United States Court of Appeals for the Fifth Circuit

United States Court of Appeals
Fifth Circuit
FILED
June 16, 2023
Lyle W. Cayce
Clerk

No. 22-20216

UNITED STATES OF AMERICA,

Plaintiff—Appellee,

versus

GREGORY EUGENE BAKER,

Defendant—Appellant.

Appeal from the United States District Court
for the Southern District of Texas
USDC No. 4:20-CR-612-1

Before JONES, CLEMENT, and HAYNES, *Circuit Judges*.

PER CURIAM:[*]

Gregory Baker brings this appeal after a jury found him guilty of receiving child pornography in violation of 18 U.S.C. § 2252A(b)(1) and possessing child pornography in violation of 18 U.S.C. § 2252A(b)(2). The evidence against him supports these charges, and his legal challenges are foreclosed. Therefore, we AFFIRM.

[*] Pursuant to 5th Circuit Rule 47.5, the court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5th Circuit Rule 47.5.4.

I. Background

Officer Bruce Moats was an investigator for the Fort Bend County District Attorney. He specializes in forensic computer analysis. During the investigation that led to this case, he was assigned to the Houston Metro Internet Crimes Against Children Task Force and worked undercover to detect child pornography on Freenet, a dark web platform where people can share files.

Freenet is designed to provide anonymity and circumvent censorship. To that end, it operates as a "closed-loop" network, meaning that users only communicate with other computers that are also on the network. To find and download files on Freenet, users need a "check key"—analogous to a URL. Users enter a check key into Freenet, and the Freenet program then attempts to retrieve the file associated with that check key.

Freenet conceals the files it stores by disassembling and dispersing them. When Freenet stores a file, it first breaks the file into hundreds or thousands of different "blocks," encrypts those blocks, and then saves them on devices that use Freenet, such that no single device contains all the blocks necessary to reassemble the file. A user whose device stores some of the blocks is unaware of their presence, and he or she is not able to determine the nature of the file based on the blocks alone.

Accessing these files requires finding and reassembling them. The process begins when a user enters the check key for a particular file into Freenet. Then, their computer sends a request for blocks associated with that file to the Freenet-using devices to which it is connected. If those devices do not have those blocks, they relay the request to other devices. Besides the initial user who entered the check key, none of the users whose devices are involved in this sequence are aware that their computers are relaying these requests; their computers conduct the search passively. The

request is relayed 17 or 18 times before the search terminates. In some cases, Freenet will not be able to assemble the file after the search.

This process leaves clues as to which device began the search for a particular file. To ensure that the search terminates after 17 or 18 relays, each request is assigned a different "hops to live (HTL) value." The request that starts the search typically has an HTL value of 18 or 17, and subsequent requests will have lower numbers. Because it is far more likely that a request with a high HTL value began the search, investigators like Officer Moats will disregard suspicious requests with HTL values lower than 17.

In July 2018, Officer Moats noticed that an IP address geolocated in Sugar Land, Texas, had recently sent 13 requests on Freenet using check keys known to be associated with child pornography. All 13 requests had HTL values of 18 or 17. However, he was not able to determine whether the requests had successfully assembled the files, or whether the requestor had downloaded them. To verify the content of the files, Officer Moats entered the same 13 check keys into Freenet, which successfully assembled 11 out of the 13. He confirmed that those 11 files contained child pornography.

Officer Moats subpoenaed Comcast, which owned and serviced the IP address, to learn the identity of the subscriber associated with the address. The subpoena response revealed that Gregory Baker—a software engineer living in Sugar Land, Texas—was the subscriber. Law enforcement obtained a warrant and searched Baker's home in April 2019. They seized 32 devices containing 12,762 images and 380 videos of child pornography during the search. Freenet was installed on several of these devices. Most of the child pornography had been deleted and moved to unallocated space on the devices' hard drives. Two of the images and one of the videos were identical to files that Officer Moats had found when he entered the suspicious check keys into Freenet. Additionally, six other files—no longer accessible, but

with titles associated with child pornography—indicated they had been downloaded between January and May 2018.

On November 18, 2020, a grand jury indicted Baker with one count of receiving child pornography in violation of 18 U.S.C. § 2252A(b)(1) (on or about July 27, 2018, the day the suspicious activity on Freenet came from Baker's IP address) and one count of possessing child pornography in violation of 18 U.S.C. § 2252A(b)(2) (on or about April 4, 2019, the day of the search). The statute of limitations for both offenses is five years. 18 U.S.C. § 3282. Baker pleaded not guilty.

At trial, after the government closed, Baker moved for an acquittal under Rule 29 of the Federal Rules of Criminal Procedure. His attorney argued that the government had not shown that Baker received child porn on or about July 27, 2018. According to him, "there were no dates associated with those files that were found on any of these devices. So there wasn't any evidence that they came as a result of what was going on, any downloads on July 2018." The court asked, "Do I have anything, any document, that show [sic] the receipt . . . anytime on or about July of 2018?" Baker's lawyer replied, "No, you don't." Later, Baker's lawyer again stated that "there is [sic] no dates associated with whatever files these are." The court denied the motion, acknowledging that the prosecution had no direct evidence of receipt in July 2018, but ruling that the circumstantial evidence was sufficient to overcome the motion. Baker renewed the motion after the jury retired, and the court again denied it.

The jury found Baker guilty on both counts. The judge sentenced him to 90 months' imprisonment for each offense, to run concurrently for a total of 90 months' imprisonment. Baker appealed.

