FOR PUBLICATION

In the

United States Court of Appeals

For the Eleventh Circuit

No. 24-12448

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

versus

KEVAN CARTER GIBBS, II,

Defendant-Appellee.

Appeal from the United States District Court
for the Northern District of Florida
D.C. Docket No. 4:23-cr-00061-MW-MAF-1

Before NEWSOM and BRASHER, Circuit Judges, and HUCK,* District Judge.

---

* Honorable Paul C. Huck, United States District Judge for the Southern District of Florida, sitting by designation.

BRASHER, Circuit Judge:

In this appeal, we must again decide whether a criminal should "go free because the constable has blundered." *People v. Defore*, 150 N.E. 585, 587 (1926) (Cardozo, J.). A software company alerted the National Center for Missing and Exploited Children that Kevan Gibbs had uploaded suspected child sexual abuse material to his account. NCMEC forwarded the tip to law enforcement. After reviewing the tip, Tallahassee Police Department Detective Paul Osborn requested and received a warrant to search the account that was the subject of the tip. He discovered images of a man sexually abusing a young girl. The investigation progressed with additional searches until Gibbs was eventually charged with sexual exploitation of a minor and possession of child pornography. Gibbs moved to suppress the evidence obtained from these searches on the ground that the initial search was conducted without probable cause in violation of the Fourth Amendment. The district court excluded the evidence, concluding that Detective Osborn's affidavit was too vague and conclusory to support probable cause or allow reasonable reliance on the resulting warrant.

The government argues that the evidence is admissible under the good faith exception to the exclusionary rule. Gibbs argues that Detective Osborn's affidavit merely recited the "bare bones" conclusions of anonymous tipsters and lacked any indicia of probable cause. We agree with the government. We believe the affidavit, which invoked the general trustworthiness of NCMEC's CyberTip program, contained sufficient indicia of probable cause to render Detective Osborn's reliance on the resulting warrant reasonable. Accordingly, the good faith exception to the exclusionary rule applies, and we reverse the district court.

I.

Synchronoss Technologies manages cloud storage accounts linked to Verizon cell phones. Verizon subscribers can use Synchronoss accounts to store their photos and videos. Under 18 U.S.C. § 2258A, electronic service providers like Synchronoss must report child sex abuse material to NCMEC's CyberTipline if they have "actual knowledge" that such material is on their platforms. *Id.* § 2258A(a)(1)(A), (B). In making a CyberTip report, electronic service providers may include information about the individual suspected of possessing child pornography, their geographic location, a depiction of the child pornography, and other relevant information. *Id.* § 2258A(b)(1)-(5).

NCMEC is a private, non-profit organization established by Congress to track missing and exploited children. It serves as an information clearinghouse, receiving and processing reports about child pornography through a CyberTipline. "Pursuant to its clearinghouse role . . . and at the conclusion of its review," NCMEC is required to forward CyberTips to law enforcement. *Id.* § 2258A(c).

Upon learning that a user had uploaded suspected child sex abuse material to his account, a Synchronoss administrator alerted NCMEC. NCMEC sent a CyberTip containing this information, including Gibbs's phone number, to law enforcement. Detective Osborn reviewed the tip and presented a Florida state court judge with an affidavit requesting a warrant to search Gibbs's Synchronoss account. The affidavit states that it was "[r]eviewed and approved by Tallahassee Police Department Legal Advisor Theresa Flury." Doc 38 at 24.

Detective Osborn's affidavit provides relevant information about his background. Specifically, it says that he was a twenty-year veteran of the Tallahassee Police Department, spent over seven years in the Special Victims Unit, attended over 1,500 hours of "advanced training" in child sexual abuse investigations, and had investigated more than 600 NCMEC CyberTips.

The affidavit provides a brief statement of probable cause. "On 10/26/2022, I reviewed Cybertip # 127205611, which was generated by the National Center for Missing and Exploited Children (NCMEC) after an administrator of Synchronoss advised a user uploaded suspected child sexual abuse material to their account on, or about, 06/15/2022. This following suspect information was included in the tip: Phone: 7792274759." *Id*. at 23. The affidavit describes the law that had been violated (possession of child pornography), the place to be searched (the account with the associated phone number), and the property to be seized (images, videos, and other content). It says that the "case was initially assigned to law enforcement" in Alabama, but "they discovered the suspect now resides" in Florida, and that Detective Osborn had confirmed a Tallahassee address associated with the account. *Id*.

