NOT FOR PUBLICATION

In the
United States Court of Appeals
For the Eleventh Circuit

No. 24-12038
Non-Argument Calendar

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

GREGORY ALLEN WILLIAMSON,
a.k.a. Vlad Vlad,

Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida
D.C. Docket No. 8:21-cr-00355-WFJ-CPT-1

Before JORDAN, JILL PRYOR, and KIDD, Circuit Judges.

PER CURIAM:

Gregory Allen Williamson appeals his convictions for coercion and enticement of a minor to engage in sexual activity, in

violation of 18 U.S.C. § 2422(b); attempted production of child pornography, in violation of 18 U.S.C. § 2251(a) and (e); production and attempted production of child pornography, in violation of 18 U.S.C. § 2251(a) and (e); distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1); and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2).

Williamson argues that the district court erred in denying two motions to suppress evidence obtained from searches of his email account and residence. He argues that the first motion should have been granted because (1) Yahoo, Inc., and the National Center for Missing and Endangered Children ("NCMEC") functioned as agents of the government when they reviewed the contents of his email account, (2) law enforcement's review of the contents of his email account exceeded the scope of Yahoo's initial search, (3) the officer who applied for a search warrant of Williamson's home recklessly made material misrepresentations and omitted material facts when applying for the warrant, and (4) the good-faith exception to the exclusionary rule does not apply to this case. He also contends that the Yahoo search warrant violated the Fourth Amendment's particularity requirement and that the good-faith exception to the exclusionary rule does not apply.

For the reasons explained below, we affirm Williamson's convictions.

I. BACKGROUND

In the section that follows, we trace how Yahoo's flagging of an email containing child sexual abuse material ("CSAM") led law enforcement to seek search warrants for Williamson's email account and residence, eventually resulting in criminal charges against Williamson. We then describe the procedural history of Williamson's criminal case.

A. Offense Conduct and Investigation

1. Yahoo and NCMEC's Initial Reviews

This case started with a tip from Yahoo, a private corporation and electronic service provider. Yahoo offers its customers various services, including email. To use these services, Yahoo's customers must first agree to the company's terms and conditions. These terms and conditions provide that a customer cannot email or transmit through its service any unlawful content, which includes CSAM. The terms also provide that the company may prescreen, access, and disclose the contents of its users' accounts under certain circumstances, including when the user transmits CSAM.

Yahoo uses hash values to search its users' communications. A hash value is "a sort of digital fingerprint." *United States v. Sotelo*, 130 F.4th 1229, 1241 n.3 (11th Cir. 2025). "After companies assign a hash value to a known image of child pornography, they can scan their services for files with the same value. When they get a match, they know that the scanned file is a duplicate of the child-pornography image without opening and viewing the file." *Id.* (citation

omitted). Yahoo scans emails sent by its users against a CSAM "hash list," which is a list of CSAM hash values.

When Yahoo's scan reveals that an attachment to an email matches the CSAM hash list, the company then uses a human moderator to examine the image. If the human moderator determines that a particular file contains illegal pornography, all the images in the user's account are archived and analyzed for additional illegal material. The moderator manually verifies that he has examined the suspect files. If the moderator is unsure whether an image qualifies as CSAM, he consults with Yahoo's legal counsel. If the moderator identifies any CSAM, Yahoo then sends a report to NCMEC, a non-profit organization receiving federal funding that operates the CyberTipline, a nationwide mechanism through which CSAM is recorded and reported.

This reporting is required by federal law. When an electronic service provider, like Yahoo, has "actual knowledge of any facts or circumstances" indicating that an individual appears to have violated a child pornography law, it must take certain steps. 18 U.S.C. § 2258A(a)(1). One of the required steps is to make a report to NCMEC's CyberTipline.[1] *Id.* § 2258A(a)(1)(B)(ii). Yahoo is aware of its obligations under federal law. Still, as a Yahoo employee testified before the trial court, Yahoo voluntarily scans for

[1] A provider that knowingly and willfully fails to make a report is subject to hundreds of thousands of dollars in fines. *See* 18 U.S.C. § 2258A(e).

