IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 18-10580

United States Court of Appeals
Fifth Circuit
FILED
August 15, 2019
Lyle W. Cayce
Clerk

UNITED STATES OF AMERICA,

Plaintiff - Appellee

v.

HUGH MICHAEL GLENN,

Defendant - Appellant

Appeal from the United States District Court
for the Northern District of Texas

Before HAYNES, GRAVES, and DUNCAN, Circuit Judges.

JAMES E. GRAVES, JR., Circuit Judge:

Hugh Michael Glenn appeals his conviction for one count of transporting and shipping child pornography in violation of 18 U.S.C. §2252A(a)(1) and one count of accessing child pornography with intent to view it in violation of 18 U.S.C. § 2252(a)(4). Finding no error in the proceedings below, we affirm.

I. BACKGROUND

A. Government Obtains a Warrant and Seizes Glenn's Computer

On or about August 30, 2016, the Dallas Police Department ("DPD") received a "cyber tip" from the National Center for Missing and Exploited Children ("NCMEC"). NCMEC informed the DPD that Chatstep, "an anonymous online chatting platform," had reported that someone with the

username "TexPerv" uploaded an image of a prepubescent male exposed in a lewd and lascivious manner to its site on August 1, 2016. According to Chatstep, the user had also accessed several chat rooms with names signaling a sexual interest in children, including "UdnreraegAvction," "byyyrooom," and "UdneraegHvmiliation."

DPD Detective Chris De Leon issued an administrative subpoena to AT&T for the subscriber information linked to the IP address in the cyber tip. AT&T's records showed Hugh Michael Glenn as the subscriber for the designated IP address. After running a search on Glenn's telephone number, DeLeon found Glenn listed as a registered sex offender with a prior federal conviction for transporting and shipping child pornography. DeLeon began surveilling the address listed on the sex offender registry and the AT&T documents; in doing so, he observed a UPS package on the doorstep addressed to Hugh Glenn.

On or about September 8, 2016, DeLeon contacted Agent Jennifer Mullican, a member of the FBI's Child Exploitation Task Force, for assistance. Based on the information Mullican collected from DeLeon, including the AT&T records, Mullican sought a warrant to search the residence of 3500 Routh for computer equipment and electronic material. In her affidavit in support of the warrant, Mullican listed 3500 Routh St as the address where Glenn was receiving internet service on August 1, 2016, the date the child pornography image was uploaded to Chatstep. However, the AT&T documents actually showed Glenn was receiving internet service at 3025 West Forest on August 1st; he transferred his billing address to 3500 Routh St on August 2nd and began service at Routh St on August 9th. Because Chatstep reported the pornography was uploaded on August 1st, Glenn could not have uploaded the picture from 3500 Routh, as Mullican's affidavit stated. Accordingly,

Mullican's statement in the affidavit about where the upload likely occurred was incorrect.

The mistake went unnoticed and the magistrate judge issued a warrant to search the Routh St address. Officers executed the search warrant on September 14, 2016. Glenn was present at the time of the search and agreed to speak with law enforcement, waiving his *Miranda* rights. During this interview, Glenn admitted that he visited Chatstep, that he was user TexPerv, and that he had downloaded and uploaded child pornography. He also acknowledged that the officers would find child pornography on his laptop. Glenn admitted he had seen the specific image referenced in the cyber tip, and although he said he did not remember sharing the image, he also stated, "Umm, I obviously saved [the image] if I sent it out." Glenn signed and dated the back of the image.

While Mullican was interviewing Glenn, FBI computer scientist Anthony Lehman performed an initial triage of Glenn's laptop to determine if the computer was encrypted and to see if he could uncover any information helpful to the officers as they interviewed Glenn. Lehman used a software program "to do a quick analysis" of the computer's "allocated space," and he used a different program to recover deleted files from the hard drive's "unallocated space."[1] These searches were consistent with FBI protocol. Lehman's searches of Glenn's computer at the scene recovered many images of child pornography in both the allocated and unallocated spaces.

[1] "Allocated space" is space on a hard drive dedicated to storing files used or saved by the user so they can be accessed at a later time. After a file is deleted, it is stored in a hard drive's "unallocated space" until the hard drive is either permanently wiped using special software or the files are overwritten by other actions of the user. A user generally cannot access files in the unallocated space of the hard drive without special software, which Glenn did not have.

