IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 14-40699

United States Court of Appeals
Fifth Circuit
FILED
August 5, 2015
Lyle W. Cayce
Clerk

UNITED STATES OF AMERICA,

Plaintiff - Appellee

v.

DAMIAN ORISAKWE,

Defendant - Appellant

Appeal from the United States District Court
for the Eastern District of Texas
USDC No. 4:12-CR-265

Before REAVLEY, PRADO, and COSTA, Circuit Judges.

PER CURIAM:*

A jury convicted Damian Orisakwe of two counts of inducing minors to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct. Orisakwe challenges his conviction on three grounds. He argues that the district court should have suppressed evidence obtained from Yahoo and Facebook pursuant to subpoenas and warrants, that evidence of other acts was improperly admitted under Rule 404(b), and that

* Pursuant to 5TH CIR. R. 47.5, the court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5TH CIR. R. 47.5.4.

the evidence was insufficient to support the jury verdict. Finding no error, we affirm.

I.

A grand jury returned an indictment charging Orisakwe with two counts of Production of Child Pornography, in violation of 18 U.S.C. § 2251 (a) and (e). Count 1 involved minor child C.M. and occurred in or about May 2012. Count 2 involved minor child N.B. and occurred in or about July 2011 through about January 2012. Early in the case, the Government filed a notice pursuant to Federal Rule of Evidence 404(b) that at trial it intended to introduce sexually explicit videos found on Orisakwe's computer of individuals other than the victims in the charged counts. Orisakwe sought to exclude that evidence as improper and also filed a motion to suppress all the seized computer evidence as the fruits of illegal searches. The district court denied both motions and admitted the evidence at trial over Orisakwe's objection.

At the trial, N.B. and C.M. testified and told similar stories involving a teenage girl named Chelsea Roberts. According to that testimony, both boys became Facebook "friends" with Chelsea (C.M. by sending a "friend request"; N.B. by accepting one) and exchanged nonsexual pictures of themselves. Eventually, Chelsea asked N.B. and C.M. to send videos to her Yahoo email address of themselves naked and masturbating, promising videos of herself in return. Chelsea gave N.B. and C.M. specific instructions regarding how she wanted the videos made. With respect to N.B., Chelsea sent him an image of a naked boy sitting on the ground as an example of how she wanted him to pose, as well as a message saying "I want to see your whole face in [the video]. Like, move back more in that same position with your knees up and make sexy faces and talk to me." ROA.1107–08. Chelsea also relayed specific instructions to C.M., telling him in one exchange to:

> Make a video, like, three min long in the sitting down floor angle. So, like, set the phone down against a wall in front of you, facing you, and record just touching your [genitals] slowly and teasing me and then start jacking off and squirting . . . and, like, show everything, your body and face and the part under your [genitals] and talk dirty to me in the video and groan when you [ejaculate].

ROA.1146. N.B. and C.M. sent Chelsea sexually explicit videos and images, testifying that they only made these materials because of Chelsea's request. At the time of their communications with Chelsea, C.M. was fourteen years old, while N.B. was between thirteen and fifteen years old.

The remaining witnesses testified that Chelsea did not exist, but had been fabricated by Orisakwe to entice N.B. and C.M. to send illicit videos. Detective Shannon Tooley of the Las Vegas Police Department testified that her department had received a forwarded email (from an individual unrelated to this case) sent by Chelsea seeking child pornography. Tooley explained that she ascertained the IP (Internet Protocol) address from which Chelsea sent the email, and then subpoenaed the internet service provider to get the subscriber information linked to that IP address. The internet service provider's response indicated that the IP address was assigned to Orisakwe's residence in Little Elm, Texas. Tooley also subpoenaed Facebook for the email address associated with Chelsea's Facebook account and a list of IP addresses from which the account had been accessed. The Facebook account was associated with the same Yahoo email address, and the IP addresses used to access the Facebook account matched Orisakwe's residence and the university that he attended. At this point, Tooley turned the investigation over to the Little Elm Police Department.

