVID R. RIVENBARK,

Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida

(September 5, 2018)

Before WILLIAM PRYOR, BRANCH and HULL, Circuit Judges.

PER CURIAM:

After a jury trial, defendant David Rivenbark was convicted of:

(1) transporting and aiding and abetting in the transport of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(1), 2252A(b)(1), and 2 (Count 1); and

(2) knowingly possessing materials containing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) (Count 2). The charges stemmed from Rivenbark's posting in an internet chatroom a Dropbox hyperlink that contained child pornography, which led to law enforcement's tracking him down and conducting a forensic search of his computer.

In his appeal, Rivenbark contends that: (1) the government did not present sufficient evidence to support his convictions; and (2) the district court's jury instruction on possession constructively amended his indictment and created a mandatory presumption that violated his due process rights. After careful review, we affirm.

I. BACKGROUND

Because defendant Rivenbark challenges the sufficiency of the evidence supporting his convictions, we start by outlining the trial evidence about the investigation that led to his arrest and the forensic examination of his laptop computer.

A. Detective Brad Gallant's Investigation

In August 2014, Detective Brad Gallant, with the York Regional Police in Ontario, Canada, led part of an investigation targeting the distribution and consumption of child pornography. As part of that investigation, Detective Gallant staked out chatrooms on a website called Chatzy, where previous investigations had uncovered the exchange of child pornography.

On August 19, 2014, Detective Gallant joined a particular chatroom named “Send and Share,” with a description that read, “Do not trade, this room is only meant for willing shares.” Detective Gallant observed the following exchange. One user, “Jackson,” stated “if you truly want to see little girl porn hit me up” and provided his username for another sharing application. A second user, “Dick6Inch,” offered to provide 10 links and asked others to click on them. A third user named “hrdgy2k00,” who was later identified as defendant Rivenbark, then posted a hyperlink to a Dropbox account.

Dropbox is a company that hosts an off-site virtual storage application based in California. After creating an account, users may place items in a Dropbox folder and then access them remotely through the application or, as in this case, by using a designated internet hyperlink. The hyperlink posted by hrdgy2k00 led to a folder entitled “Share For” and contained over 100 videos of child pornography.

Hrdgy2k00 asked the others in the chatroom to post more hyperlinks containing child pornography, stating: “anyone got more like that link? . . . that

actaly [sic] work.” Dick6Inch retorted that all of his hyperlinks worked, and hrdgy2k00 replied, “then post em pls.” Dick6Inch then posted a series of links and introduced them as “Free Pedo Boys and Girls Fucking Links.” “Pedo” is short for pedophile and denotes a sexual interest in children.

Detective Gallant screen captured the Chatzy conversation and the contents of the Dropbox account posted by hrdgy2k00. After reviewing a cross-section of the video content, Detective Gallant contacted Dropbox about who had created that account. Detective Gallant was not able to tie hrdgy2k00 to the creation of the Dropbox account.

But, Detective Gallant did determine that the internet protocol (“IP”) address for hrdgy2k00 originated in Oviedo, Florida.¹ From Canada, Detective Gallant forwarded his investigation materials to his liaison for the United States Department of Homeland Security (“DHS”), who then forwarded the materials to a DHS field office in Orlando, Florida.

B. DHS Investigation and Interview

The DHS field office in Florida submitted a subpoena request to the service provider associated with the IP address identified by Detective Gallant and found that the account was registered to David R. Rivenbark at 1008 Wainwright Drive, Oviedo, Florida.

¹An IP address is a temporary address that a computer uses to communicate with the internet.

On November 26, 2014, three DHS agents conducted an interview with Rivenbark at his home. The agents told Rivenbark that someone had posted hyperlinks to child pornography in a chatroom on Chatzy and that they had traced this activity to his address. According to the agents, Rivenbark calmly responded that he was familiar with Chatzy and that he had seen child pornography on that website before.

When the officers pressed further, Rivenbark admitted that he had used his personal laptop to view child pornography online. Rivenbark denied that he ever saved or downloaded any of this child pornography, but he also told the officers that he routinely used a computer program to delete information from his computer hard drives.

The DHS agents asked about the profile name hrdgy2k00, and Rivenbark claimed that he had used it previously on a dating website but did not use it to post hyperlinks on Chatzy. Rivenbark later confessed to being hrdgy2k00 from Chatzy and to posting the Dropbox hyperlink that he knew led to a folder containing videos of child pornography.