In addition to this statement of probable cause, the affidavit also contains an extensive definitions section. It defines NCMEC as a "repository for information about child pornography" and states that "[c]ompanies that suspect child pornography has been stored or transmitted on their systems can report that information to NCMEC in the form of a CyberTipline Report (CyberTip)." *Id.* at 20. CyberTips are defined as investigative reports transmitted to law enforcement under section 2258A. The affidavit explains that an electronic service provider can "provide to NCMEC information about the child exploitation activity it believes has occurred" including any "information it may have collected in connection with the suspected criminal activity." *Id.* at 21. "NCMEC then attempts to locate where the activity occurred" and sends the CyberTip to law enforcement. *Id.*

The affidavit defines "Electronic Service Providers" as commercial organizations in business to provide individuals and businesses with Internet access. They "provide a range of functions" including "remote storage." They also "maintain records pertaining to their subscribers," including "information concerning content uploaded and/or stored on or via the ESPs [sic] servers." *Id.* at 20. The affidavit describes a "Categorization System" used by some electronic service providers to assist with the classification of child sex abuse material. The affidavit also defines "Hash Value," a mathematical algorithm that was not relevant to the investigation.

The judge approved the warrant. Detective Osborn executed it and found pictures on the Synchronoss account of a man sexually abusing a young girl. He then obtained another warrant for a pen register and trap-and-trace device for Gibbs's phone number. The data Detective Osborn collected led law enforcement to the victim and to Gibbs's arrest. Subsequent searches of Gibbs's cell phone uncovered additional child sex abuse material. Gibbs was charged with sexual exploitation of minors and possession of child pornography under 18 U.S.C §§ 2251 and 2252A.

Gibbs moved to suppress the evidence against him. He asserted that the affidavit for the initial Synchronoss warrant failed to establish probable cause. He also argued that the good faith exception did not apply because the warrant lacked indicia of probable cause. If the initial search was unlawful, Gibbs argued and the government agreed that all subsequently discovered evidence would be inadmissible as fruit of the poisonous tree.

The district court granted Gibbs's motion to suppress. The court concluded that Detective Osborn's probable cause statement was "bare-bones" and "conclusory." Doc. 41 at 5. The affidavit did not describe the images, discuss how the CyberTip was generated, or explain whether anyone had viewed the content of Gibbs's files. The court also observed that the lengthy definitions section was overly general. It took issue with the affidavit's inclusion of extraneous definitions, like the discussion of "hash values," reasoning that their inclusion could have misled the state judge into believing those tools were used in the investigation. Because the affidavit was bare bones, the court held that no reasonable officer could have relied on it. Accordingly, the good faith exception did not apply to Detective Osborn's search. The court suppressed all evidence obtained from the search of Gibbs's Synchronoss account and subsequent searches.

The government timely appealed.

II.

Rulings on motions to suppress evidence involve mixed questions of law and fact. Legal questions are reviewed *de novo* and underlying facts are reviewed for clear error. *United States v. Reid*, 69 F.3d 1109, 1113 (11th Cir. 1995). We review *de novo* whether the good faith exception applies. *United States v. Morales*, 987 F.3d 966, 974 (11th Cir. 2021). The government bears the burden of demonstrating that the good faith exception applies. *Id.*

III.

The Fourth Amendment protects "[t]he 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. Under the exclusionary rule, the government may not use evidence seized during an unlawful search in a subsequent criminal prosecution. *United States v. Martin*, 297 F.3d 1308, 1312 (11th Cir. 2002). Under the good faith exception to the exclusionary rule, the government may rely on evidence obtained in violation of the Fourth

Amendment if law enforcement acted in objectively reasonable good faith. *United States v. Leon*, 468 U.S. 897, 907-08 (1984).

The government does not argue that the warrant in this case was supported by probable cause. It argues only that the district court erred in declining to apply the good faith exception to the exclusionary rule. We will therefore assume, without deciding, that Detective Osborn's affidavit did not establish probable cause to search Gibbs's Synchronoss account.

