US v. Marques Bynum Doc. 920100505

PUBLISHED

UNITED STATES COURT OF APPEALS

FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,
v.
MARQUES DRAKEFORD BYNUM, a/k/a markie_zkidluv6, a/k/a keyido126@netzero.net,
Defendant-Appellant.

No. 08-4207

Appeal from the United States District Court
for the Western District of North Carolina, at Charlotte.
Martin K. Reidinger, District Judge.
(3:06-cr-00401-MR-DCK-1)

Argued: March 25, 2010

Decided: May 5, 2010

Before WILKINSON and MOTZ, Circuit Judges,
and Joseph R. GOODWIN, Chief United States District
Judge for the Southern District of West Virginia,
sitting by designation.

Affirmed by published opinion. Judge Motz wrote the opinion, in which Judge Wilkinson and Judge Goodwin joined.

COUNSEL

ARGUED: Aaron Edmund Michel, Charlotte, North Carolina, for Appellant. Adam Christopher Morris, OFFICE OF

Dockets.Justia.com

THE UNITED STATES ATTORNEY, Charlotte, North Carolina, for Appellee. **ON BRIEF:** Gretchen C. F. Shappert, United States Attorney, Charlotte, North Carolina, for Appellee.

DIANA GRIBBON MOTZ, Circuit Judge:

A jury convicted Marques Drakeford Bynum of transporting and possessing child pornography, in violation of 18 U.S.C. § 2252A (2006). The district court sentenced him to 192 months in prison. Bynum appeals, challenging his conviction and sentence. Finding no reversible error, we affirm.

I.

On July 8, 2003, FBI Special Agent Gregory Zack, working undercover and using an informant's password, entered a child-pornography online chat group administered by Yahoo! Inc. ("Yahoo"). Agent Zack observed that someone using the moniker "markie_zkidluv6" had, on June 22, 2003, uploaded to the group's website a dozen photos depicting children engaged in sexual acts. On July 10, 2003, Agent Zack again accessed the group and observed that the same user had uploaded several more illicit images.

In an effort to identify "markie," the FBI served an administrative subpoena on Yahoo, requesting the subscriber information "markie" had entered into the Yahoo website when he opened his account, and the internet protocol ("IP") addresses (numbers generated automatically by the internet service provider) associated with the user's uploads to the Yahoo website.

Once Yahoo provided the FBI with this information, Agent

Zack plugged the IP addresses into a free, public website that directed him to the internet service provider associated with those addresses, UUNET Technologies ("UUNET"). The FBI then issued a subpoena to UUNET asking for information on the customer associated with the IP addresses. After receiving from UUNET an email address and telephone number—which indicated to Agent Zack that "markie" had used a phone-based "dial-up service and not a cable or DSL line" to access the internet—Agent Zack subpoenaed the phone and internet companies that operated the dial-up service.[1] Drawing from their "subscriber information" records, these companies provided Agent Zack with Bynum's name and the physical address from which the uploads emanated: the Charlotte, North Carolina home of Bynum's mother.

On September 22, 2003, Agent Zack entered the online chat group again and observed a third upload from "markie," this time containing a video entitled "4yo-refusing-cumshot-wsound[1].mpg." That same day, Agent Zack accessed "markie's" profile information, in which the user identified himself as a 24-year-old single male living in North Carolina who "want[s] to chat with any cute girls that live close by thats [sic] up for a little fun." The profile also included a photo of Bynum.

The FBI used this information to prepare an affidavit in support of a search warrant of the Bynum home. A federal magistrate judge issued the warrant and, during the December 2003 search that followed, the FBI found a laptop computer in a bedroom that the agents recognized as the background for Bynum's profile photo. A subsequent search of the computer revealed the images and video Agent Zack had earlier found uploaded online, as well as 5,074 photos and 154 videos of child pornography.

[1]All the administrative subpoenas served in this case requested that the recipients not disclose to Bynum or anyone else the existence of the subpoenas.

Three years later, in September 2006, a federal grand jury indicted Bynum on three counts of transporting child pornography in interstate commerce (by uploading it to Yahoo's out-of-state servers on July 8, July 10, and September 22, 2003), *see* 18 U.S.C. § 2252A(a)(1), and one count of possessing child pornography that had moved in interstate commerce, *see id.* § 2252A(a)(5)(B).