The agents asked him how long he had been looking at child porn. Rivenbark responded that he began while in college in the mid-1990s and that he was primarily interested in high-school-aged girls. Rivenbark admitted that he was sexually aroused by the images and that he had masturbated to them. When asked

if he had a problem, Rivenbark responded that he did not know why he had a “compulsion” for “young girls.”

Rivenbark gave the DHS agents permission to check his laptop and other devices. This initial search yielded no results, but the agents seized Rivenbark’s laptop and two external hard drives for further investigation. Near the end of the interview, the agents presented Rivenbark with a voluntary waiver containing his Miranda rights,² and he signed it. Rivenbark was not arrested that day.

C. Forensic Scan of Rivenbark’s Computer

A DHS forensic analyst later examined Rivenbark’s laptop computer and hard drives to check for child pornography.

At trial, the following facts were established about files on a computer. While browsing images on the internet, a user has the opportunity to download and save images at any time. Even if the user does not download or save images when visiting a web page, the computer automatically generates temporary internet files of the images and stores them in a cache. These cached files represent the images available to the user while he or she browses a particular page. This process assists the user by allowing that page to load faster if the user chooses to return to it.

Periodically—or when the user elects to do so—the temporary internet files are deleted from the cache. Deleted files go into unallocated space on the hard

²See Miranda v. Arizona, 384 U.S. 436, 86 S. Ct. 1602 (1966).

drive and reside there until they are overwritten or replaced by new information. Unallocated data is not accessible to the user without manipulation or the use of recovery tools on the system, but signifies a file that was present on the computer's allocated space at one time.

From the unallocated space on Rivenbark's laptop computer, the DHS forensic analyst recovered nearly 400 images of child pornography deleted from Rivenbark's temporary internet files. Among the files recovered, some were located in what the DHS analyst identified as the "pagefile," or the virtual memory file for the computer's operating system. These files, whether image or video, were portrayed as thumbnail images when saved in Rivenbark's temporary internet files.

The DHS forensic analyst also received video files recovered from the Dropbox account that Rivenbark posted on Chatzy. When viewed on the operating system, the videos from the Dropbox account were also portrayed as thumbnail images. The DHS analyst compared these thumbnails side by side and concluded that five of them were a visual match. Based on this information, the DHS analyst opined that Rivenbark had viewed these five videos from the Dropbox account on his laptop, which resulted in his computer's memory storing a cached image on his hard drive.

The DHS forensic analyst also reviewed Rivenbark's internet search history and discovered numerous search variations of the terms PTHC (meaning "pre-teen hard core"), "PTH C," PTSC (meaning "pre-teen soft core"), pre-teen, toddler, and daughter, along with various ages and sexually explicit phrases. Rivenbark also accessed chatroom and file-sharing websites associated with child pornography on numerous occasions and attempted over 50 times to access chatrooms that were closed for the exchange of child pornography.

D. Procedural History and District Court's Jury Instruction on Possession

At the close of the government's case-in-chief at trial, defendant Rivenbark moved for a judgment of acquittal, which the district court denied. He renewed his motion at the close of all evidence, and the district court denied it again.

Over Rivenbark's objection, the district court instructed the jury that "[k]nowingly possessing child pornography images includes intentionally viewing images sent to a defendant's computer from an outside source whether or not the viewer tries to save, edit or, otherwise, exert more control over the images," but that "inadvertent receipt of child pornography does not violate the statutes." (Emphasis added.)

The jury convicted Rivenbark on both counts. After trial, Rivenbark filed a written motion for judgment of acquittal, challenging: (1) the sufficiency of the

evidence supporting his convictions; and (2) the district court's jury instruction on possession. The district court denied this motion as well.

Applying the Sentencing Guidelines, the district court calculated an offense level of 40 and a criminal history category of I, which yielded an advisory guidelines range of 292 to 360 months' imprisonment. Ultimately, the district court sentenced Rivenbark to 240 months on Count 1 and 240 months on Count 2 to run concurrently. Rivenbark does not appeal any advisory guidelines calculations or the reasonableness of his sentence. Rather, Rivenbark appeals his convictions.