CSAM to keep its users safe and create a safe environment on its platform.

Once an electronic service provider submits a CyberTipline report, NCMEC takes it from there by conducting an independent review of the submitted images and their hash values. NCMEC has lists for various types of images, including "apparent [child pornography]," "CP unconfirmed," and more. Doc. 99 at 23–24.[2] An image is labeled "apparent child pornography" when it meets the federal definition of child pornography and clearly depicts a child. *Id.* at 66. In contrast, an image is labeled "CP unconfirmed" when the activity depicted appears to meet the federal definition of child pornography but there is some question as to the age of the person in the image. *Id.* at 35. At least two NCMEC analysts must review a file and come to the same conclusion before an image is put on a hash list.

When NCMEC runs its hash value analysis for an image, one of two things happens: if there is a match between a value on one of NCMEC's lists and the reported image, the image gets the same designation. So, for example, if a reported image's hash value matches that of an image on the "apparent child pornography" list, the reported image is also categorized as "apparent child pornography." But if there is no match between NCMEC's list and the reported image, NCMEC does its own analysis and assigns the image what it believes is the correct label.

---

[2] "Doc." numbers refer to the district court's docket entries.

NCMEC conducts its own analysis of an image only if the reporting electronic service provider attests that either (1) it has viewed the contents of the file, or (2) the contents of the file were publicly available. NCMEC forwards any CyberTipline reports that warrant further review to the appropriate law enforcement agency or department.

This process was followed here. Yahoo flagged an email account with the username "vladlover50@yahoo.com" for sending correspondence with an attachment matching the hash value of known CSAM. One of Yahoo's moderators archived all the images and videos in that account. Yahoo's moderation team reviewed the emails and found seven images it believed to be illegal CSAM. But, importantly, when a Yahoo employee was later asked which moderator reviewed each image, she was unable to identify the team member who reviewed each file.

Two days later, Yahoo submitted a CyberTipline report to NCMEC with the seven images and disabled the "vladlover50@yahoo.com" account. Yahoo's report included the phone number associated with the email account, the date and time the account sent the first email that Yahoo flagged, and the account's IP address at the time. For each of the seven files, Yahoo affirmed in its report that it had viewed the contents of the file.

NCMEC generated its own report. Its report stated that NCMEC had not opened or viewed the files and that the hash values matched files it had previously reviewed. The statement that NCMEC had not opened or viewed the seven files turned out to be

incorrect; NCMEC had reviewed six of the files. Of the seven files sent by Yahoo, NCMEC categorized four as "CP (Unconfirmed)," two as "Apparent Child Pornography," and one as "Child Clothed."

NCMEC traced the IP address Yahoo had provided for the "vladlover50@yahoo.com" account to North Port, Florida. It then forwarded the CyberTip to the Central Florida Internet Crimes Against Children task force, as well as the North Port Police Department.

2. Law Enforcement's Review and Search Warrant Applications

Upon receiving the tip from NCMEC, the North Port Police Department assigned the case to Detective James Keller. Keller reviewed NCMEC's report and the seven files it included. At that time, Keller did not review any files other than those seven. Keller then issued a subpoena to Comcast, the internet service provider for the "vladlover50@yahoo.com" account's IP address, and learned the residential address of the individual using the account.

After reviewing the seven images and concluding that some of the files contained CSAM, Keller sought a search warrant for the "vladlover50@yahoo.com" account (the "Yahoo warrant"). The application for the Yahoo warrant set forth facts in support of the warrant. It discussed Keller's background and familiarity with criminal investigations related to child sexual abuse. It then described the seven suspect images in graphic detail, classifying four of them as "child sexual abusive material," one as legal child erotica, and

the last two as "age difficult." Doc. 134-1 at 4–5. These facts, the application stated, gave rise to probable cause to search and seize evidence from the Yahoo account.

Keller sought to use the search warrant to obtain categories of information pertaining to the "vladlover50@yahoo.com" account. The search warrant requested (1) account information, (2) evidence of who used the account, (3) all calendars and contacts in the account, (4) all email messages in the account, (5) all media files associated with the account, and (6) all search history from the account. A state court judge issued a search warrant for the information requested.

