

No. _____

IN THE SUPREME COURT OF THE UNITED STATES

GREGORY ALLEN WILLIAMSON,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent,

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF
APPEALS FOR THE ELEVENTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

BJORN E. BRUNVAND
Brunvand, Wise & Farinella Law Group
615 Turner Street
Clearwater, Florida 33756
Ph: (727) 446-7505
Email: bjorn@acquitter.com
Florida Bar No. 0831077
Counsel of Record for Petitioner

QUESTIONS PRESENTED

I.

Whether email service providers and the National Center for Missing and Exploited Children act as government entities when they conduct hash value searches of private email accounts?

II.

Whether the private search doctrine applies when email service providers conduct hash value searches of private email accounts, but no human being reviews the alleged contraband located therein?

III.

Whether the Good Faith Exception can Apply to Save a Facially Overbroad Search Warrant when the Same Law Enforcement Officer is Both the Affiant and the Executing Officer?

LIST OF PARTIES

The parties to the judgment from which review is sought are the Petitioner and appellant in the lower court, Gregory Allen Williamson, and the Respondent and appellee in the lower court, the United States of America.

CORPORATE DISCLOSURE STATEMENT

No corporations or publicly held companies are a party to this case or have any direct interest therein.

LIST OF RELATED CASES

Direct Appeal:

United States v. Gregory Williamson, --- Fed.Appx. ----, No. 24-12038, 2026 WL 1876371 (11th Cir. Jun. 30, 2026).

District Court Motion to Suppress:

United States v. Williamson, Case No. 8:21-cr-355-WFJ-CPT, 2023 WL 6210841 (M.D. Fla. Jul. 6, 2023).

District Court Motion to Suppress:

United States v. Williamson, Case No. 8:21-cr-355-WFJ-CPT, 2023 WL 4056324 (M.D. Fla., Feb.10, 2023).

TABLE OF CONTENTS

	Page
Questions Presented.....	ii
List of Parties.....	iii
Corporate Disclosure Statement.....	iii
List of Related Cases	iii
Table of Contents.....	iv
Table of Cited Authorities	vi
Opinion Below.....	1
Grounds for Jurisdiction.....	1
Constitutional and Statutory Provisions Involved.....	1
Statement of the Case	2
Reasons for Granting the Petition	14
I. The Question of Whether Email Service Providers and the NCMEC Act as Government Entities When They Search Private Email Accounts.....	14
II. The Question of Whether the Private Search Doctrine Applies when no Human Reviews the Alleged Contraband Contained in a Private Email Account	20
III. The Question of Whether the Good Faith Exception can Apply to Save a Facially Overbroad Search Warrant when the Same Law Enforcement Officer is Both the Affiant and the Executing Officer	27
Conclusion.....	34
APPENDICES	Page
Appendix A: The Eleventh Circuit Opinion Below.....	A
Appendix B: The District Court Order Denying Motion to Suppress (Jul. 6, 2023) ..	B

Appendix C: The District Court Order Denying Motion to Suppress (Feb. 10, 2023)C

TABLE OF CITED AUTHORITIES

Cases	Page(s)
<i>Brentwood Acad. v. Tennessee Secondary Sch. Athletic Ass’n</i> ,	
531 U.S. 288, 121 S.Ct. 924, 148 L.Ed.2d 807 (2001).....	14
<i>Coolidge v. New Hampshire</i> ,	
403 U.S. 443, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971).....	27, 29
<i>Lebron v. Nat’l R.R. Passenger Corp.</i> ,	
513 U.S. 374, 115 S.Ct. 961, 130 L.Ed.2d 902 (1995).....	17
<i>Lugar v. Edmondson</i> ,	
457 U.S. 922, 102 S.Ct. 2744, 73 L.Ed.2d 482 (1982);.....	14
<i>Riley v. California</i> ,	
573 U.S. 373, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014).....	29
<i>Trustees of Dartmouth College v. Woodward</i> ,	
17 U.S. (4 Wheat.) 518, 4 L.Ed. 629 (1819).....	23
<i>United States v. Ackerman</i> ,	
831 F.3d 1292 (10th Cir. 2016).....	9, 19, 22-25
<i>United States v. Alford</i> ,	
744 F. App’x 650 (11th Cir. 2018)	28-31
<i>United States v. Allen</i> ,	
854 Fed. Appx. 329 (11th Cir. 2021)	14