We conduct a two-part analysis to determine whether the good faith exception permits us to consider evidence obtained in violation of the Fourth Amendment. First, we consider whether the facts fall into any of four limited circumstances where the good faith exception does not apply: (1) where the judge issuing the warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) where the issuing judge "wholly abandoned his judicial role"; (3) where the affidavit supporting the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) where, depending on the circumstances of the particular case, a warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Martin*, 297 F.3d at 1313 (citation modified). Second, if none of those circumstances is present, we ask whether the officer reasonably relied on the search warrant. *Morales*, 987 F.3d at 974.

We address each element in turn.

A.

Of the four categories to which the good faith exception does not apply, Gibbs argues only in favor of the third: that the affidavit underlying the warrant was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable. We disagree. Although all too brief, we believe Detective Osborn's affidavit contained sufficient indicia of probable cause to justify relying on the resulting warrant.

Probable cause exists when "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). An affidavit in support of a warrant must state facts sufficient to justify the conclusion that evidence will probably be found at the premises to be searched. *Martin*, 297 F.3d at 1314 (citing *United States v. Hove*, 848 F.2d 137, 140 (9th Cir. 1988)). The affidavit should establish a connection between the defendant and the place to be searched. *Id.* If the affidavit mentions an informant, the affidavit should demonstrate the informant's basis of knowledge and veracity. *Id.*

Of course, the question here is not whether the affidavit establishes actual probable cause—the government concedes it did not. The question is whether the affidavit was so lacking in indicia of probable cause that it was unreasonable to rely on the resulting warrant. "We look only to the face of the affidavit to determine whether it lacked sufficient indicia of probable cause." *United States v. McCall*, 84 F.4th 1317, 1325 (11th Cir. 2023) (citation omitted). An affidavit lacks indicia of probable cause when it provides "no hint" as to why police believed they would find incriminating evidence. *Id.* (quoting *Morales*, 987 F.3d at 976). That belief must be so "plainly incompetent" in light of the affidavit that "no officer of reasonable competence would have requested the warrant." *Id.* (first quoting *Messerschmidt v. Millender*, 565 U.S. 535, 553 (2012); and then quoting *Malley v. Briggs*, 475 U.S. 335, 346 n.9 (1986)).

Gibbs argues that the affidavit lacks sufficient indicia of probable cause because it does not describe the images found in his Synchronoss account. [1] As the Supreme Court has explained, however, the existence of probable cause depends on the totality of the circumstances, not any particular factor. *Gates*, 462 U.S. at 233, 238. It is true that an affidavit *may* establish probable cause by describing the alleged contraband—in this case child pornography. *See United States v. Lapsins*, 570 F.3d 758, 764-65 (6th Cir. 2009); *United States v. Chrobak*, 289 F.3d 1043, 1044-45 (8th Cir. 2002). And it is true that this affidavit did not describe the pictures that were on Gibbs's account.

But information from a trustworthy source can also provide probable cause. In *Jones v. United States*, for example, the Supreme

[1] Courts disagree about the circumstances that allow a law enforcement officer to conduct a warrantless examination of digital files that form the basis of a CyberTip. *Compare United States v. Miller*, 982 F.3d 412 (6th Cir. 2020), *and United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018), *with United States v. Maher*, 120 F.4th 297 (2d Cir. 2024), *and United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021).

Court upheld a warrant based on an anonymous tip by an informant who had previously given accurate information and was considered trustworthy. 362 U.S. 257, 271 (1960), *overruled on other grounds by United States v. Salvucci*, 448 U.S. 83 (1980). The affidavit merely referred to a "supply of heroin" and did not otherwise describe the illegal contraband. *Id.* at 267 n.2. But because the informant had proved reliable in the past, his statement helped to establish probable cause. *Id.* at 271. Likewise, in *United States v. Harris*, the Court found probable cause where an affidavit relied on an unidentified informant who had experience purchasing illicit whiskey, knew about the trade, and averred that whiskey was being consumed on the defendant's property. 403 U.S. 573, 575-76 (1971). Once again, the affidavit did not describe the contraband such that the reviewing magistrate could make an independent determination of its legality. *Id.*