Through information obtained from the Yahoo warrant, law enforcement officers learned that the "vladlover50@yahoo.com" email account had been used to send CSAM to a minor's email account. They further determined that, over the course of several months, the email in question had sent a series of images and messages to the minor, a female child in Gregory Williamson's family. The emails included CSAM. Further investigation provided reason to believe Williamson was the person communicating with the minor.

Keller applied for a search warrant for the residence linked to the IP address in the CyberTip, using a warrant application that largely mirrored the first one. The application described each of the seven files, classifying four of them as "child sexual abusive material." Doc. 48-2 at 5. Importantly, Keller's second warrant application also included the labels that NCMEC had given each of the

images. The warrant affidavit recited that NCMEC had categorized three of the images as "Child Pornography" and one of them as "Apparent Child Pornography." *Id.* But this was a mistake: NCMEC's report actually had classified three of the images as "CP (Unconfirmed)." Doc. 48-1 at 9. Unaware of this error, a state court judge issued a search warrant for Williamson's home, seeking various electronic devices, correspondence, and documents (the "residential search warrant").

Law enforcement executed the warrant. At Williamson's residence, they located several electronic devices, including a computer, a cellular phone, and two hidden cameras. Forensic analyses of these devices revealed scores of illegal materials, including images and videos of the minor victim, as well as other CSAM. Analysts also discovered data connecting the seized computer to the "vladlover50@yahoo.com" email address.

B. Williamson's Criminal Case

A federal grand jury charged Williamson with child sex-related offenses. He pleaded not guilty. In the criminal case, he filed two motions to suppress evidence. In his first motion, he argued that Yahoo was a state actor when it searched the "vladlover50@yahoo.com" account, and thus his constitutional rights were violated when the company searched his emails without obtaining a warrant. His motion made a similar argument about NCMEC. Williamson further argued that, even if Yahoo acted as a private entity during the search, law enforcement had exceeded the scope of that private search.

Williamson's first motion also challenged the warrant application itself. He contended that the search warrant application for his residence included material misrepresentations and omissions, rendering the subsequent search unconstitutional. Specifically, he argued that the warrant application misrepresented whether the images first discovered on the "vladlover50@yahoo.com" account were all CSAM, a defect he contended was fatal to the warrant's constitutionality. He also argued that Yahoo's records showed that the last login to the account was on September 5, 2020, three days before the illegal image was uploaded, and that Detective Keller's failure to explain the discrepancy was a material omission.

The magistrate judge recommended that Williamson's first motion to suppress be denied. Relevant to this appeal, the magistrate judge concluded that Yahoo was not a government actor. He recognized that Yahoo was required to report online sexual child exploitation to NCMEC and would be subject to sanctions otherwise. Still, the magistrate judge concluded that mere compliance with the law was insufficient to make Yahoo a government actor. He further noted that the relevant statute, 18 U.S.C. § 2258A, imposed only an obligation to report known child pornography, not to search for it, leaving the decision to search users' data for illegal material up to Yahoo. Moreover, the magistrate judge highlighted that (1) there was no evidence that the government either instigated or cooperated with Yahoo's review of the emails, and (2) Yahoo had an independent interest in safeguarding both the individuals who use its services and its own reputation, providing ample incentive to search emails sent on the platform. For these reasons,

the magistrate judge concluded that Yahoo was not acting as a state actor when it searched Williamson's emails. And although Williamson claimed that NCMEC was also a state actor, the magistrate judge did not reach that issue because, even if it were, NCMEC's examination of the materials did not exceed the scope of Yahoo's review. The magistrate judge made a similar finding as to the scope of Detective Keller's review. Over Williamson's objection, the district court adopted the magistrate judge's recommendation and denied the first motion to suppress.

Williamson filed a second motion to suppress. The second motion took a different approach, contending that the Yahoo search warrant was unconstitutionally overbroad. Because the good-faith exception did not apply to the warrant, Williamson argued, the results of the Yahoo search warrant should have been excluded.