B. Glenn's Computer Installs Update in Government Custody

While back at the laboratory after the execution of the search warrant, Lehman attempted to create an "image"[2] of the hard drive before the agents searched it further. In accordance with FBI procedures, Lehman removed the hard drive from the computer and tried to image it. However, the hard drive had a "non-standard" connector that was proprietary to its manufacturer and Lehman ran into several issues, requiring multiple attempts to image the drive.

Lehman sought help from his colleagues, but nobody had "seen this type of hard drive." He tried again using a different software program, but that attempt also failed. Lehman then tried two more times, once from a CD and once from a USB drive. Importantly, when Lehman attempted to run a program from the USB drive, the computer "didn't boot to the USB" as Lehman expected it would. Instead, "it tried to start up Windows," and Lehman "powered off the machine."

When Glenn's computer "tried to start up Windows," updates installed automatically onto the hard drive.[3] Although the update did not affect the "thumb cache"[4] of the computer—which contained numerous images of child pornography—one of the updates was a defrag.exe process that reallocated information on the drive so that data could be written more efficiently. Lehman

---

[2] In this context, an image of a hard drive is "an identical copy of [the] hard drive."

[3] A Windows update proceeds in two steps: the updates are downloaded onto the computer either automatically or by the user; and then the user can either install the updates immediately by restarting the computer or they will automatically install the next time the computer is restarted. The updates on Glenn's laptop had automatically downloaded to Glenn's computer the day before the execution of the search warrant; however, because Glenn had not restarted his computer, the updates had not yet been installed. It is undisputed that the Windows update did not contain images of child pornography.

[4] A "thumb cache" is a database file that "basically stores every picture that you have knowingly opened on the computer" to help files load faster when they are opened subsequently. The thumb cache is located in the allocated space on the hard drive.

testified that the defrag did not "completely actually run" and he "did not purposefully execute defrag.exe." Glenn contends that the update destroyed at least ten gigabytes of data in the unallocated space of his hard drive.

Eventually, Lehman was able to image the hard drive. All of the information about Lehman's attempts to image Glenn's hard drive, including the Windows update, was logged in the computer's registry. Lehman was supposed to write a "302 report" summarizing his efforts to image Glenn's hard drive, but Lehman failed to make his 302 report until about five months before trial. Lehman testified that this delay was an "oversight" because he "thought that [he] had written it" earlier.

Glenn's computer expert, Brian Ingram, was so disturbed by Lehman's failures that he brought them to the attention of the FBI. However, Ingram confirmed that he had no reason to doubt that 2,000 images of child pornography were on Glenn's computer before the FBI took custody of the computer. Additionally, Tom Petrowski, Division Counsel for the FBI, testified that Ingram said he thought Glenn was "guilty as sin."

After the hard drive was imaged, Mullican reviewed it. She located numerous images of child pornography—including the image referenced in the cyber tip—on Glenn's hard drive. Mullican also found explicit stories on the hard drive that depicted "the sexual exploitation of minor boys."

C. Pretrial Proceedings, the Trial, and Sentencing

Glenn was charged in a superseding indictment with one count of transporting and shipping child pornography in violation of 18 U.S.C. § 2252A(a)(1) and one count of accessing child pornography with intent to view it in violation of 18 U.S.C. § 2252(a)(4). Count 1 related to the image user TexPerv uploaded to Chatstep on August 1; Count 2 related to four images found in Glenn's thumb cache.

Glenn moved to suppress the evidence obtained during the search once it came to light that Mullican's affidavit incorrectly stated Glenn's address was Routh St at the time the image was uploaded to Chatstep. No one contested that Mullican's affidavit supporting the warrant contained a false statement, and the district court judge therefore conducted an evidentiary hearing in accordance with *Franks v. Delaware*, 438 U.S. 154 (1978). After asking Mullican a number of questions, the district court denied the motion to suppress, finding her testimony credible and concluding that her failure to state the correct address "simply was a mistake."