Of course, an affidavit must describe some of the underlying circumstances to justify good faith reliance on a resulting warrant. The Supreme Court's opinions in *Nathanson v. United States*, 290 U.S. 41 (1933), and *Aguilar v. Texas*, 378 U.S. 108, 114 (1964), *abrogated on other grounds by Illinois v. Gates*, 462 U.S. 213 (1983), are illustrative. The Supreme Court has cited these precedents as examples of search warrants that so clearly lacked probable cause that law enforcement officers could not have relied on them in good faith. *See Leon*, 468 U.S. at 915. In *Nathanson*, a warrant was issued upon the sworn allegation that the affiant "has cause to suspect and does believe that certain merchandise" was in a specified location. 290 U.S. at 44. The Court held that the warrant was improperly issued because "[m]ere affirmance of belief or suspicion is not enough" without "supporting facts or circumstances" to explain why the affiant had the belief. *Id.* at 47. In *Aguilar*, the affidavit stated that police "received reliable information from" an unidentified "credible person" that a dwelling contained heroin. 378 U.S. at 109. The Court held that the warrant was invalid because, "[a]lthough an affidavit may be based on hearsay information and need not reflect the direct personal observations of the affiant, the magistrate must be informed of some of the underlying circumstances" for an unidentified informant's conclusion. *Id.* at 114.

Applying this case law, we see several details in Detective Osborn's affidavit that go to the reliability of his "informant" and explain the circumstances of the informant's report. According to the affidavit, the CyberTip went through two layers of review: the initial generation of the tip by Synchronoss, and NCMEC's receipt and forwarding of the tip to law enforcement. Under 18 U.S.C. § 2258A(a)(1)(A), referenced in the affidavit, Synchronoss was obligated to generate the CyberTip only upon obtaining "actual knowledge" of child pornography. The affidavit states that "an administrator of Synchronoss advised a user uploaded suspected child sexual abuse material to their account," establishing that Synchronoss had knowledge of the contents of the files. As in *Harris*, the affidavit explained the circumstances of the administrator's knowledge. That is, the Synchronoss administrator was in a position to know about the existence of child pornography on the very platform that he monitored.

We also think it reasonable for a law enforcement officer to conclude that, when an electronic service provider says it has identified suspected child pornography on a customer's account, there is probable cause to believe there is child pornography on the account. According to the affidavit, electronic service providers "maintain records pertaining to their subscribers," including "information concerning content uploaded and/or stored on or via the ESPs [sic] servers." Doc. 38 at 20. Of course, the electronic service provider could be wrong. But the tip here is not much worse than the tips in *Jones* and *Harris*, where informants merely reported seeing heroin and whiskey. Although the informants did not *describe* the heroin or whiskey, they were the kind of informants who could be expected to distinguish illegal contraband from innocuous substances. So too here.

NCMEC is also a particularly reliable source from which to receive a tip. Like the tipster in *Jones*, who was known as an accurate informant, NCMEC regularly informs police of potential child pornography. As the affidavit makes clear, Congress created NCMEC to support law enforcement in the aid of sexually exploited children. It has "serve[d] as a repository for information about child pornography" for over forty years. Doc. 38 at 20. Recognizing its accuracy, we have held that NCMEC reports and spreadsheets bear sufficient indicia of reliability in the restitution context. *United States v. Sotelo*, 130 F.4th 1229, 1249 (11th Cir. 2025) ("It is also notable that the report comes from the NCMEC, the only organization in the country dedicated to the notification and identification of child pornography victims."). The Fifth Circuit has similarly observed that "NCMEC cyber-tips regularly form the basis of investigations in both this circuit and across the nation; their reliability ha[s] seemingly been rarely questioned." *United States v. Landreneau*, 967 F.3d 443, 453 (5th Cir. 2020).

Detective Osborn's affidavit also contained a definitions section that bolstered the reliability of NCMEC and the reporting process in general. The affidavit describes NCMEC as a "repository for information about child pornography" and states that companies report child pornography on their platforms to NCMEC. Doc. 38 at 20. It also states that CyberTips can come from both companies and concerned individuals, and that electronic service providers can provide NCMEC with information regarding incident type and incident time, as well as files and screenshots. And, as we have explained, Synchronoss had to have actual knowledge of child pornography. These are the kinds of "supporting facts" and "underlying circumstances" the Supreme Court has found necessary to establish probable cause. *Nathanson*, 290 U.S. at 47; *Aguilar*, 378 U.S. at 114.