Bynum moved to suppress the evidence seized during the December 2003 search, arguing that this evidence constituted the fruit of "unlawful administrative subpoenas," and that the affidavit supporting the search warrant did not demonstrate probable cause and lacked critical information. He also moved to exclude proffered expert Government testimony as to whether the images in question depicted real children or were computer-generated, and thus protected under the First Amendment. After holding separate hearings, the court denied both motions.

Bynum proceeded to trial on the four counts charged in the indictment. At the conclusion of the Government's case, Bynum moved for judgment of acquittal, which the court denied. Bynum offered no evidence, and the jury found him guilty on all counts. Bynum then renewed his motion for acquittal, which the court again denied.

At sentencing, Bynum objected, without success, to the sentence recommended in his presentence investigation report, and advanced arguments in support of a downward variance from the United States Sentencing Guidelines' ("U.S.S.G." or "Guidelines") advisory range of 168-210 months in prison. For its part, the Government sought an upward variance from the Guidelines, urging the district court to impose the maximum statutory penalty of 20 years in prison. *See* 18 U.S.C. § 2252A(b)(1). Bynum elected not to allocute. The district court denied both parties' requests. Instead, it imposed a mid-Guidelines sentence of 192 months' imprisonment.

Bynum timely noted this appeal.

II.

Bynum raises two Fourth Amendment challenges to the district court's refusal to suppress evidence seized during the search of the Bynum home, including the computer that uploaded and stored the child pornography at issue here. "Whether certain conduct by law enforcement officers infringes upon rights guaranteed by the Fourth Amendment is a question of law subject to de novo review." *United States v. Breza*, 308 F.3d 430, 433 (4th Cir. 2002).

A.

First, Bynum contends that the Government's use of "secret" administrative subpoenas violated his Fourth Amendment rights. He offers no case law supporting this theory, and we have found none.

"The 'touchstone' of Fourth Amendment analysis is whether the individual has a reasonable expectation of privacy in the area searched . . . ." *Id.* at 433 (quoting *Oliver v. United States*, 466 U.S. 170, 177 (1984)). In order to demonstrate a legitimate expectation of privacy, Bynum "must have a subjective expectation of privacy, and . . . that subjective expectation must be reasonable." *United States v. Kitchens*, 114 F.3d 29, 31 (4th Cir. 1997).

In this case, Bynum can point to no evidence that he had a subjective expectation of privacy in his internet and phone "subscriber information"—*i.e.*, his name, email address, telephone number, and physical address—which the Government obtained through the administrative subpoenas. Bynum voluntarily conveyed all this information to his internet and phone companies. In so doing, Bynum "assumed the risk that th[os]e compan[ies] would reveal [that information] to police." *Smith v. Maryland*, 442 U.S. 735, 744 (1979). Moreover, Bynum

deliberately chose a screen name derived from his first name, *compare* "markie_zkidluv6" *with* "Marques," and voluntarily posted his photo, location, sex, and age on his Yahoo profile page.

Even if Bynum could show that he had a subjective expectation of privacy in his subscriber information, such an expectation would not be objectively reasonable. Indeed, "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation." *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (collecting cases).

In sum, because the FBI's administrative subpoenas did not invade any legitimate privacy interest possessed by Bynum, their issuance did not violate the Fourth Amendment.[2]

B.

Bynum also challenges the sufficiency of the affidavit supporting the search warrant. The Fourth Amendment mandates that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Probable cause to search exists if

[2]Because Bynum does not allege a privacy interest in the IP addresses the FBI obtained from Yahoo—numbers that Bynum never possessed—he has abandoned any such claim. *See Edwards v. City of Goldsboro*, 178 F.3d 231, 241 n.6 (4th Cir. 1999). Furthermore, because we decide that the nature of the information that Bynum voluntarily conveyed carries no constitutional expectation of privacy, we need not address his argument that the subpoenas in this case, because "secret," should be subject to a standard more stringent than "general reasonableness," Petr.'s Br. 16-17; *see In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000), or the Government's contention that Bynum lacks Fourth Amendment standing to contest the subpoenas because they were "directed at [internet service providers], not at him," Govt.'s Br. 19.

there is "'a *fair probability* that contraband or evidence of a crime will be found in a particular place.'" *United States v. Gary*, 528 F.3d 324, 327 (4th Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)).