Glenn also moved to dismiss the indictment "due to prosecutorial misconduct" because Lehman allowed the computer to reboot in his custody, which triggered the installation of the Windows update and defrag program, resulting in at least ten gigabytes of destroyed data. The district court carried the motion to dismiss with the case so that it could hear live testimony from both Lehman and Glenn's computer experts, but it indicated that it was unlikely to grant the motion.

During trial, Mullican testified that she found numerous images of child pornography on Glenn's computer, including the image uploaded to Chatstep. Glenn objected, arguing that Mullican was not an expert in "hash values" used to identify specific images, nor was she an expert in the program used to find the illicit images on Glenn's computer. The district court overruled the objection and admitted the images into evidence. After trial, the district court denied Glenn's motion to dismiss. It also denied Glenn's request for a spoliation of the evidence instruction because it found that there was "not sufficient evidence of bad faith." The jury convicted Glenn on both counts of the indictment. The district court sentenced Glenn to a total of 360 months of imprisonment.

Glenn timely appealed.

II. DISCUSSION

Glenn raises four issues on appeal to challenge his convictions. He does not challenge his sentence. We address each of his arguments in turn.

A. Motion to Dismiss for Prosecutorial Misconduct

Glenn first argues that the district court erred by denying his motion to dismiss. He bases this argument on two different legal theories: 1) the Government suppressed exculpatory evidence under *Brady v. Maryland*, 373 U.S. 83 (1963), and 2) the Government failed to preserve exculpatory evidence under *Arizona v. Youngblood*, 488 U.S. 51 (1988). As the Government observes, each argument is based on the same facts: primarily that while Glenn's laptop was in Government custody, the Windows update "destroyed" at least ten gigabytes of data in the unallocated space, and the Government did not specifically communicate this fact to Glenn prior to trial. Glenn contends he is entitled to dismissal of the indictment with prejudice on these bases.

1. Standard of Review

"We generally review whether the government violated *Brady de novo*, although even when reviewing a *Brady* claim *de novo*, we must proceed with deference to the factual findings underlying the district court's decision[.]" *United States v. Cessa*, 861 F.3d 121, 128 (5th Cir. 2017) (quoting *United States v. Brown*, 650 F.3d 581, 589 (5th Cir. 2011) (internal quotation marks and citations omitted)). "We review a district court's bad-faith determination for clear error." *United States v. McNealy*, 625 F.3d 858, 868–69 (5th Cir. 2010). While this court has not "foreclose[d] the possibility that governmental ineptitude and carelessness could be so abhorrent as to warrant a dismissal with prejudice," *United States v. Fulmer*, 722 F.2d 1192, 1196 (5th Cir. 1983), "mere error or oversight is neither gross negligence nor intentional misconduct." *United States v. Swenson*, 894 F.3d 677, 684 (5th Cir.) (quoting

United States v. Fulmer, 722 F.2d 1192, 1195 (5th Cir. 1983) (internal quotations omitted)), *cert. denied,* 139 S. Ct. 469 (2018).

2. *Brady* Argument

"To establish a *Brady* violation, a defendant must show: (1) the evidence at issue was favorable to the accused, either because it was exculpatory or impeaching; (2) the evidence was suppressed by the prosecution; and (3) the evidence was material." *United States v. Dvorin*, 817 F.3d 438, 450 (5th Cir. 2016). Bad faith is irrelevant to whether the Government has met its obligations under *Brady*. *See Youngblood*, 488 U.S. at 57. Both Glenn and the Government discuss all three elements of the *Brady* analysis; however, we find that Glenn cannot show the overwritten data was material. Accordingly, we do not address the first two elements.

"Evidence is material if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different." *Dvorin*, 817 F.3d at 451 (quoting *Brown,* 650 F.3d at 588 (internal quotation marks omitted)). Stated differently, the favorable evidence must "put the whole case in such a different light as to undermine confidence in the verdict." *Banks v. Dretke*, 540 U.S. 668, 698 (2004) (quoting *Kyles v. Whitley*, 514 U.S. 419, 435 (1995)).