The magistrate judge recommended that the district court reject Williamson's second motion's arguments. He found that the warrant was sufficiently particularized, but even if not, the good-faith exception applied to the warrant. Williamson objected to the magistrate judge's recommendation. After a hearing, the district court adopted the magistrate judge's recommendation and denied the second motion to suppress.

After the court denied the motions to suppress, Williamson was tried by a jury, who found him guilty on all counts. The district court sentenced him to a term of life imprisonment. This timely appeal followed.

II. STANDARD OF REVIEW

"A district court's ruling on a motion to suppress presents a mixed question of law and fact." *United States v. Zapata*, 180 F.3d 1237, 1240 (11th Cir. 1999). We review the district court's factual findings for clear error and its application of the law to the facts *de novo*. *Id*. Further, all facts are construed in the light most favorable to the party that prevailed below, here, the government. *See United States v. Bervaldi*, 226 F.3d 1256, 1262 (11th Cir. 2000). We also review *de novo* whether the good-faith exception to the exclusionary rule applies to a particular case. *United States v. Martin*, 297 F.3d 1308, 1312 (11th Cir. 2002).

III. DISCUSSION

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and provides 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. On appeal, Williamson argues that his Fourth Amendment rights were violated when the government searched his email account and later searched his home. We address each issue in turn.

A. Challenges to the Searches of the Yahoo Account

On appeal, Williamson challenges the searches of his email account. First, he argues that Yahoo was acting as a government actor when it searched his account. Because Yahoo was acting pursuant to federal law, received special immunity for its actions, and

would otherwise be subject to harsh penalties if it failed to comply, Williamson argues, it was acting as an agent of the government. He makes a similar argument that NCMEC was a government actor. He further argues that, even if we conclude that Yahoo acted as a private entity when it searched his account, law enforcement exceeded the scope of Yahoo's search. Finally, Williamson asserts that the Yahoo search warrant, which enabled law enforcement to conduct a more expansive search of the account, was insufficiently particularized, violating the Fourth Amendment.

We now address each of these arguments.

1. Whether Yahoo Acted as a Private Entity when It Searched Williamson's Email Account

Although the Fourth Amendment protects the right to be free from "unreasonable searches and seizures," U.S. Const. amend. IV, this constitutional protection is wholly inapplicable to "a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (citation omitted). In determining whether a private entity should be considered an agent of the government for Fourth Amendment purposes, "we look to two critical factors: (1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the private actor's purpose was to assist law enforcement efforts rather than to further his own ends." *United States v. Steiger*, 318 F.3d 1039,

1045 (11th Cir. 2003).[3] We also consider whether the government "openly encouraged or cooperated in the search." *See United States v. Ford*, 765 F.2d 1088, 1090 (11th Cir. 1985). The district court's determination that a private entity was not acting as an agent of the government is reviewed for clear error. *See id.*

Here, the district court concluded that Yahoo acted as a private entity, not an agent of the government, when it searched Williamson's email account. This conclusion was not clearly erroneous. As to the first factor, the record is devoid of evidence that the government either knew of or acquiesced in Yahoo's search. As to the second factor, the evidence shows that Yahoo searched Williamson's emails to further its own ends, namely, keeping its users safe and creating a safe online environment. Nor is there any evidence in the record that the government openly encouraged Yahoo to search Williamson's emails or cooperated in the search. The district court's conclusion that Yahoo acted as a private entity is amply supported by the record.

Williamson does not point us to evidence undermining the district court's conclusion. He argues instead that Yahoo's legal obligations necessarily indicate that the government knew of Yahoo's

---

[3] Williamson seems to suggest that we should import the test for state action under 42 U.S.C. § 1983 into the Fourth Amendment arena. *See* Appellant's Br. 28 (citing *Washington v. Veterans of Foreign Wars of U.S.*, 196 F. App'x 777, 779 (11th Cir. 2006) (unpublished)). But under our binding precedent, we apply the two-factor test in *United States v. Steiger* to determine whether a private entity is a government agent whose actions implicate the Fourth Amendment, not a § 1983 state action test. *See Steiger*, 318 F.3d at 1045.

activities. In his view, the fact that federal law required Yahoo to report findings of suspected child pornography lest it be subject to significant penalties is enough to show that the government had the requisite knowledge.