II. SUFFICIENCY OF THE EVIDENCE AS TO TRANSPORTATION

We review de novo the sufficiency of the evidence supporting a criminal conviction, viewing all evidence in the light most favorable to the government and drawing all reasonable inferences and credibility choices made in the government's favor. United States v. Pruitt, 638 F.3d 763, 765 (11th Cir. 2011).

The indictment charged Rivenbark in Count 1 with knowingly transporting and aiding and abetting the transportation of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(1) and 2.

Under § 2252A(a)(1), it is illegal to “knowingly transport[]” child pornography “using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.”

18 U.S.C. § 2252A(a)(1). Under 18 U.S.C. § 2, an individual who aids and abets a crime may be punished as a principal to that crime. See United States v. Hornaday, 392 F.3d 1306, 1313 (11th Cir. 2004) (explaining aiding and abetting as a situation where “a defendant with the requisite intent to commit a crime gets someone [or something] else to act in a way necessary to bring about the crime, even if that other person [or entity] is innocent”). Aiding and abetting requires the government to prove: (1) a third party committed the substantive offense; (2) the defendant committed an act that contributed to and furthered the offense; and (3) the defendant intended to aid in the commission of the offense. United States v. Cruickshank, 837 F.3d 1182, 1189 (11th Cir. 2016); see 18 U.S.C. § 2.

A. Transportation of “Child Pornography”

On appeal, Rivenbark argues that the government failed to prove substantive transportation of child pornography under § 2252A(a)(1) because the hyperlink that Rivenbark posted on Chatzy was not itself child pornography. Put differently, Rivenbark claims that the only thing he “transported” was a hyperlink, which was not technically child pornography. Since that hyperlink does not meet the statutory definition for child pornography, Rivenbark claims he did not commit a substantive violation of § 2252A(a)(1).

The problem for Rivenbark is that he was also charged in Count 1 with aiding and abetting the transportation of child pornography. Under that theory, the

government did not need to prove that Rivenbark actually transported the child pornography himself. Rather, to establish that Rivenbark aided and abetted transportation, the government had to prove that Rivenbark took an affirmative step to induce an unknowing third party—namely, Dropbox—to transport the images or videos of child pornography over the internet. The record evidence established these facts.³

Dropbox provides off-site virtual storage over the internet. The contents of a Dropbox account can be shared by hyperlink, which provides immediate access to anyone who clicks on it. The Dropbox account in this case contained over 100 videos of child pornography within a folder entitled “Share For.” With knowledge of the contents of this particular Dropbox account, Rivenbark posted a hyperlink to this Dropbox account on a Chatzy chatroom designated for the exchange of child pornography. By doing so, Rivenbark caused and facilitated Dropbox’s software to be used for the transportation of child pornography over the internet.

Although we need not address it here, crediting Rivenbark’s technical argument about the hyperlink versus actual pornography would permit individuals sharing child porn to avoid prosecution simply by using third-party virtual storage

³Rivenbark’s reliance on United States v. Navrestad, 66 M.J. 262 (C.A.A.F. 2008), is misplaced. In Navrestad, the United States Court of Appeals for the Armed Forces concluded that sending a hyperlink to a digital-storage site containing child pornography did not constitute distribution of child pornography. 66 M.J. at 266–67. However, the Navrestad court also noted that the government had not charged the defendant under an aiding-and-abetting theory or any sort of attempt liability. Id.

to remain one step removed from the illicit materials. It is the difference between providing a location for pickup and handing over the materials directly. In any event, Rivenbark provided access to and facilitated the transportation of child pornography by placing the Dropbox hyperlink in that particular chatroom on Chatzy. We conclude that there was sufficient evidence for the jury to find that Rivenbark aided and abetted in the transportation of child pornography. See 18 U.S.C. § 2.

B. Intent to Aid and Abet Transportation

Rivenbark also argues that the government failed to prove he intended to aid and abet the transportation of child pornography because the government did not show that he specifically intended the other Chatzy users to transport child pornography from one location to another. In the context of aiding and abetting, the defendant's intent "must go to the specific and entire crime charged." Rosemond v. United States, 572 U.S. 65, 76, 134 S. Ct. 1240, 1248 (2014). So, Rivenbark is correct that the government was required to prove he intended others to transport the pornography across the internet. However, the record evidence here demonstrates that intent.