Bynum maintains that the affidavit supporting the search warrant was deficient because it (1) did not disclose that June 22, 2003 was the actual date of the first two uploads (rather than July 8 and 10, when Zack observed those uploads); (2) did not explain why the administrative subpoenas revealed information for July 25, 26, and 27, rather than June 22, July 8, or July 10; and (3) lacked "probable cause to believe that the suspect would still be at t[he searched] address" in December, six months after the first charged uploading. Petr.'s Br. 19.

These arguments fail because Bynum presents no reason—nor can we fathom one—as to why these minor date discrepancies, or the delay between the administrative subpoenas and the request for a warrant, undermine the magistrate judge's reasonable conclusion that the home of Bynum's mother likely contained evidence of a crime. The affidavit established that on July 8 and 10, the FBI observed that "markie_zkidluv6" had uploaded suspected child pornography to the internet, and that, later in July, somebody at the Bynum address used that screen name. Regardless of the dates of the uploads, the affidavit plainly established a "fair probability" that a search of the premises might uncover evidence of possession and transmission of child pornography. In a different case, slight date discrepancies might call into question a finding of probable cause. *Cf. United States v. Rattenni*, 480 F.2d 195, 199 (2d Cir. 1973). Here, however, "[t]he magistrate's determination of probable cause rested on the actual facts of the [illegal uploads], not [any] erroneous date[s] stated in the warrant." *Gary*, 528 F.3d at 328.

Moreover, even assuming that probable cause did not support the warrant, the district court found "no bad faith" in the

FBI's reliance on the warrant or affidavit, which was not "bare bones," and Bynum presents no evidence or argument demonstrating this finding to be clearly erroneous. Therefore, suppression of the evidence against Bynum would not serve the deterrent purposes of the Fourth Amendment's exclusionary rule. *See id.* at 329-30; *United States v. Leon*, 468 U.S. 897, 913 (1984) (establishing good-faith exception to exclusionary rule when "officers reasonably rely[ ] on a warrant issued by a detached and neutral magistrate").

III.

Bynum poses two evidentiary challenges.

A.

He first contends that the Government offered insufficient evidence that he, "rather than some other occupant or resident or friend" at his parents' home "was up to suspected mischief," and that "the suspected child pornography was in fact pictures of the molestation of real children." Petr.'s Br. 21-22.[3] In determining sufficiency of the evidence, "we ask whether, viewing the evidence in the light most favorable to the gov-

[3]Bynum also contends that prosecution of those who merely transmit and possess child pornography (as opposed to child molesters who produce child pornography) violates the First Amendment's guarantee of free speech. Petr.'s Br. 24-25. Our case law forecloses this argument. *See United States v. Matthews*, 209 F.3d 338, 342 (4th Cir. 2000) (finding that "[t]he protection of children clearly constitutes a 'public welfare' interest justifying regulation of speech in certain circumstances," including child pornography, and rejecting a journalist's First Amendment defense to transmission-of-child-pornography charges). Bynum apparently recognizes this, asserting that *Matthews*—the only case he cites—subordinates "freedom" to "the misplaced policies of the government," and constitutes an "assault on the specific designs of our founding generation." Petr.'s Br. 25. Even if this were so, *Matthews* is circuit precedent that we must follow in the absence of "an en banc overruling or a superseding contrary decision of the Supreme Court." *United States v. Prince-Oyibo*, 320 F.3d 494, 498 (4th Cir. 2003).

ernment, any rational trier of facts could have found the defendant guilty beyond a reasonable doubt." *United States v. Harvey*, 532 F.3d 326, 333 (4th Cir. 2008) (internal quotation marks omitted).