Williamson misunderstands the inquiry. The relevant question is not whether the government knew that the entity conducted searches; it is whether the government knew of and acquiesced in the challenged conduct. *See United States v. Simpson*, 904 F.2d 607, 609–10 (11th Cir. 1990) (looking, for purposes of the private party inquiry, not at whether the government knew that Federal Express searched parcels, but at whether the government instructed Federal Express employees to open and inspect the box in that case). That Yahoo scans emails and reports CSAM does not mean that the government had any knowledge of, or role in, Yahoo's search of the "vladlover50@yahoo.com" account. And as Yahoo's employee testified, the company voluntarily chooses to scan its users' accounts for CSAM.

Williamson also argues that the first factor was satisfied because federal law compelled "Yahoo and other ESPs to proactively search for child pornography." Appellant's Br. 29. Not so. Yahoo's reporting obligation only arose once it had "actual knowledge of any facts or circumstances" indicating that an individual had violated a child pornography law. *See* 18 U.S.C. § 2258A(a)(1). When Yahoo first scanned Williamson's email, it had no actual knowledge that he had violated the law, and thus, no reporting

obligation. Williamson's argument is contrary to what the law actually requires.

Williamson likens this case to *United States v. Henry*, 447 U.S. 264 (1980), arguing that Yahoo is essentially a confidential informant. In *Henry*, the Supreme Court considered whether a defendant's Sixth Amendment right to counsel was violated when the government sought to introduce incriminating statements made to a covert government informant while the defendant was in custody after indictment. 447 U.S. at 269. *Henry* says nothing about the issue here, which is whether Yahoo's search can be attributed to the government.

Evidence relevant to the second factor, whether Yahoo's purpose was to assist law enforcement efforts rather than to further its own ends, also supports the district court's conclusion. The district court heard—and credited—testimony from Yahoo that it knew it was not required to scan for CSAM but did so of its own accord. Yahoo's employee also testified that the company searches email accounts for CSAM because it wants to keep its users safe and create a safe environment on its platform. The district court did not clearly err in finding that Yahoo conducted the search in this case to further its own business interests.

Williamson disagrees, pointing, in part, to the fact that Yahoo's searches turn no profit. But the second factor does not require a private entity to turn a profit for its actions to be in furtherance of its own ends. *See, e.g.*, *United States v. Castaneda*, 997 F.3d 1318, 1328 (11th Cir. 2021) (concluding that two private individuals

who turned over incriminating evidence to law enforcement were not acting as government agents because they acted out of a desire to avoid prosecution themselves). Profit can be a motivation, sure. But preserving one's own reputation can surely be one, too. As the record shows, Yahoo has an independent interest in rooting out illegal activity on its platform. The district court did not err when it came to the same conclusion. Thus, we find no clear error in the district court's determination that Yahoo acted as a private entity, not a government agent.

2. Whether NCMEC's Search Exceeded the Scope of Yahoo's Search

Williamson's next argument is that NCMEC acted as an agent of the government for Fourth Amendment purposes. Highlighting that NCMEC is tasked with operating the CyberTipline and receives funding from the government, Williamson contends that NCMEC serves as a government actor. When Williamson pressed this argument below, the district court concluded that it need not reach this question because, even if NCMEC was acting as a government actor, its search did not exceed the scope of the search Yahoo conducted.

"Law enforcement agents may use in an application for a search warrant information that is given to them by a private party even if that private party unlawfully obtained the information." *Castaneda*, 997 F.3d at 1328. When a private actor initially invades an individual's privacy, any invasion of privacy by the government must be tested by the degree to which it exceeded the scope of the private search. *Jacobsen*, 466 U.S. at 115. Once a private entity,

acting of its own accord, conducts a search—even one that frustrates a defendant's reasonable expectation of privacy—the Fourth Amendment does not forbid the government from replicating the search, so long as government officials constrain their search to the parameters of the search the private entity conducted. *United States v. Young*, 350 F.3d 1302, 1306–07 (11th Cir. 2003).