According to their testimony, officers from Little Elm used the information provided by Tooley to obtain a search warrant for the Orisakwe residence. The officers testified that they found no signs of anyone named

Chelsea Roberts living in the house; only Orisakwe and his mother resided there. During their search, the officers seized a Toshiba laptop from a common area, as well as an iPhone and a Hewlett-Packard laptop from Orisakwe's bedroom.

Multiple investigators specializing in computer forensics testified about the seized items. Forensic analysis revealed that the iPhone had been used to access Chelsea's Yahoo email account, had the specific messaging application used to communicate with C.M. called "Textfree," and had an image of a play-doh stick figure that Chelsea had sent to N.B. In addition, the analysis revealed that both the Toshiba and Hewlett-Packard laptops contained hundreds of images of "nude minor males" with "[t]heir genitalia exposed in a lewd and lascivious manner," ROA.963–64; the Hewlett-Packard laptop additionally contained videos that depicted nude young males moving in a way that the district court concluded was similar to the movements N.B. and C.M. had made based on Chelsea's instructions. The forensic analysis also showed that the laptop contained backed-up iPhone files, including a picture of Chelsea that N.B. had received and text messages, some from "Damian Orisakwe" but others from Chelsea. Finally, the analysis revealed internet files indicating that the laptop had been used to access Chelsea's Yahoo and Facebook accounts. But none of the conversations found in the computer files involved C.M. or N.B. The Little Elm Police Department used this information to obtain search warrants to discover the contents of Chelsea's Facebook and Yahoo accounts, which showed the actual instructions that Chelsea had sent.

After presenting this evidence, the Government rested. Orisakwe moved for a verdict of acquittal, which the district court denied. Orisakwe then rested without presenting any evidence. The jury returned a guilty verdict on both counts. The court later sentenced Orisakwe to a prison term of 324 months.

Orisakwe timely appealed, challenging his convictions but not his sentence. We address the issues in the same order as they arose before the district court.

II.

Orisakwe first argues that the district court should have suppressed the evidence that led law enforcement to him, specifically challenging (1) subpoenas issued pursuant to Nevada law directing Facebook to turn over the logs of IP addresses used to access Chelsea's account, and directing internet service providers to turn over subscriber information for IP addresses found on those logs; and (2) search warrants issued to Facebook and Yahoo pursuant to Nevada and Texas law permitting officials to search the contents of Chelsea's accounts.[1] Orisakwe argues that (1) the subpoenas violated Nevada law and thus the Stored Communications Act (SCA); and (2) the Facebook and Yahoo search warrants violated the SCA because they were served outside the borders of the issuing court's state. *See* 18 U.S.C. § 2703(c). Then, in order to obtain the suppression remedy that applies to Fourth Amendment violations but not violations of the SCA, Orisakwe argues that the searches conducted pursuant to these allegedly defective court orders infringed on privacy

[1] Law enforcement officials obtained several subpoenas and warrants throughout the investigation. First, in October 2011, Nevada issued an administrative subpoena at LVPD's request to Facebook for a user ID connected to "Chelsea Roberts." The subpoena requested basic subscriber information pursuant to 18 U.S.C. § 2703(c)(2) as well as other subscriber information pursuant to 18 U.S.C. § 2703(c)(1). In January 2012, Nevada issued three more administrative subpoenas at the request of LVPD: two to Grande Communications, an internet service provider, for IP addresses located in the IP log returned from Facebook; and one to Time Warner Cable, an internet service provider, for an IP address located in the IP log returned from Facebook. Tooley also obtained a search warrant under Nevada law to obtain the contents of emails in the Yahoo account between May 2011 and January 2012. At that point, the investigation was turned over to the Little Elm Police Department in Texas. Little Elm used the information from Tooley to obtain a search warrant for Orisakwe's home. The final search warrant, which was issued after the search of Orisakwe's home, was obtained to gain the contents of Chelsea's Facebook and Yahoo accounts between January 2012 and June 2012.

interests protected by the Constitution. *See United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014) (holding that "suppression is not a remedy for a violation of the Stored Communications Act" that does not also amount to a Fourth Amendment violation).