Recently, the Seventh Circuit held that a similar CyberTip-based affidavit established probable cause in part because of the system's reliability. In *United States v. Braun*, the court reasoned that an officer's affidavit established probable cause in part because the officer explained that electronic service providers had generated CyberTips to NCMEC, that NCMEC had forwarded these tips to police as required by law, and that the officer had previously relied on NCMEC CyberTips and considered them reliable. No. 25-2740, slip op. at 11-12 (7th Cir. Aug. 20, 2026). Citing the Fifth Circuit's decision in *Landreneau*, the court concluded that "[s]uch indicia of reliability lent credence to the accuracy of the CyberTip reports." *Id.* at 12. To be sure, there were other statements in the warrant application that also helped establish probable cause—allegations about previous internet chats with young girls and a suspicious file name. *See id.* at 13-14. But, in finding probable cause to search based on the CyberTip, the Seventh Circuit did not require that the officer personally view the images or describe them in the warrant application. *Id.* at 9. If the warrant affidavit in *Braun* was sufficient to establish probable cause, then this affidavit had enough indicia of probable cause for an officer to rely on the resulting warrant.

Finally, we note that, unlike the affidavits in *Jones* and *Harris*, Detective Osborn's affidavit disclosed the names of the entities that had generated and forwarded the tip. A tip from a known informant is stronger than an anonymous one because it is possible to assess the known informant's knowledge and reputation. *Cf. Florida v. J.L.*, 529 U.S. 266, 270 (2000) (discussing principle in the reasonable suspicion context).

Gibbs makes three arguments to resist the conclusion that the affidavit contained sufficient indicia of probable cause. None works.

First, Gibbs argues that Detective Osborn should have tried to "corroborate, verify, or investigate" the CyberTip before seeking a warrant. No doubt, the indicia of probable cause would have been greater if Detective Osborn had recounted his review of the child abuse material. But affidavits may be based on hearsay and need not reflect the affiant's direct personal observations. *Aguilar*, 378 U.S. at 114. Though desirable, independent police corroboration of an informant is not necessary to create indicia of probable cause if an affidavit otherwise establishes an informant's basis of knowledge and veracity. *United States v. Brundidge*, 170 F.3d 1350, 1353 (11th Cir. 1999).

Second, Gibbs takes issue with Detective Osborn's inclusion of a few unrelated definitions in the affidavit, such as "Hash Value" and references to a "Categorization System." To be sure, Detective Osborn's inclusion of unrelated terms was sloppy. But these were relatively minor definitions included at the end of the section. Gibbs does not take issue with the more relevant definitions of "NCMEC," "ESP," and "CyberTip," which the affidavit actually referenced in its probable cause section. Affidavits do not have to be perfect; we have applied the good faith exception even where the affidavit contained significant imperfections. *See Martin*, 297 F.3d at 1315 (finding indicia of probable cause even though affidavit's deficiencies as to dates, times, and links between the defendant and criminal activity "le[ft] much to be desired"). There is no reason to conclude that the state judge was misled by the extraneous definitions of terms that did not actually appear in the probable cause narrative.

Finally, Gibbs argues that it was "possible" that no one ever viewed the contents of the Synchronoss account. That is, he posits that, perhaps, neither the electronic service provider nor anyone at

NCMEC actually saw images of child pornography on Gibbs's account. This argument flips the standard for the good faith exception. To avoid the good faith exception, it must have been "entirely unreasonable" for Detective Osborn to rely on the warrant that he secured. *Id.* at 1313, 1315. At the beginning of any investigation, it is "possible" for an informant to be wrong. After all, even when an affidavit establishes obvious, ironclad probable cause, the resulting search may prove fruitless. But the good faith exception requires that we weigh likelihood and reasonableness; it does not demand certainty.

In short, we conclude that the affidavit, although it did not describe the contraband and obviously could have been better, contained sufficient indicia of probable cause to render Detective Osborn's reliance on the resulting warrant reasonable. At the very least, we cannot say the affidavit provides "no hint" as to why police believed they would find incriminating evidence in Gibbs's Synchronoss account. *McCall*, 84 F.4th at 1325.

B.