Like the district court, we find it unnecessary to decide whether NCMEC acted as a government actor because any search NCMEC conducted stayed within the parameters of Yahoo's initial search. Recall how the searches unfolded in this case: Yahoo, a private actor, flagged Williamson's account as having CSAM. Yahoo employees then archived Williamson's emails, reviewed the correspondence, and found seven images that the company believed contained child pornography. In its report to NCMEC, Yahoo affirmed that it had viewed the entire contents of each of the seven suspect files. NCMEC went on to review six of the seven reported files.

Under this set of facts—which Williamson does not contest—there is no need to determine whether NCMEC was a government actor. NCMEC's search was coextensive with Yahoo's search; NCMEC did not review any files that Yahoo had not first reviewed. And so, even if we were to assume that NCMEC was a government actor, its search did not exceed the parameters of Yahoo's search, and there was no Fourth Amendment violation.

3. Whether Law Enforcement's Search Exceeded the Scope of Yahoo's Search

Williamson further asserts that, even if we find that Yahoo was a private actor, law enforcement exceeded the scope of Yahoo's search when it reviewed the files. According to Williamson, the government failed to establish the scope of the search because the government presented no testimony from the employees of Yahoo and NCMEC who viewed the suspect images.

The district court found otherwise. The court credited a Yahoo employee's testimony that the company's agents review all images that are submitted in a NCMEC report. It also credited Keller's testimony that he looked only at images that were first reviewed by Yahoo and NCMEC before seeking the search warrants. Based on this evidence, the district court concluded that Keller's review did not exceed the parameters of Yahoo's search.

The district court did not err in its conclusion. The district court found that Keller's search stayed within the parameters of the search Yahoo conducted. And since Yahoo was a private actor, Keller was permitted to search the seven files originally flagged by the company without violating the Fourth Amendment.

Williamson makes much of the fact that the government failed to present testimony from the Yahoo agent who viewed each image. He is right that a Yahoo employee testified that she was unable to identify which Yahoo moderator viewed each of the seven images. But there is no requirement that the government present testimony from the person who reviewed the files; its burden is to

present sufficient evidence from which the district court could conclude that the searches at issue did not violate Williamson's rights. The district court heard testimony that specifically identified the Yahoo employees who archived and reviewed Williamson's files. The court also credited testimony that a human moderator at Yahoo must review suspect images before it can submit a report to NCMEC. This is a sufficient factual basis for the court's conclusions.

Williamson suggests that the district court improperly based its conclusions on the existence of a "largely undefined company policy." Appellant's Br. 38–40. Not so. The district court received evidence in addition to information about Yahoo's policies. We see no clear error in the district court's findings of fact.

4. Particularity of the Search Warrant

Williamson also contends that the Yahoo search warrant was insufficiently particularized. Because the warrant was not tailored to the activity under investigation and was facially overbroad, Williamson maintains, the warrant was unconstitutional and the good-faith exception did not apply. The government disagrees, contending that the Yahoo warrant was sufficiently particularized. And even if it was not, the government asserts, the good-faith exception applies and suppression was not required.

The Fourth Amendment requires search warrants to "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity requirement is intended to protect individuals from "being subjected

to general, exploratory searches." *United States v. Khanani*, 502 F.3d 1281, 1289 (11th Cir. 2007). Generally, under the well-known exclusionary rule, "[e]vidence seized as the result of an illegal search may not be used by the government in a subsequent criminal prosecution." *Martin*, 297 F.3d at 1312. And if a warrant runs afoul of the particularity requirement, evidence seized under that warrant may be suppressed under this rule. *United States v. Travers*, 233 F.3d 1327, 1329 (11th Cir. 2000).