We need not reach the question of whether Orisakwe has a reasonable expectation of privacy in IP addresses because he has not convinced us that the subpoenas or warrants were unlawful.[2] The SCA permits subpoenas issued in accordance with a state statute. *See* 18 U.S.C. § 2703(c)(2) (stating that a provider shall disclose to a governmental entity certain information pursuant to, among other things, "an administrative subpoena authorized by a Federal or State statute"). Here the initial subpoenas to Facebook and companies that sell internet service were issued under Nevada Revised Statutes (N.R.S.) Section 193.340, which permits a "sheriff of any county" to subpoena "provider[s] of Internet service" upon a showing of "reasonable cause" to "carry out the procedure set forth in [the SCA]." Orisakwe contends the different subpoenas failed to meet these requirements. First, Orisakwe argues that the Sheriff's Lieutenant—rather than the Sheriff himself—signed the subpoenas. But the subpoenas were issued under the authority of the Sheriff

[2] We note that every circuit to have addressed the issue has held that there is not a reasonable expectation of privacy in IP addresses that implicates the Fourth Amendment. *See, e.g.*, *United States v. Wheelock*, 772 F.3d 825, 828 (8th Cir. 2014) ("With Comcast in possession of his subscriber data, Wheelock cannot claim a reasonable 'expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers.'" (alteration in original)); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007) ("Neither this nor any other circuit has spoken to the constitutionality of computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account. We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*." (footnote omitted)); *see also United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information [associated with an IP address] provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.").

and the Lieutenant merely signed on the Sheriff's behalf. Orisakwe also argues that no reasonable cause existed to issue any of the subpoenas, but such cause was provided by the tip the LVPD received that someone used Chelsea's Facebook account to request explicit videos from a minor. As to the Facebook subpoena specifically, Orisakwe makes two arguments. He contends that Facebook is not a "provider of Internet service," but that term is expansively defined in the statute to include any entity that provides "an electronic mail address," which Facebook does.[3] *See* N.R.S. § 193.340 (defining a "provider of Internet service" by cross-reference to N.R.S. § 205.4758); N.R.S. § 205.4758 (stating that a "'provider of Internet service' means any provider who provides subscribers with access to the Internet *or* an electronic mail address" (emphasis added)). He next argues that the Facebook subpoena was overbroad because it requested content records that can only be obtained by search warrant. Orisakwe, however, has not actually identified any information obtained from Facebook, or used at trial, that failed to comply with the statute's restrictions on administrative subpoenas. *See* 18 U.S.C § 2703(c)(2) (procedure for administrative subpoena).

Orisakwe has also failed to demonstrate the unlawfulness of the later-issued search warrants directing Facebook and Yahoo to turn over the contents of Chelsea's accounts. The SCA provides that a warrant may be issued "by a court of competent jurisdiction." 18 U.S.C. § 2703(a). At the federal level, that includes a federal district or circuit court that "has jurisdiction over the offense being investigated [or] is in or for a district in which the provider of a wire or electronic communication service is located." 18 U.S.C. § 2711(3)(A). At the

[3] *See generally* Facebook, *How do I use my @facebook.com email address?* (Feb. 2015), https://www.facebook.com/help/224049364288051. As the district court noted, Facebook has taken the position that subpoenas issued to it are covered by the Stored Communications Act. *See In re Facebook*, 923 F. Supp.2d 1204, 1205 (N.D. Cal. 2012).

state level, it includes "a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants." 18 U.S.C. § 2711(3)(B). Orisakwe argues that, because there are no geographical restrictions on state courts but there are on federal courts, Congress intended to deny state courts the power to issue a search warrant for out-of-state records. But the plain text of the statute permits a state to issue a search warrant if authorized by the law of that state. Here, there is no dispute that Nevada and Texas law authorized the search warrants issued to Facebook and Yahoo, despite these entities' storing the requested information outside the issuing state. *See* N.R.S. § 193.340 (containing no restrictions based on a company's data being located elsewhere); Tex. Code Crim. Proc. Ann. art. 18.01 (same).