Glenn cannot show that, had he had access to the overwritten data, the outcome of the trial would have been different. As for the uploaded image that was the subject of Count I, Glenn admitted having seen the uploaded image, and while he told Mullican he did not remember sharing the image, he later stated, "Umm, I obviously saved [the image] if I sent it out." Taken together with the facts that Glenn admitted to being user "TexPerv," he signed and dated the back of the image, and that the only other person to have had access to his computer was confirmed to have been at work on the date of the upload, there is little likelihood that the overwritten data would have changed the

outcome of this case, even assuming it had some exculpatory or impeachment value.[5] As to the four images that made up Count II, Glenn's own expert agreed that the Windows update would not have moved files in Glenn's thumb cache. Moreover, Glenn told Mullican she would find child pornography on his computer. Consequently, Glenn's *Brady* arguments are without merit.

3. *Youngblood* Claim

Unlike *Brady*, where the good or bad faith of the officer is irrelevant, *Youngblood* establishes that "the Due Process Clause requires a different result when we deal with the failure of the State to preserve evidentiary material of which no more can be said than that it . . . *might* have exonerated the defendant." *Youngblood*, 488 U.S. 57 (emphasis added). Glenn states several times that the overwritten data included metadata that had "potentially exculpatory" value, but also argues that the "evidence was of critical importance to the case and had exculpatory value." We agree that the overwritten data was at most possibly exculpatory, and therefore Glenn must show the district court clearly erred in determining the Government did not engage in bad faith in overwriting the data. *See McNealy*, 625 F.3d at 868–69 (concluding "potentially available" exculpatory evidence "should be considered 'potentially useful evidence' rather than 'material exculpatory evidence.'").

The district court concluded, albeit in the context of a spoliation instruction, that Lehman's actions in allowing the Windows update to install were at most negligent. This is not clear error, especially where the district court waited to rule on Glenn's motion until hearing testimony both from Glenn's computer expert and from Lehman regarding his actions leading to the overwritten data. *See United States v. Anderson*, 755 F.3d 782, 791 (5th Cir.

[5] To the extent Glenn implied at oral argument that the Government may have intentionally placed the images on Glenn's computer, there is simply nothing in the record to support such a contention.

2014) ("[W]e defer to the district court's credibility determination . . . ."). Glenn's *Youngblood* claim is therefore without merit.

B. Spoliation Instruction

Glenn next argues that the district court erred by denying his request for a spoliation instruction regarding Lehman's failure to stop the Windows update on his computer. We review the district court's denial of such an instruction for abuse of discretion. *United States v. Valas*, 822 F.3d 228, 239 (5th Cir. 2016).

To receive a spoliation instruction, Glenn had to show that the Government acted in bad faith or with bad conduct. *Valas*, 822 F.3d at 239. As we noted above, he has not done so. This case is comparable to *Valas*, where this court affirmed the denial of a spoliation instruction where a government technician inadvertently destroyed data on the defendant's phone by removing the phone's data chip after multiple unsuccessful attempts by several officials to access the data. *Valas*, 822 F.3d at 239. Here, the overwriting of data occurred when Lehman, after several failed attempts to image the laptop, tried a different imaging method and inadvertently triggered an automatic update that had already been installed on Glenn's computer, thereby erasing data on Glenn's hard drive. We see no meaningful difference between this case and *Valas*. Accordingly, the district court did not abuse its discretion in finding no bad faith, nor did the district court err by deciding the bad faith issue itself rather than sending it to the jury. *See United States v. Wise*, 221 F.3d 140, 156 (5th Cir. 2000).

C. Motion to Suppress

Glenn contends that the district court erred in denying his motion to suppress Glenn's statements and the images found on his computer. He argues the warrant was invalid based on the incorrect address included in Mullican's application for the search warrant.

1. Standard of Review

We "review[] the '[f]actual findings in a ruling on a motion to suppress . . . for clear error' and questions of law de novo." *United States v. Jarman*, 847 F.3d 259, 264 (5th Cir. 2017) (quoting *United States v. Moore*, 847 F.3d 259, 264 (5th Cir. 2017)). "The clearly erroneous standard is particularly deferential where, as here, 'denial of a suppression motion is based on live oral testimony . . . because the judge had the opportunity to observe the demeanor of the witnesses." *Id.* (quoting *United States v. Robinson*, 741 F.3d 588, 594 (5th Cir. 2014)). We view the evidence in the light most favorable to the prevailing party. *United States v. Moore*, 805 F.3d 590, 593 (5th Cir. 2015).