"To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, 555 U.S. 135, 144 (2009). "[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id*. But suppressing evidence does not help achieve these goals "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *United States v. Leon*, 468 U.S. 897, 920 (1984). "After all, it is the magistrate's responsibility to determine whether the officer's allegations establish probable cause and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment." *United States v. Morales*, 987 F.3d 966, 973 (11th Cir. 2021) (citation modified).

Enter the good-faith exception. That exception "requires suppression only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively

reasonable belief in the existence of probable cause." *Martin*, 297 F.3d at 1313 (citation modified). The government has the burden of demonstrating that the good-faith exception applies, and it can meet its burden by referencing facts in the affidavit. *United States v. Robinson*, 336 F.3d 1293, 1297 (11th Cir. 2003).

The Supreme Court has identified four situations where the good-faith exception does not apply: (1) where the magistrate or judge was misled by information the affiant knew was false or was reckless in determining its veracity; (2) where the magistrate or judge wholly abandoned her judicial role; (3) where the warrant is based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where a warrant is so facially deficient that the executing officers cannot reasonably presume it to be valid. *Leon*, 468 U.S. at 923. "If none of these four circumstances exists, we proceed to determine whether the executing officer reasonably relied upon the search warrant." *Morales*, 987 F.3d at 974 (citation modified).

Our decision in *United States v. Blake*, 868 F.3d 960 (11th Cir. 2017), is instructive on both the particularity of the Yahoo warrant and the good-faith exception. In that case, we affirmed the district court's denial of a motion to suppress, holding that warrants issued to Microsoft and Facebook came under the good-faith exception. *Id.* at 973–75. In reaching our conclusion, we discussed the Fourth Amendment's particularity requirement. We concluded that the Microsoft warrant, which sought limited data related only to emails that had the potential to contain incriminating evidence,

complied with the particularity requirement. *Id.* at 973. We contrasted that with the Facebook warrants, which unnecessarily required disclosure of "virtually every kind of data that could be found in a social media account." *Id.* at 974. But we declined to decide whether the Facebook warrants were sufficiently particularized because we concluded that all the warrants fell within the good-faith exception to the exclusionary rule. *Id.* We reasoned that the warrants were supported by probable cause and were not so facially deficient that the executing officers could not have reasonably believed them to be valid. *Id.* at 975.

We reach a similar conclusion here. Williamson is correct that the Yahoo warrant in this case is broader than the Microsoft warrant at issue in *Blake*. The Microsoft warrant was limited to specified categories of emails that were linked to the charges at issue. *Id.* at 966. Compare that to the Yahoo warrant in this case, which sought (1) account information, (2) evidence of who used the account, (3) all calendars and contacts in the account, (4) all email messages, (5) all media files associated with the account, and (6) all search history from the account. The Yahoo warrant certainly cast a much wider net.

But we need not determine whether the Yahoo warrant was too broad because the good-faith exception applies. None of the four situations in which the good-faith exception does not apply is present here.

Williamson disagrees, arguing that the Yahoo warrant was so facially deficient that the executing officers could not have

reasonably presumed it to be valid. A warrant falls within this category when, for example, it fails to "particularize the place to be searched or the things to be seized." *Martin*, 297 F.3d at 1313 (quoting *Leon*, 468 U.S. at 923).

That was not true here. The Yahoo warrant identified the place to be searched (the Yahoo account) and the things to be seized (information from the account). Although the warrant was not the most particularized—after all, it sought large swaths of information that could be found in the email account—it was not so broad that the executing officers could not have reasonably presumed its validity. We have reached a similar conclusion in similar cases. *See, e.g.*, *Blake*, 868 F.3d at 973–75 (concluding that a warrant that sought "virtually every kind of data that could be found in a social media account" was not so broad that it fell outside the good-faith exception); *United States v. McCall*, 84 F.4th 1317, 1328–29 (11th Cir. 2023) (concluding that a warrant that had no temporal limitation and sought most of an account's conceivable data was not so facially deficient that officers could not have reasonably relied on it). We see nothing so egregious about the warrant that it falls outside the umbrella of the good-faith exception.