Because Orisakwe has identified no defects with the subpoenas or warrants, the district court properly denied his motion to suppress.

III.

Orisakwe next challenges the district court's admission of a video as evidence under Rule 404(b). "We 'review a district court's evidentiary rulings for abuse of discretion,' subject to harmless-error analysis." *United States v. Girod*, 646 F.3d 304, 318 (5th Cir. 2011) (internal citation omitted). "If evidence is extrinsic, Rule 404(b) and *United States v. Beechum,* 582 F.2d 898 (5th Cir. 1978) (en banc), require that we first determine 'that the extrinsic evidence is relevant to an issue other than the defendant's character, *i.e.,* motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident.'" *Id.* at 319 (quoting *United States v. Sanders,* 343 F.3d 511, 518 (5th Cir. 2003)). "Second the evidence must possess probative value that is not substantially outweighed by its undue prejudice and must meet the other requirements of Rule 403." *Id.* (internal quotation marks omitted) (quoting *Sanders*, 343 F.3d at 518).

The video at issue—which depicted "a young man without any clothes on moving around and showing his genitals," ROA.998—was one of three similar "orphan file" videos found on the laptop seized from Orisakwe's bedroom. An "orphan file" is a remnant of a deleted application or file, so that, with respect to this video, there was no date-stamp associated with the video, no way to tell who created that video and put it on the computer, and no way to identify the male in the video. What the forensic analysis does tell us, however, is that the "images resided on that computer." The Government sought to introduce the video as evidence of identity, plan, knowledge, and absence of mistake under 404(b) by arguing that the orphan file video was "virtually identical" to the video that C.M., acting on specific instructions from Chelsea, produced. The district court found "[n]o question but that the two videos . . . are similar." ROA.999. Specifically, the court observed, in comparing the orphan file video to the one C.M. made at Chelsea's direction, that "[b]oth young men appeared to be approximately the same age," and that "they were both, I think it's pretty obvious from the video, moving their bodies in the same way." ROA.999. The district court overruled Orisakwe's objections, and gave the jury a limiting instruction regarding the orphan file video. That instruction informed the jury that the "video is not of either CM or NB," and that "[w]e don't know who this is a video of." ROA.1157. Thus, the court instructed, the jury could only consider the video for the "limited purposes" of "determining whether or not you believe Mr. Orisakwe acted according to a particular scheme of preparation or plan, you can consider it for purposes of identity of the accused here, whether or not it was the accused who was involved in this or some other person, or whether this occurred as a result of a mistake or accident." ROA.1157–58.

Orisakwe first argues that the video is not probative because there was no evidence the video was made at Orisakwe's direction. Moreover, Orisakwe points out that, without knowing the identity of the male in the video, there is

no way to know if he was a minor or adult when the video was created. Orisakwe also argues that in order for the video to establish *modus operandi*, the similarities between the videos must be striking, and here the act of dancing in the nude or videotaping oneself masturbating is not specific enough to be probative *modus operandi* evidence.

We disagree with Orisakwe's contentions. In evaluating this Rule 404(b) evidence, it is important to note that the defense argument at trial was that the evidence did not establish that Orisakwe used the "Chelsea" account. In connection with this, the defense emphasized the absence of any files concerning N.B. and C.M. found on Orisakwe's computers. The video of another individual that the district court admitted under Rule 404(b) was directly responsive to these arguments and probative on the identity and *modus operandi* of the perpetrator of the charged conduct.

