[DO NOT PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 17-14073
Non-Argument Calendar

D.C. Docket No. 5:16-cr-00028-RH-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

MICHAEL RAY ALFORD,

Defendant-Appellant.

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

(August 3, 2018)

Before WILSON, JORDAN and BLACK, Circuit Judges.

PER CURIAM:

Michael Ray Alford appeals his conviction for knowingly receiving and attempting to receive material containing child pornography. Alford brings three issues on appeal, which we address in turn. After review, we affirm Alford's conviction.

I. DISCUSSION

A. Motion to Suppress

Alford first argues the district court erred by refusing to suppress evidence obtained as a result of a Montana search warrant issued to Google after concluding the warrant was sufficiently particular. The warrant requested that Google provide:

> Any and all records, files, data, and/or other forms of information including names, user names, dates of birth, IP addresses, home addresses, phone numbers, e-mail addresses, photos, videos, e-mail content, search history, call history, or other information held by Google Inc. which may aid in obtaining the identification and/or location of the individual whom contacted K-mart in Hamilton, MT via phone call [to various phone numbers] on September 16th, 2014 at approximately 2145 hours MST.

A search warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend IV. The Fourth Amendment requires searches be as limited as possible, and the goal is to prevent "rummaging" through a person's belongings by requiring warrants to include a particular description of the things to be seized. *United States v. Blake*, 868 F.3d 960, 973 (11th Cir. 2017), *cert. denied* 138 S. Ct. 1580 (2018). In *Blake*, we

concluded a warrant requiring Microsoft to turn over all e-mails containing potentially incriminating evidence was constitutional because that limitation prevented a general rummaging through the defendant's e-mails. *Blake*, 868 F.3d at 973. However, we concluded warrants requiring Facebook to disclose "virtually every kind of data that could be found in a social media account" were unconstitutional because, for example, the warrants could have limited the search of private messages to only those sent or received from persons suspected of being involved with the offense. *Id.* at 974. We also noted the warrants should have only requested data from the period of time during which the defendant was suspected of taking part in a conspiracy. *Id.* We ultimately concluded, however, that although the Facebook warrants violated the particularity requirement, they were not so facially deficient the officers could not have reasonably believed them to be valid. *Id.* at 975.

The district court did not err when it denied Alford's motion to suppress all evidence found as a result of the Montana search warrant because the warrant was sufficiently particular and not overbroad. *See United States v. Hollis*, 780 F.3d 1064, 1068 (11th Cir. 2015) (stating when reviewing the denial of a motion to suppress, we review the district court's legal conclusion *de novo* and its findings of fact for clear error). The warrant here falls somewhere between the Microsoft and Facebook warrants in *Blake* because, like the Facebook warrants, it requested

nearly every kind of data that could be found in a Google account, but like the Microsoft warrant, the information requested was all potentially incriminating because it could have identified the K-Mart caller. *See Blake*, 868 F.3d at 973-74. However, using a practical margin of flexibility, the warrant here was as specific as the circumstances and nature of the activity under investigation permitted. *See United States v. Bradley*, 644 F.3d 1213, 1259 (11th Cir. 2011) (explaining the particularity requirement must be applied with a practical margin of flexibility); *United States v. Moody*, 977 F.2d 1425, 1432 (11th Cir. 1992) (stating a description of the property to be seized will be acceptable if it is as specific as the circumstances and nature of the activity under investigation permit). The only information Officer Brunner-Murphy had when drafting the language of the warrant was a phone call to K-Mart from an anonymous Google Voice phone number. Under those circumstances, the warrant was as limited as possible because it requested the account information of only the Google user who called the K-Mart at the specific time in question. Although the warrant requested nearly every kind of data that could be found in a Google account, any of that data could have helped identify the owner of the account. Brunner-Murphy was not merely rummaging around Alford's Google account to find whatever he could, but rather was trying to find the identity of the caller and potential victim. *See Blake*, 868 F.3d at 973. As to Alford's argument that it was wrong for Brunner-Murphy to

look for a victim under the language of the search warrant, that question was related to the identity of the caller because the caller claimed the victim was his daughter. Thus, under the specific circumstances and nature of the activity under investigation, the warrant was as limited as possible because all of the evidence seized could have helped identify the owner of the Google account.