Rivenbark not only posted a Dropbox hyperlink to a massive collection of child pornography but he also did so in an internet chatroom created for the purpose of exchanging and sharing such materials. Rivenbark had full knowledge

that the other users in this chatroom would not only view the videos that he shared but also transfer and save them to their own devices and private collections. The name and description of the chatroom suggested that users “Send and Share” their collections of child pornography and that the chatroom was “only meant for willing shares.” Similarly, the folder contained in the Dropbox hyperlink was entitled “Share For.” From this evidence, the jury could reasonably find that Rivenbark anticipated and intended the other users—which included Detective Gallant with the York Regional Police in Ontario—to save and transport the posted materials.

Further, the conversation in this chatroom made it very clear what the users, and specifically what Rivenbark, sought to share. After posting the Dropbox hyperlink using the profile name hrdgy2k00, Rivenbark asked the other users if “anyone got more like that link?” (Emphasis added.) The import of this statement is two-fold: (1) Rivenbark implicitly asked the other users to click and view his hyperlink to determine “like” or similar content; and (2) he explicitly asked the other users to post similar hyperlinks containing child pornography. Viewed in the light most favorable to the government, the evidence supports the jury’s conclusion that Rivenbark intended to aid and abet the transportation of child pornography.

III. SUFFICIENCY OF THE EVIDENCE AS TO POSSESSION

The indictment charged Rivenbark in Count 2 with knowingly possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Under § 2252A(a)(5)(b), it is illegal to “knowingly possess[], or knowingly access[] with intent to view, any . . . image of child pornography that has been . . . transported using any means or facility of interstate or foreign commerce . . . by any means, including by computer.” 18 U.S.C. § 2252A(a)(5)(B).

On appeal, Rivenbark argues that he did not “possess” the images of child pornography located in his temporary internet files because these images were saved on his computer by the automatic operation of his internet browser. Rivenbark also argues that the government failed to prove that he knew the images were located on his computer.

Rivenbark’s arguments are red herrings at best. Under this Court’s precedent in United States v. Woods, 684 F.3d 1045 (11th Cir. 2012), “a person who intentionally views, but does not download, child pornography necessarily ‘possesses’ child pornography within the meaning of § 2252A(a)(5)(B).” Id. at 1059 (emphasis added); see 18 U.S.C. § 2252A(a)(5)(B). While sufficiency of the evidence was not at issue in Woods, its holding as to possession under § 2252A(a)(5)(B) nonetheless controls. Compare Pruitt, 638 F.3d at 767 (analyzing sufficiency of the evidence as to receipt and holding that a person “knowingly receives” child pornography by “intentionally viewing” it), with

Woods, 684 F.3d at 1059 (applying “viewing” principle from Pruitt to possession of child pornography under § 2252A(a)(5)(B)).

There is no dispute that Rivenbark intentionally viewed child pornography. The record evidence shows that Rivenbark sought out these images and videos in numerous ways and over the course of many years. In the Chatzy chatroom, for example, Rivenbark posted the Dropbox hyperlink containing over 100 videos of child pornography and then asked the other users to “pls” post more hyperlinks to child pornography.

Aside from his conduct on Chatzy, Rivenbark admitted to DHS agents that he had begun looking at child pornography in the mid-1990s and that he was primarily interested in high-school-aged girls. He also admitted that he was sexually aroused by images of child pornography, that he masturbated to them, and that he did not know why he had a “compulsion” for “young girls.” Rivenbark acknowledged that he viewed child pornography on his laptop computer and that he routinely used a computer program to delete information, including the child pornography, from his hard drives. Based on this evidence, the jury could have reasonably inferred that Rivenbark was sophisticated in technology and that his long history of viewing child pornography made him develop this system of viewing and then deleting images of child pornography to avoid detection.

Moreover, DHS's forensic analyst uncovered nearly 400 deleted images of child pornography in the unallocated space on Rivenbark's laptop. The analyst also found that Rivenbark would regularly conduct internet searches on his laptop computer using a broad range of sexually explicit terms associated with child pornography. Among other things, Rivenbark sought over 50 times to access chatrooms that were closed due to the exchange of child pornography.