Given this deferential standard, abundant evidence supports the jury's conclusion that Bynum, and not someone else, committed the offenses charged in the indictment. At trial, the Government offered evidence that the agents found the computer in question in Bynum's bedroom, the same bedroom visible in Bynum's Yahoo profile photo, which had been taken using the computer's camera; that the computer had a login name of "Marques" (Bynum's first name) and contained the actual uploaded images and video; and that, on the day of the search, Bynum admitted that he had used the "markie" account and kept the password on a piece of paper in his bedroom at his parents' home. The Government also presented evidence of chats, *i.e.*, online conversations using instant messaging, found on that computer, in which Bynum discussed the group and photos. Notwithstanding Bynum's vague and unsupported suggestions of "IP-spoofing," and assertedly weak "ties to his mother's home," Petr.'s Br. 21, a rational fact finder could have found, beyond a reasonable doubt, that Bynum knowingly possessed and transmitted child pornography.

Sufficient evidence similarly supports the jury's conclusion that the images and videos in question depicted real children. *See* 18 U.S.C. § 2256(8)(A) (2006) (defining "child pornography" as a visual depiction the production of which "involves the use of a minor engaging in sexually explicit conduct"). "[T]here seems to be general agreement among the circuits that pornographic images themselves are sufficient to prove the depiction of actual minors." *United States v. Salcido*, 506 F.3d 729, 734 (9th Cir. 2007) (per curiam) (collecting cases). In other words, the Government need not present *any* extrinsic evidence as to this issue, so long as the jury has had an opportunity—as it did here—to view the relevant images. *See,*

e.g., United States v. Rodriguez-Pacheco, 475 F.3d 434, 440-41 (1st Cir. 2007). Of course, in this case the Government did present substantial extrinsic evidence to establish that the children depicted were real minors, including testimony drawn from the personal investigative experience of various officers as to the identity and age of some of the children in the photos Bynum was alleged to have transported or possessed, and testimony from FBI Analyst Peter Smith to the effect that the images and videos in question depicted real children and did not appear to be computer-generated. Again, a rational fact finder could certainly conclude that the Government proved beyond a reasonable doubt that actual minors appeared in the photos and videos.

B.

Bynum argues next that the district court erred in admitting the expert testimony of Analyst Smith because the Government failed to demonstrate the reliability of his methods of determining the authenticity of child pornography. Petr.'s Br. 22-23. "We review for abuse of discretion the district court's decision to admit expert testimony under Federal Rule of Evidence 702."[4] *United States v. Wilson*, 484 F.3d 267, 273 (4th Cir. 2007).

Although not directly addressing the issue, several appellate courts have assumed that the testimony of experienced forensic or medical professionals establishing the authenticity of alleged child pornography constitutes appropriate expert

[4]Federal Rule of Evidence 702 provides as follows:

> If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

testimony. *See, e.g.*, *Rodriguez-Pacheco*, 475 F.3d at 437-39; *United States v. Anderton*, 136 F.3d 747, 750 (11th Cir. 1998); *United States v. Broyles*, 37 F.3d 1314, 1317-18 (8th Cir. 1994). Even the Supreme Court has noted the use of experts in this context. *See Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 254 (2002).

If, as we and other courts have held, "law enforcement officers with extensive drug experience are qualified to give expert testimony on the meaning of drug-related code words," *Wilson*, 484 F.3d at 275, it follows that forensic photographic investigators with extensive child pornography experience are qualified to give expert testimony as to whether images depict real children. For Bynum's claim that Analyst Smith's "method has not been tested, or subject to peer review and publication," and "does not have a[n] . . . error rate," Pet'r Br. 22, also is true of drug-code testimony. And as we observed in *Wilson*, the Supreme Court has admonished that "'the test of reliability is flexible' and 'the law grants a district court the same broad latitude when it decides *how* to determine reliability as it enjoys in respect to its ultimate reliability determination.'" 484 F.3d at 274 (quoting *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 141-42 (1999)). We concluded, therefore, that although "[e]xperiential expert testimony . . . does not rely on anything like a scientific method," such testimony is admissible under Rule 702 so long as an experiential witness "explain[s] how [his] experience leads to the conclusion reached, why [his] experience is a sufficient basis for the opinion, and how [his] experience is reliably applied to the facts." *Id.* (internal quotation marks omitted).