The district court also did not err in concluding that, even if the warrant was insufficiently particular and overbroad, the evidence would not need to be suppressed under the good-faith exception. *See Blake*, 868 F.3d at 974-75 (explaining even where a search warrant was overbroad, the evidence seized need not be suppressed where it was obtained in objectively reasonable reliance on a subsequently invalidated search warrant). Alford does not contend on appeal that the search was so lacking in indicia of probable cause as to render official reliance on it unreasonable. Moreover, as in *Blake*, the warrant was not so facially deficient that Brunner-Murphy could not have reasonably presumed it to be valid. *See United States v. Leon*, 468 U.S. 897, 923 (1984) (stating exclusion could still be warranted if: (1) the warrant was based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable;" or (2) the warrant was "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers [could not have] reasonably presume[d] it to be valid"). The goal of the warrant was to

identify the K-Mart caller, and all of the evidence furthered that goal. Even if the warrant should have been further limited in scope, it is a close question and the warrant was not so obviously flawed that Brunner-Murphy could not have reasonably believed it to be valid. *See Blake*, 868 F.3d at 975. Accordingly, even if the warrant was insufficiently particular and overbroad, the evidence need not have been suppressed because Brunner-Murphy's reliance on it was objectively reasonable.

B. Propensity Evidence

Second, Alford argues the district court abused its discretion by admitting improper propensity evidence at trial, specifically, child erotica found on Alford's computer. "Evidence of a crime, wrong, or other act is not admissible to prove a person's character in order to show that on a particular occasion the person acted in accordance with their character." Fed. R. Evid. 404(b)(1). However, such evidence may be admissible for another purpose, such as proving intent, knowledge, absence of mistake, or lack of accident. Fed. R. Evid. 404(b)(2).

The district court did not abuse its discretion by allowing the Government to present evidence of child erotica found on the computer. *See United States v. Edouard*, 485 F.3d 1324, 1343 (11th Cir. 2007) (stating a district court's evidentiary rulings are ordinarily reviewed for an abuse of discretion). First, Rule 404(b) does not apply because the evidence of child erotica was intrinsic to the

charged offenses. *See United States v. Ford*, 784 F.3d 1386, 1394 (11th Cir. 2015) (stating Rule 404(b) does not apply to evidence that is intrinsic to the charged offenses). The child erotica was an integral and natural part of Dowdy's testimony about the search of the computers because it provided further context about the search records found on the computers. *See United States v. Ramsdale*, 61 F.3d 825, 829 (11th Cir. 1995) (explaining evidence is intrinsic if it arose out of the same transaction or series of transactions as the charged offense, is necessary to complete the story of the crime, or is inextricably intertwined with the evidence regarding the charged offense). Although the child erotica was not illegal, its presence on the computers was an important part of the circumstances surrounding the offense given the existence of search terms like "7yro+preteen," even if it reflected negatively on Alford's character. *See Edouard*, 485 F.3d at 1344 (stating evidence is inextricably intertwined with evidence regarding the charged offense, and therefore admissible, if it forms an "integral and natural part of the witness's accounts of the circumstances surrounding the offenses").

Second, even if the evidence of child erotica was extrinsic, it was admissible under Rule 404(b) because it helped prove intent, knowledge, and lack of mistake or accident. This case is analogous to *United States v. Kapordelis*, 569 F.3d 1291, 1313 (11th Cir. 2009), where we concluded that the defendant's prior trips to the Czech Republic to engage in sexual trysts with underage boys were admissible

under Rule 404(b) as proof of knowledge, identity, or absence of mistake or accident with regard to his collection of child pornography. *Id.* Here, the user of the computer legally downloaded a large amount of child erotica, and the district court properly concluded the child erotica was admissible under Rule 404(b) as proof of knowledge, identity, or absence of mistake or accident. This was not merely a propensity argument because someone who downloads child erotica is more likely to recognize child pornography and not download it by mistake. *See* Fed. R. Evid. 404(b)(1). Although the court stated that "somebody who is interested in [child erotica] is more likely to be interested in child pornography," it was referring to the probative value of the evidence for proving intent or lack of mistake, not merely a propensity argument.

Finally, under Rule 403, the probative value of the child erotica was not substantially outweighed by its prejudicial effect because the jury was already shown examples of child pornography and they were not likely to convict Alford on the child pornography charges based on the child erotica. *See* Fed. R. Evid. 403 (providing the district court may exclude relevant evidence if its probative value is substantially outweighed by a danger of unfair prejudice). And Alford specifically challenged the knowledge element of the offense, which increased the probative value of the child erotica. *See Kapordelis*, 569 F.3d at 1313-14 (concluding the probative value of the prior-bad-acts evidence was substantial and outweighed the

prejudicial effect where the defendant specifically challenged the knowledge element of the offense). Notably, the court told Alford it would give an instruction to the jury about the proper consideration of the child erotica evidence if he requested one, but Alford never requested the instruction at trial and did not object to the court's instructions. As a result, the court gave an instruction regarding the proper consideration of Alford's prior conviction, but not the child erotica. Accordingly, the district court did not abuse its discretion by allowing the Government to present evidence of child erotica found on the computer because it was either intrinsic, and thus outside the scope of Rule 404(b), or admissible under Rule 404(b) because it helped prove intent, knowledge, and lack of mistake or accident.