2. Analysis

Ordinarily, "[t]he Fourth Amendment's exclusionary rule will not bar the admission of evidence obtained with a warrant later found to be invalid so long as the executing officers acted in reasonable reliance on the warrant." *United States v. Alvarez*, 127 F.3d 372, 373 (5th Cir. 1997). However, "[u]nder the Supreme Court's decision in *Franks*, a search warrant must be voided if the defendant shows by a preponderance of the evidence that the affidavit supporting the warrant contained a false statement made intentionally or with reckless disregard for the truth and, after setting aside the false statement, the affidavit's remaining content is insufficient to establish probable cause." *United States v. Ortega*, 854 F.3d 818, 826 (5th Cir. 2017) (citing *Franks v. Delaware*, 438 U.S. 154, 155–65 (1978)).

Here, the district court held an evidentiary hearing in accordance with *Franks*. There are three questions in the *Franks* inquiry: 1) "does the affidavit contain a false statement?"; 2) "was the false statement made intentionally or with reckless disregard for the truth?"; and 3) "if the false statement is excised, does the remaining content fail to establish probable cause?" *Ortega*, 854 F.3d

at 826. All three questions must be answered in the affirmative for the motion to be granted. *Id.*

It is undisputed that Mullican's statement that Routh St was the address associated with Glenn's AT&T account on the date of the upload was incorrect.[6] Therefore, Glenn has satisfied the first prong. However, Glenn cannot satisfy the second prong. Mullican testified at the hearing about her state of mind as she was completing the affidavit. She expressed she had no doubts as to the correctness of the Routh Street address as of August 1st and that she made an effort to get the address correct. The district court found her testimony to be credible and her mistake to be understandable considering the "relative[ly] opaque nature of the AT&T records." The district court even went so far as to find that Mullican was not "even negligent." We must view Mullican's statements in the light most favorable to the district court's ruling and give deference to the district court's credibility determination; in doing so, we see no clear error.[7]

D. *Daubert* Challenge

Glenn's final argument is that the district court erred in allowing Mullican to testify regarding the images of child pornography she found on Glenn's computer. Glenn raises this as a challenge under *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993), which requires the district court to assess "whether the reasoning or methodology underlying the testimony is scientifically valid and . . . whether that reasoning or methodology properly can be applied to the facts in issue." *Id.* at 592–93. According to Glenn,

---

[6] Mullican's statement was as follows:

> AT&T responded that during the time the file was uploaded, IP address 99.8.79.141 was assigned to an account registered to the following individual: Michael Glenn, 3500 Routh Street, Dallas, Texas 75219. Service dates: 5-18-2016 through the date of legal process.

[7] Because Glenn has not satisfied the second *Franks* inquiry, we do not reach the third.

"Mullican was not the proper witness for introduction of the exhibit[s] because *Daubert* required the person who ran the program that retrieved the image to lay the foundation for the exhibit's admissibility." Glenn appears to argue that Lehman should have been the one to testify about the images on Glenn's computer because he was the one that imaged the hard drive and could verify the images actually came from his laptop. Therefore, as Glenn sees it, even if Mullican properly understood how "hash values" attach to and identify images based on her experience at the FBI, she could not testify that the hash values on the images she found were the same as those on Glenn's hard drive.

It is not clear to us that Glenn's argument falls within *Daubert*, as he seems to be faulting Mullican's alleged lack of personal knowledge simply because she did not run the imaging program. Regardless, our review is for abuse of discretion. *United States v. Valencia*, 600 F.3d 389, 423 (5th Cir. 2010) ("We review the admission or exclusion of expert testimony for an abuse of discretion."); *United States v. Watkins*, 591 F.3d 780, 786 (5th Cir. 2009) ("[W]e review a district court's evidentiary rulings for an abuse of discretion."). We find no abuse of discretion here, as Glenn has not adequately explained why Mullican's personal knowledge is insufficient, nor has he directed us to any cases supporting his position.

III. CONCLUSION

For the foregoing reasons, we AFFIRM the judgment of the district court.