Here, as in *Wilson*, "[w]e have little trouble concluding that the district court did not abuse its discretion in qualifying [Analyst Smith] as an expert." *Id.* Analyst Smith testified at length as to his 18 years with the FBI, as well as his training and 13 years of experience in examining "questioned photographic evidence," his completion of proficiency testing in image authentication, and his qualification as an expert 35

times in the past. He further testified as to exactly the steps he takes in determining the authenticity of images under the approved FBI "checklist," including ascertaining an image's resolution and focus, examining its sharpness and depth, comparing it to images in the FBI database, and identifying in the image certain human characteristics—like skin, teeth, ears, and hair—that are difficult to recreate by computer. Finally, Analyst Smith testified that two other FBI employees always review his work, and that he has never identified an image as real that was later determined to be computer-generated. These ample indicia of reliability preclude a finding that the district court abused its considerable discretion in qualifying Analyst Smith as an expert.

Moreover, even if the district court erred in admitting Analyst Smith's testimony—which we do not believe to be the case—the error was clearly harmless because the Government presented to the jury the images and video, and testimony from people who knew the actual children depicted in them. *See, e.g.*, *Salcido*, 506 F.3d at 734 ("[P]ornographic images themselves are sufficient to prove the depiction of actual minors.")

IV.

Finally, Bynum challenges the substantive reasonableness of his within-Guidelines 192-month sentence. He labels this sentence "insane," Petr.'s Br. 15, because it is "severe relative to the sentences imposed on others," *id.* at 27 (charting average sentences for various other crimes by offenders in Bynum's criminal history category, I). Bynum argues that "nothing about [him] or the offense" merits this sentence. *Id.* at 28.

This argument also fails, for it ignores controlling federal law. Congress defines federal crimes and establishes the proper factors to be considered in fashioning a sentence for those crimes. *See* 18 U.S.C. § 3553(a) (2006). Under this

framework, Congress has determined that when selecting a proper sentence, the sentences imposed on other defendants for other crimes are irrelevant. Rather, federal law expressly limits a sentencing court's consideration of the sentences of other criminals to those imposed for "the applicable *category of offense* committed by the applicable *category of defendant* as set forth" in the advisory Guidelines established by the United States Sentencing Commission. *Id.* § 3553(a)(4)(A) (emphases added); *see also id.* § 3553(a)(6) (requiring a sentencing court to consider "the need to avoid unwarranted sentence disparities among defendants with *similar* records who have been found guilty of *similar* conduct" (emphases added)). Bynum makes no effort to demonstrate that his mid-Guideline 192-month sentence is unreasonably excessive compared to the sentences of other defendants in the same criminal history category convicted of crimes in the same offense level.

Moreover, Bynum does not argue that the district court otherwise unreasonably applied federal law in fashioning his sentence. If he did, such an argument would fail. Although Congress has deemed Bynum's personal characteristics and history relevant in the sentencing analysis, *id.* § 3553(a)(1), nothing in Bynum's past suggests that the district court imposed a substantively unreasonable sentence in sentencing him within the advisory Guidelines range. *See id.* § 3553(a)(4) (directing sentencing courts to consider the recommended Guidelines range). Thus, Bynum can point to no evidence rebutting the presumption of substantive reasonableness that we afford properly calculated within-Guidelines sentences. *See Rita v. United States*, 551 U.S. 338, 347 (2007); *United States v. Wright*, 594 F.3d 259, 267, 268 (4th Cir. 2010).

In fact, in determining Bynum's sentence, the district court expressly refused to consider Bynum's conduct leading to 2002 child pornography charges, which the Government subsequently dismissed. The court denied the Government's

request for an upward variance and sentenced Bynum—who uploaded several illicit, and sometimes violent, sexual photos and video of children to the internet, and on whose computer authorities found more than 5000 photos and 150 videos of child pornography—to a within-Guidelines sentence. We cannot deem this sentence substantively unreasonable.[5]

V.

The judgment of the district court is therefore

AFFIRMED.

[5]Bynum does not argue that the district court committed any *procedural* sentencing error. *Compare United States v. Thompson*, 595 F.3d 544, 546-48 (4th Cir. 2010). Accordingly, we can only conclude that Bynum has "abandoned" any such contention. *See United States v. Smith*, 441 F.3d 254, 274 (4th Cir. 2006). Bynum's abandonment of this contention distinguishes the case at hand from *Thompson*, in which the appellant forcefully argued on appeal, indeed devoted his entire appellate brief to the claim, that the district court committed procedural sentencing error. *See* Petr.'s Br. in *Thompson*, *available at* 2009 WL 1158702.