Having rejected Gibbs's argument that the affidavit lacked indicia of probable cause, we turn to whether Detective Osborn reasonably relied on the warrant. *Morales*, 987 F.3d at 974. We have held that, "[i]n 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 (quoting *United States v. Stowers*, 32 F.4th 1054, 1067 (11th Cir. 2022)). Only if the circumstances of the warrant establish that a reasonably well-trained officer would know the resulting warrant was illegal despite the state judge's authorization may we conclude that the detective acted unreasonably. *Id.*

We cannot say it was unreasonable for Detective Osborn to rely on the warrant. Information in the affidavit can support a finding of good faith reliance on the warrant. *United States v. Robinson*, 336 F.3d 1293, 1297 (11th Cir. 2003); *Morales*, 987 F.3d at 976. As we have already explained, the warrant was based on a CyberTip reviewed by NCMEC and generated by a Synchronoss administrator based on actual knowledge of child pornography on the Synchronoss platform. Detective Osborn's reliance on the warrant was neither entirely unreasonable nor "plainly incompetent." *McCall*, 84 F.4th at 1325.

Two other facts in the affidavit also serve to justify Detective Osborn's reliance on the resulting warrant. First, in determining whether an officer reasonably relied on a warrant, we consider "a particular officer's knowledge and experience." *Herring v. United States*, 555 U.S. 135, 145 (2009). And Detective Osborn explained in the affidavit that he was a seasoned detective with years of experience in child sex abuse investigations, was familiar with NCMEC and its reliability, and had investigated hundreds of NCMEC CyberTips. Second, the affidavit states that Detective Osborn received approval from a Tallahassee Police Department legal advisor before submitting his warrant application to the judge. The Supreme Court and this Court have consistently held that an officer's effort to receive approval from lawyers is indicative of objectively reasonable good faith reliance. *Massachusetts v. Sheppard*, 468 U.S. 981, 989 (1984); *United States v. Taxacher*, 902 F.2d 867, 872 (11th Cir. 1990); *McCall*, 84 F.4th at 1329.

Finally, there is no evidence that Detective Osborn intentionally omitted facts that would have defeated a finding of probable cause, provided information he knew was false, or otherwise engaged in misconduct. *United States v. Gregory*, 128 F.4th 1228, 1245 (11th Cir. 2025). "Assuming such evidence existed, [Gibbs] would have been free to present it, but he did not." *Robinson*, 336 F.3d at 1297.

* * *

When asked to exclude evidence of crime, we must keep in mind that the purpose of the exclusionary rule is to deter police misconduct. *McCall*, 84 F.4th at 1323. Suppression of evidence is a remedy of last resort. *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). The Supreme Court has recognized that good faith mistakes cannot be deterred and are not worth the "heavy toll" the exclusionary rule takes on society and the courts. *Davis v. United States*, 564 U.S. 229, 237-38 (2011). In a case like this one—the execution of a warrant based on a tip from a source established by Congress that has proven credible in the past—we see little deterrence benefit from the exclusionary rule.

IV.

We **REVERSE** and **REMAND** for further proceedings consistent with this opinion.

NEWSOM, Circuit Judge, concurring:

For me, this is a close case. The affidavit that Detective Osborn submitted in support of his warrant application leaves a lot to the imagination—and thus a lot to be desired. Detective Osborn explained that he had received a CyberTip generated by the National Center for Missing and Exploited Children after an unnamed "administrator" at a company called Synchronoss advised NCMEC that a user had uploaded "suspected" child sexual abuse material to his account. Br. of Appellant at 8. Questions abound: Who is this nameless, faceless "administrator"? Why did he or she "suspect[]" the material was illicit? Did NCMEC review the tip's contents before forwarding it along to law enforcement? Did Detective Osborn verify the content himself? And how often do NCMEC tip-based investigations yield evidence of a crime? Lots of questions—not many answers. A judge confronted with this affidavit would have to pile inference on top of inference in order to conclude that "there [wa]s a fair probability that contraband or evidence of a crime w[ould] be found" on Gibbs's account. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983). With so many weak links in the causal chain, probable cause seems like a stretch. Such a stretch, in fact, that the government doesn't even contend that probable cause existed.

But here's the thing: In "marginal cases," we've said, "suppression is inappropriate." *United States v. McCall*, 84 F.4th 1317, 1323 (11th Cir. 2023) (quoting *United States v. Ventresca*, 380 U.S. 102, 109 (1965)). The good-faith exception to the exclusionary rule applies to all but the most clear-cut Fourth Amendment violations. Gibbs asserts that two exceptions to the exception (so to speak) apply here. First, he says that Detective Osborn's affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *See United States v. Leon*, 468 U.S. 897, 923 (1984) (citation omitted). And second, he says that Detective Osborn unreasonably relied on the search warrant that the judge ultimately issued. *See United States v. Martin*, 297 F.3d 1308, 1318 (11th Cir. 2002). It seems to me that these two categories substantially overlap, but I'll just take them in turn.