II. Discussion

Baker brings three challenges to his conviction. *First*, he argues that there was insufficient evidence that he received child pornography within the statute of limitations period. *Second*, he argues that there was a material variance that affected his substantial rights between the evidence presented at trial and the dates given in the indictment. *Third*, he argues that the statute of conviction is unconstitutionally vague. Each challenge fails.

A. Statute of Limitations

Baker's statute of limitations argument is based on a misapprehension of the law. In their initial briefs, both parties agreed that the general five-year statute of limitations for noncapital offenses found in 18 U.S.C. § 3282(a) applies to this case. However, as the government belatedly pointed out in a Rule 28(j) letter to this court, there has been no statute of limitations for the receipt of child pornography since the Adam Walsh Child Protection and Safety Act of 2006. 18 U.S.C. § 3299. Baker makes no attempt to show that the child pornography at issue here was received before the passage of the Act, and the facts outlined above provide ample support for the opposite conclusion. Thus, Baker's challenge is foreclosed by statute.

B. Material Variance

When a defendant raises a preserved claim that the evidence presented at trial varies from the terms of his indictment, the claim is reviewed for harmless error. *United States v. Ekanem*, 555 F.3d 172, 174 (5th Cir. 2009). That means he "must show that the variance was material and prejudiced his substantial rights." *Id.* However, if the claim is not preserved, it is reviewed for plain error. *United States v. Perez-Solis*, 709 F.3d 453, 465 (5th Cir. 2013).

Harmless error review applies. Baker argued at trial that the evidence varied from the terms of his indictment. Nevertheless, the government contends that plain error review should apply because Baker never responded to their counterargument that (1) the six files mentioned above had dates from the first half of 2018, and (2) those dates did not materially vary from the July 27 date charged in the indictment. But this court's precedent establishes that a defendant need only "raise his material variance objection at trial" to preserve the claim; he is not obligated to counter the prosecution's counterarguments. *United States v. Meza*, 701 F.3d 411, 423 (5th Cir. 2012).

Regardless of the standard of review, Baker's variance claim fails. "An allegation as to the time of the offense is not an essential element of the offense charged in the indictment, and, within reasonable limits, the offense need only occur before the return of the indictment and within the statute of limitations." *United States v. Valdez*, 453 F.3d 252, 259–60 (5th Cir. 2006) (brackets and quotation marks omitted). The evidence at trial sufficiently proved that Baker received three files containing child pornography from Freenet on July 27, 2018. As stated above, all thirteen of the requests from Baker's IP address had HTL values of 17 or 18. Relying on the testimony of Officer Moats, the jury could have therefore concluded that there was "a high likelihood" that the searches originated with Baker. Combined with the fact that three of the files were later discovered on his devices, the evidence supports a finding that there was no variance from the dates alleged in the indictment.

The government also showed that Baker received other files containing child pornography around the same time. During the search of Baker's home, police seized a hard drive belonging to Baker containing six timestamped files. The timestamps indicated the files were downloaded between January 12 and May 23, 2018. Each had titles consistent with child

pornography. A government witness testified that two of these titles were recognizable labels for popular series of child pornography. These six files from the first half of 2018 were received (1) "before the return of the indictment," (2) "within the statute of limitations," and (3) "within reasonable limits." *Id.* Only the third requirement is arguable here, but this court has found similar variances to be reasonable. *United States v. Girod*, 646 F.3d 304, 316 (5th Cir. 2011) (four months); *United States v. Wilson*, 116 F.3d 1066, 1089 (5th Cir.) (five months), *rev'd on other grounds by sub nom. United States v. Brown*, 161 F.3d 256 (5th Cir. 1998) (en banc).

Baker has also failed to show that any variance "prejudiced" or "affected" his substantial rights. *Ekanem*, 555 F.3d at 174; *Meza*, 701 F.3d at 423. His prejudice argument hinges on the proposition that it violates the Double Jeopardy Clause to convict him for both receiving and possessing the same child pornography, "since the possessing provision does not require[] proof of any fact that the receiving provision does not." *United States v. Ehle*, 640 F.3d 689, 694 (6th Cir. 2011) (relying on the test set forth in *Blockburger v. United States*, 284 U.S. 299, 52 S. Ct. 180 (1932)); *see also United States v. Miller*, 527 F.3d 54, 72 (3d Cir. 2008); *United States v. Davenport*, 519 F.3d 940, 947 (9th Cir. 2008). Baker claims that the jury could have relied on the government's evidence regarding any of the roughly 12,000 images and 300 videos of child pornography to support the possession conviction. Therefore, he argues, to exclude the possibility that he is being convicted for receiving the same files that he was convicted for possessing, the government can only rely on evidence regarding the Freenet files allegedly received on July 27.

This court need not decide the constitutional question because Baker's factual premise is false. His possession indictment was solely for child pornography contained on a Fujitsu hard drive, serial number K617T8325W0B. The six files from the first half of 2018 were contained on

a Samsung M.2 hard drive. Therefore, his two convictions rely on separate child pornography files, regardless of whether the reception conviction is supported by the files from July 27 or the files from the first half of 2018.

C. Void for Vagueness

Baker's final argument is foreclosed by precedent. He argues that there is "no rational difference between the acts of receiving and possessing child pornography," and that therefore the statutes of his conviction are unconstitutionally vague. But as he concedes, this court has already ruled otherwise in *United States v. Ross*, 948 F.3d 243, 247 (5th 2020) ("[The] claim that possession and receipt are logically inseparable conduct, and that, as a result, § 2252A's criminalizing both invites unconstitutionally arbitrary enforcement, is incorrect.").

III. Conclusion

For the foregoing reasons, the judgment of the district court is AFFIRMED.