Notably too, DHS's forensic analyst also opined that, based on thumbnail images recovered from the unallocated space on Rivenbark's laptop, Rivenbark viewed at least five videos of child pornography from the Dropbox account he posted on Chatzy. While viewing these and other videos or images online, Rivenbark had the ability to save, copy, print, screen capture, and email them to other people. See Woods, 684 F.3d at 1059.

When viewed in the light most favorable to the government, and consistent with this Court's opinion in Woods, the record evidence supports the jury's conclusion that Rivenbark knowingly possessed child pornography. Accordingly, the district court correctly denied Rivenbark's motion for judgment of acquittal as to both counts in the indictment.

IV. JURY INSTRUCTIONS

A. Constructive Amendment

Rivenbark next argues that the district court’s jury instruction on possession constructively amended his indictment by adding that possession included “intentionally viewing images.” Specifically, Rivenbark contends that the district court’s jury instruction merged “possession” with “access with intent to view” under § 2252A(a)(5)(B) and thus constructively amended his indictment.

“A constructive amendment to the indictment occurs where the jury instructions so modify the elements of the offense charged that the defendant may have been convicted on a ground not alleged by the grand jury’s indictment.” United States v. Sanders, 668 F.3d 1298, 1309 (11th Cir. 2012); see United States v. Gutierrez, 745 F.3d 463, 473 (11th Cir. 2014); United States v. Keller, 916 F.2d 628, 634 (11th Cir. 1990). This Court reviews whether jury instructions constructively amended the indictment de novo. Gutierrez, 745 F.3d at 473.

Section 2252A(a)(5)(B) criminalizes both “possession” of and “access[ing] with intent to view” child pornography. See 18 U.S.C. § 2252A(a)(5)(B). Count 2 of Rivenbark’s indictment specifically charged that Rivenbark “did knowingly possess” images containing child pornography in violation of § 2252A(a)(5)(B). (Emphasis added.) The indictment did not charge that he accessed them with the intent to view.

The statute does not define “possession,” and this Court’s Pattern Jury Instructions simply list and identify different types of legal possession, including

actual, constructive, sole, and joint. See id.; Eleventh Circuit Pattern Jury Instructions (Criminal Cases) S6 (2016). However, this Court in Woods concluded that possession “necessarily” includes intentionally viewing child pornography, even if it is never downloaded. 684 F.3d at 1059 (“[A] person who intentionally views, but does not download, child pornography necessarily ‘possesses’ child pornography within the meaning of § 2252A(a)(5)(B).”).

Consistent with Woods, the district court’s jury instruction made clear that, in this digital age, possession can include the completed act of “intentionally viewing images,” which is different than having access and intent to view images but not actually viewing them. See 684 F.3d at 1059. The key distinction is that, to establish possession in this case, the government had to prove that Rivenbark actually viewed the child pornography. See Woods, 684 F.3d at 1059. By contrast, under the “access with intent to view” prong, the government had no such burden. The district court’s instruction on “possession” of child pornography was consistent with the law of our Circuit, reflected the substance of the indictment, and did not amount to a constructive amendment.

B. Mandatory Presumption

Lastly, Rivenbark argues that this same jury instruction on possession created a mandatory presumption in favor of the government as to the element of possession under § 2252A(a)(5)(B).

“A jury instruction which creates a burden shifting presumption or a conclusive presumption deprives a defendant of his right to the due process of the law.” United States v. Dean, 517 F.3d 1224, 1231 (11th Cir. 2008) (citing Sandstrom v. Montana, 442 U.S. 510, 524, 99 S. Ct. 2450, 2459 (1979)). We review the correctness of a jury instruction and its propensity to mislead the jury *de novo*. Palmer v. Bd. of Regents of the Univ. Sys., 208 F.3d 969, 973 (11th Cir. 2000).

In this case, the district court’s jury instruction that possession included “intentionally viewing images” did not create a mandatory presumption as to possession. As discussed above, the district court’s instruction was consistent with the law of this Circuit, and the government was still required to prove beyond a reasonable doubt that Rivenbark intentionally viewed the images of child pornography. See Woods, 684 F.3d at 1059. Just because Rivenbark admits that he is a long-time viewer of child pornography does not mean that his due process rights were violated when the government used that fact against him at trial.

V. CONCLUSION

For all of these reasons, we affirm Rivenbark’s convictions.

AFFIRMED.