Orisakwe first contends that there was insufficient evidence tying this video to him. But the admissibility standard for Rule 404(b) evidence is just a preponderance of the evidence. *See United States v. Gutierrez-Mendez*, 752 F.3d 418, 424 (5th Cir.) *cert. denied*, 135 S. Ct. 298 (2014) (inquiring whether the bad-act offered as 404(b) evidence was proved by a preponderance). That threshold was met by the following facts: 1) the video was on Orisakwe's laptop, which was seized from his own bedroom and that contained numerous other files belonging to him, and 2) the conduct in the 404(b) video, in terms of body movements, was very similar to the videos that N.B. and C.M. sent to Chelsea. *See United States v. Grimes*, 244 F.3d 375, 384 (5th Cir. 2001) (noting that relevancy "is a function of the degree of similarity between the extrinsic act and the offenses charged," which means that "the common characteristic must be 'the significant one for the purpose of the inquiry at hand'" (quoting *United States v. Guerrero,* 650 F.2d 728, 733 (5th Cir. Unit A 1981)). Orisakwe also argues that there in insufficient evidence to show that the individual in the

video is a minor. The district court concluded otherwise, and we do not find error in that conclusion. Moreover, the "other acts" admitted under Rule 404(b) need not themselves be unlawful. *See United States v. Stephens*, 571 F.3d 401, 411 (5th Cir. 2009) (observing that "extrinsic evidence of using the same scheme repeatedly is relevant to knowledge and intent, in that it demonstrate[s] how [an] operation work[s,]" and stating "there is no requirement that the [extrinsic evidence] result[ ] in formal charges" to be admissible under 404(b) (alterations in original) (citations and quotation marks omitted)). So even if the individual depicted in the video was slightly older than the victims in the charged counts, Orisakwe's possession of a video of that individual engaging in similar behavior to the conduct he instructed N.B. and C.M. to perform is probative on the issue of whether Orisakwe acted as the "Chelsea" who issued those instructions. If anything, the potentially older age of the individual in the 404(b) video makes it less likely that the jury would consider the video as evidence that Orisakwe was a pedophile—an impermissible use of "other act" evidence—but instead consider it for the permissible purpose of proving identity of the person who committed the charged offenses.

Orisakwe next argues that the orphan file video's probative value is outweighed by its prejudicial impact under *Grimes*, 244 F.3d at 384. But that stretches *Grimes* too far. In that case, the district court admitted extrinsic evidence of narratives which had been downloaded onto the defendant's computer containing violent depictions of rape, torture, and sexual assault of young girls. *Id.* at 379, 385. Notably, these narratives "were of a different sexual nature from the photographs," in that the pornographic photographs depicted no violence while the narratives were "vile in their graphic and violent nature: young girls in chains, a young girl in handcuffs, and references to blood." *Id.* at 385. In light of the "gruesome violence" of the narratives, we

found the probative value substantially outweighed by the danger of unfair prejudice. *Id.* That is not the situation at hand here, where the extrinsic video depicts the same sex act performed in a very similar way. Indeed, not admitted in this case were the numerous other child pornography files that had been found on Orisakwe's computers. And the probative value of the video was substantial given that the core defense at trial was that Orisakwe was not Chelsea. *See United States v. Caldwell*, 586 F.3d 338, 342 (5th Cir. 2009) ("While all relevant evidence tends to prejudice the party against whom it is offered, Rule 403 excludes relevant evidence when the probative value of that evidence is *substantially* outweighed by the *unfairly* prejudicial nature of the evidence." (emphasis in original)).

The district court did not abuse its discretion in admitting the video.

IV.