C. Sufficiency of the Evidence

Finally, Alford argues the Government presented insufficient evidence to prove that he knowingly received or attempted to receive child pornography. Any person who knowingly receives or distributes any child pornography that has been shipped or transported in interstate commerce by any means, including by computer, violates the law. 18 U.S.C. § 2252A(a)(2). A person "knowingly receives" child pornography when he intentionally views, acquires, or accepts child pornography on a computer from an outside source. *United States v. Pruitt*, 638 F.3d 763, 766 (11th Cir. 2011). An intentional viewer of child pornography

may be convicted regardless of whether he saves the images to a hard drive, edits them, or otherwise exerts more control over them. *Id.* However, inadvertent receipt of child pornography is not a violation of the statute. *Id.* Evidence that a person has searched for child pornography on the internet and has a computer containing child-pornography images, whether in the hard drive, cache, or unallocated spaces, can count as circumstantial evidence that they knowingly received child pornography. *Id.*

As an initial matter, plain error review applies because Alford's motion for a judgment of acquittal was insufficient to preserve the specific argument he now raises. *See United States v. Joseph*, 709 F.3d 1082, 1103 (11th Cir. 2013) (stating plain error review applies where a defendant raises a general insufficient evidence argument below and then seeks to challenge the sufficiency of the evidence supporting a specific element of the crime on appeal). However, regardless of whether reviewed *de novo* or for plain error, the Government presented sufficient evidence that Alford knowingly received or attempted to receive child pornography. A reasonable jury could have concluded that it was Alford who downloaded the child pornography, not someone else, based on the evidence that: (1) the "michellecuty013" e-mail address belonged to Alford; (2) his parents could not use the computer without his help; and (3) both computers were used to sign on to the "michellecuty013" account and were used as part of Alford's business.

Second, a reasonable jury could have concluded that Alford had previously viewed the images in the thumbcache based on Investigator Dowdy's testimony that these images would not exist as thumbnails if they had not been viewed on the computer. Dowdy also testified that the computer contained a program that could recover deleted files and that child pornography was in a folder created by the program. Although Alford presented testimony that it was not uncommon for computers to save thumbnails of images that were never opened, the jury was entitled to believe Dowdy's testimony, and this court must resolve all reasonable credibility evaluations in favor of the jury's verdict. *See United States v. Doe*, 661 F.3d 550, 560 (11th Cir. 2011) (stating this Court must draw all reasonable inferences in favor of the jury's verdict).

Third, a reasonable jury could have concluded Alford did not access the child pornography inadvertently based on the evidence that the search history on both computers included terms that would normally return child pornography. These search terms, combined with the existence of child pornography on the computer, were circumstantial evidence that Alford knowingly received child pornography. *See Pruitt*, 638 F.3d at 766. Finally, a reasonable jury could have concluded that Alford had opened or viewed the e-mails containing child pornography because, although there was no direct evidence that Alford opened or viewed the e-mails, there would have been no record of the e-mails had he deleted

them. Given this evidence, the jury could have reasonably drawn the inference that Alford knowingly received child pornography. *See Doe*, 661 F.3d at 560; *Pruitt*, 638 F.3d at 766. Accordingly, the Government presented sufficient evidence that Alford knowingly received or attempted to receive child pornography.

II. CONCLUSION

The district court did not err by refusing to suppress evidence obtained as a result of a search warrant issued to Google because the warrant was sufficiently particular and not overbroad under the specific circumstances and the nature of the activity under investigation. Second, the district court did not abuse its discretion by allowing the Government to present evidence of child erotica found on a computer because it helped prove intent, knowledge, and lack of mistake or accident. Finally, the Government presented sufficient evidence for a reasonable jury to conclude that Alford knowingly received or attempted to receive child pornography where it presented evidence supporting an inference that he used the e-mail and computers containing child pornography, he searched for and viewed the child pornography, and he had not deleted the e-mails containing child pornography. Accordingly, we affirm Alford's conviction.

AFFIRMED.