First, while I agree with the majority that the affidavit contains at least *some* indicia of probable cause, those indicia are pretty doggone weak. The majority notes, for instance, that "[a]ccording to the affidavit, the CyberTip went through two layers of review: [(1)] the initial generation of the tip by Synchronoss, and [(2)] NCMEC's receipt and forwarding of the tip to law enforcement." Maj. Op. at 12. That's true, but neither layer of "review" inspires much confidence. I agree, for instance, that Synchronoss "was *obligated* to generate the CyberTip only upon obtaining 'actual knowledge' of child pornography," *id.* at 12–13 (emphasis added), but nothing would have prevented the company from generating a tip based on something less—it wasn't obligated, that is, *not* to generate a tip without such knowledge. Indeed, the governing statutory framework at least arguably promotes over-reporting and thus skews the balance. Companies are penalized for failing to report illegal material, but not for mistakenly reporting material that turns out to be lawful. 18 U.S.C. §§ 2258A(e), 2258B(a) & (b). And perhaps tellingly, all Detective Osborn's affidavit says is that the unnamed Synchronoss administrator "suspected" CSAM—not that he or she actually *saw* anything.

Nor do I put a lot of stock in NCMEC's "review." Of course, I take seriously the majority's point that NCMEC's involvement lends credibility to the tip because "NCMEC regularly informs police of potential child pornography." Maj. Op. at 13. But unlike a tipster who law enforcement knows provides reliable tips, we don't know, at least from Detective Osborn's affidavit, whether NCMEC's reports regularly unearth evidence of crime. Indeed, based on the affidavit, we don't know whether NCMEC regularly reviews tips before sending them to law enforcement or simply serves as a conduit. And we most certainly don't know whether NCMEC reviewed this one.

Having said all that, and despite what seem to me to be some pretty glaring shortcomings, I agree with the majority that Detective Osborn's affidavit isn't *so* bare-bones that it lacks *any* indicia of probable cause. After all, we've said that an affidavit lacks such indicia only when it provides "no hint" as to why law enforcement believed they would find incriminating evidence—when it is so bereft that it would be "plainly incompetent" to so conclude. *McCall*, 84 F.4th at 1325 (quoting *Messerschmidt v. Millender*, 565 U.S. 535, 553 (2012)). I can't say that here. We know why Detective Osborn believed there was illicit material on Gibbs's computer: because he received a tip from NCMEC that Gibbs had "uploaded suspected child sexual abuse material to [his] account." Br. of Appellant at 8.

Thus, the affidavit "establish[ed] a connection between the [account] and any criminal activity." *Martin*, 297 F.3d at 1314.

Second, let me turn briefly to objective reasonableness. Recall that in this case, after Detective Osborn prepared his affidavit, it was vetted twice. First, he had it "[r]eviewed and approved by [a] Tallahassee Police Department Legal Advisor." Br. of Appellant at 9. Then, of course, a state-court judge deemed it sufficient and issued a warrant based on it. I would be *extremely* reluctant to hold that an officer acted unreasonably in declining to countermand the conclusions *both* of his in-house lawyer *and* of a neutral magistrate. I won't say never, but the bar is—and has to be—extremely high.

The case law bears out my reluctance. We've long held that seeking approval from lawyers and judges "is indicative of objective good faith." *United States v. Taxacher*, 902 F.2d 867, 872 (11th Cir. 1990) (citing *Massachusetts v. Shephard*, 468 U.S. 981, 989–90 (1984)); *see also Messerschmidt*, 565 U.S. at 553–555. And for good reason: Taking the care to confirm with a lawyer and a judge that an affidavit establishes probable cause—and then acting on their directives—is hard to square with the "deliberate, reckless, or . . . grossly negligent" conduct that the Supreme Court has required before excluding evidence. *See Herring v. United States*, 555 U.S. 135, 144 (2009).

* * *

Bottom line: This was a bad affidavit. But it was not completely bankrupt, and both a lawyer and a neutral magistrate signed off on it. That's enough to trigger the good-faith exception and forestall the application of the exclusionary rule.