Finally, Orisakwe challenges the sufficiency of the evidence to support the guilty verdict. Orisakwe was convicted of two counts of violating 18 U.S.C. § 2251(a), which requires proof beyond a reasonable doubt that he: (1) employed, used, persuaded, induced, enticed, or coerced a minor to engage in any sexually explicit conduct; (2) with the purpose of producing a visual depiction of such conduct; and (3) knew or had reason to know that such visual depiction would be transmitted using any means or facility of interstate commerce. We review the district court's denial of Orisakwe's motion to acquit de novo, viewing all evidence in the light most favorable to the verdict. *United States v. Woerner*, 709 F.3d 527, 535 (5th Cir. 2013). We uphold the jury verdict if "a rational trier of fact could have found that the evidence established the essential elements of the offense beyond a reasonable doubt." *Id.*

Orisakwe argues that the evidence fails in two ways. First, he argues that, even assuming Chelsea enticed C.M. and N.B. into producing the videos, the Government failed to present sufficient evidence that *he* was Chelsea.

Orisakwe specifically questions the evidence related to the IP addresses, contending that the logs listed his home IP address for only 23.5% of the total logins to the Yahoo email account. Orisakwe concludes that the jury could not have found that he was the person logging into the account every time, and thus could not have found him responsible for all of the messages sent to C.M. and N.B. The Government responds that the evidence was sufficient to show Orisakwe posed as Chelsea, and the remaining 76.5% of login attempts merely show he accessed the accounts from locations other than home and school.

We observed in *United States v. Woerner* that the Government must often rely on circumstantial evidence in child pornography cases because direct evidence tying the defendant to the use of a computer at a particular time often does not exist. *See* 709 F.3d at 537. In that case, we affirmed a conviction for possession of child pornography based on the defendant's home IP address being used to download and distribute child pornography and the pornography being found on a computer and accounts associated with him. *Id.* at 537, 541. The evidence is at least as strong here, as it targets Orisakwe as the computer user from more angles. The evidence showed that Chelsea's accounts were accessed from Orisakwe's computers based not just on the IP logs from Yahoo, but also the IP logs from Facebook. The files found on both computers and Orisakwe's iPhone contain internet history showing they were used to access Chelsea's Facebook and Yahoo accounts. The iPhone also had a unique image of a play-doh stick figure that Chelsea sent to N.B., and the iPhone backup files showed a picture of Chelsea sent to N.B. and text message conversations with Chelsea. As explained above, the orphan files also supported the inference that it was Orisakwe posing as Chelsea. Perhaps because the only other person living in his home was his mother, Orisakwe does not argue that someone else in the home used the computers. The evidence therefore permitted the jury to conclude that Orisakwe was the one using Chelsea's accounts.

Orisakwe's second sufficiency argument relates only to the count involving victim N.B., as he contends that the evidence did not show that Chelsea enticed N.B. to produce the sexually explicit videos. *See* 18 U.S.C. § 2251(a) ("Any person who . . . entices, or coerces any minor *to engage* in . . . any sexually explicit conduct for the purpose of *producing* any visual depiction . . . shall be punished" (emphasis added)). N.B. testified that he filmed the videos after receiving the very specific instructions from Chelsea and "w[as] doing that because Chelsea asked [him] to do that." ROA.627–30. The jury was entitled to believe that testimony even if the defense had raised significant doubts about it on cross examination. *See, e.g.*, *United States v. McCall*, 553 F.3d 821, 835 (5th Cir. 2008) (holding that the jury has the right to believe a witness despite evidence impeaching that witness's credibility). But Orisakwe's arguments on this point do not even rise to the level of serious impeachment. He relies on an email in which N.B. tells Chelsea he could not perform the requested sexual acts because he had already performed similar acts earlier that day as well as testimony that N.B. suspected Chelsea was not a real person. Evidence that N.B. might have performed similar acts in private does not undermine the conclusion that Chelsea enticed him to do so for the purpose of producing a video of the sexual act. And suspecting that the Chelsea name was a ruse does not change the fact that N.B. was enticed by whomever it was sending those instructions.

The evidence is therefore sufficient to uphold the jury's verdict. The judgment is AFFIRMED.