Lastly, as to whether the executing officers reasonably relied on the warrant, "[w]e have held that in all but the most unusual circumstances, it is objectively reasonable for a law enforcement officer to rely on a court order." *McCall*, 84 F.4th at 1329 (citation modified). Here, nothing about the warrant or the surrounding circumstances of the search would render an officer's reliance on the

warrant objectively unreasonable. Law enforcement therefore reasonably relied on the Yahoo warrant, and the good-faith exception saves the fruits of that search.

B. Challenges to the Residential Search Warrant

Williamson challenges the sufficiency of the residential search warrant as well. He argues that he was entitled to a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). He asserts that Keller "recklessly omitted material facts and made material misrepresentations in the application for the [residential] search warrant," vitiating any probable cause found there. Appellant's Br. 42. And he says that the good-faith exception does not apply to the evidence seized pursuant to that warrant.

A search warrant affidavit is presumptively valid. *Franks*, 438 U.S. at 171. But in *Franks*, the Supreme Court held that a defendant is entitled to a hearing on the validity of an affidavit if he made a substantial preliminary showing that the affiant included a false statement made knowingly and intentionally, or with reckless disregard for the truth, and the allegedly false statement was necessary to the finding of probable cause. *Id.* The search warrant must be voided, and fruits of the search excluded under *Franks*, where: (1) at the hearing, the defendant established the allegation of perjury or reckless disregard by a preponderance of the evidence; and (2) with the false material set aside, the affidavit's remaining content was insufficient to establish probable cause. *Id.* at 156. If, with the false material set aside, there remained probable cause, no hearing is required. *Id.* at 171–72. The same analysis from *Franks* applies

when facts are intentionally or recklessly omitted from a warrant affidavit if the omitted facts would have precluded a finding of probable cause. *See United States v. Barsoum*, 763 F.3d 1321, 1328–29 (11th Cir. 2014).

Williamson argues that the residential search warrant affidavit was invalid under *Franks*, pointing to two aspects of the warrant he contends were deficient. First, he points out that Keller incorrectly stated that NCMEC classified three of the seven images as child pornography even though NCMEC in fact had categorized them as "CP (Unconfirmed)." Second, he argues that Keller failed to include the fact that he did not know "whether the Yahoo account was logged-in or logged-out on September 8, 2020, when a pornographic image was sent from the account." Appellant's Br. 43. These errors, Williamson argues, were enough to entitle him to a *Franks* hearing and invalidate the warrant affidavit.

We begin with the first argument. Williamson is correct that Keller erroneously stated that NCMEC categorized three of the images as CSAM when NCMEC had labeled those images as "CP (Unconfirmed)." But even assuming that Keller's errors should have been excluded and NCMEC's correct classifications included, those changes would have had no impact on the sufficiency of the application. The search warrant affidavit correctly stated that NCMEC classified one of the seven images as "apparent child pornography," and this one image, coupled with all the other information in the application, was sufficient to establish probable cause. Moreover,

the warrant application separately included the graphic details about the illegal CSAM contained in four of the seven files.

Williamson's second argument is similarly unavailing. He maintains that the warrant affidavit should have said that Keller did not know whether the Yahoo account was logged in on September 8, 2020, the date the precipitating image was sent. It is unclear why Keller needed to specify that there wasn't evidence about a login on September 8, 2020, especially since the warrant affidavit explained that the last time someone logged into the Yahoo account before the incident was September 5, 2020. The affidavit also specified that the last recorded login occurred three days before the incident. Sharing the lack of information about September 8, 2020, would not have had an impact on the probable cause finding whatsoever. Accordingly, Williamson was not entitled to a *Franks* hearing, and the residential search warrant was sufficient to establish probable cause.

Finally, Williamson argues that the residential search warrant affidavit cannot be saved by the good-faith exception to the exclusionary rule. The exclusionary rule prohibits the use of evidence seized during, or as a result of, an unlawful search. *Murray v. United States*, 487 U.S. 533, 536 (1988). We need not determine whether the good-faith exception applies to this issue because the search was supported by a constitutional warrant.

AFFIRMED.