<i>United States v. Blake</i> ,	
868 F.3d 960 (11th Cir. 2017).....	13, 27-32
<i>United States v. DiTomaso</i> ,	
81 F. Supp. 3d 304 (S.D.N.Y. 2015).....	15
<i>United States v. Harling</i> ,	
705 Fed. Appx. 911 (11th Cir. 2017)	21
<i>United States v. Henry</i> ,	
447 U.S. 264, 100 S.Ct. 2183, 65 L.Ed.2d 115 (1980).....	16
<i>United States v. Jacobsen</i> ,	
466 U.S. 109, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984).....	21, 23, 25
<i>United States v. Leon</i> ,	
468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984).....	32
<i>United States v. Lowers</i> ,	
170 F.4th 134 (4th Cir. 2026)	26
<i>United States v. Maher</i> ,	
120 F.4th 297 (2d Cir. 2024).....	25-26
<i>United States v. Martin</i> ,	
297 F.3d 1308 (11th Cir. 2002).....	32
<i>United States v. Miller</i> ,	
982 F.3d 412 (6th Cir. 2020).....	10, 22, 25
<i>United States v. Montijo</i> ,	
2022 WL 93535 (M.D. Fla. Jan. 10, 2022)	9, 22

United States v. Reddick,

900 F.3d 636 (5th Cir. 2018)..... 10, 22, 24-25

United States v. Rosenow,

50 F.4th 715 (9th Cir 2022) 8

United States v. Simpson,

904 F.2d 607 (11th Cir. 1990)..... 12

United States v. Steiger,

318 F.3d 1039 (11th Cir. 2003)..... 14

United States v. Williamson, --- Fed.Appx. ----,

No. 24-12038, 2026 WL 1876371 (11th Cir. Jun. 30, 2026) 1

United States v. Wilson,

13 F.4th 961 (9th Cir. 2021) 9, 22, 25-26

United States v. Young,

350 F.3d 1302 (11th Cir. 2003)..... 21

Walter v. United States,

447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 410 (1980)..... 21, 23, 25

Constitutional Provisions

U.S. CONST. amend. IV 1, 8, 10, 14, 19, 22-28, 31

Statutes and Rules

18 U.S.C. § 2258A..... 8, 15, 18-19

28 U.S.C. § 1254.....	1
SUP. CT. R. 10	33

OPINION BELOW

The United States Court of Appeals for the Eleventh Circuit affirmed the judgment of the district court in an unpublished opinion, *United States v. Gregory Williamson*, --- Fed.Appx. ----, No. 24-12038, 2026 WL 1876371 (11th Cir. Jun. 30, 2026), which is attached hereto as Appendix A.

GROUND FOR JURISDICTION

The United States Court of Appeals for the Eleventh Circuit issued its panel opinion on June 30, 2026. *See* Appendix A. Petitioner seeks the jurisdiction of this Court pursuant to 28 U.S.C. § 1254(1) through the filing of the instant petition for a writ of certiorari.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

U.S. CONST. amend. IV:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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.

STATEMENT OF THE CASE

The instant case involved the warrantless searches of email accounts linked to the Petitioner and a subsequently issued search warrants for the Petitioner's email account. Yahoo, Inc is an Electronic Service Provider ("ESP") that provides email services to users. Yahoo employs "trust and safety moderators" who review emailed content for the presence of possible child pornography. Pursuant to statute, Yahoo reports any such suspected child pornography to the National Center for Missing and Exploited Children ("NCMEC").

Yahoo uses various methods to scan emails to determine if they contain suspected child pornography. Those methods include the use of a program titled "CSAi Match" as well as the review of "photo DNA." Through those methods, files are compared against larger databases for matches to hash values of known child pornography files. The hash value is akin to a digital footprint for media.

If those methods result in a match, a trust and safety moderator typically then manually reviews the suspect file to determine if it contains child pornography. If the moderator believes the file contains child pornography, the file is archived along with any other attachments, images, or videos from the email account at issue. Yahoo then reports its findings to the NCMEC. Yahoo also sends to NCMEC the known contact information for the person who created the email account at issue as well as the IP address of the device or network from which the suspect email was sent. Yahoo has no way of determining, however, the identity of the person who sent any such suspect emails.

The Yahoo moderators have a system of rating any child pornography based on the egregious nature of the material. The files are ranked with an A1, A2, B1, or B2 rating depending on the severity of the pornography.

In September 2020, Yahoo's review system flagged a Yahoo account belonging to username "Vladlover50" as having been suspected of sending child pornography. A trust and safety moderator then allegedly reviewed the account and found seven images believed to be child pornography. Yahoo reported those findings and the corresponding information to NCMEC. The moderator did not rate the images on the A-B-1-2 scale. The Yahoo employee who purportedly would have reviewed the images did not testify at an evidentiary hearing that was later held on a motion to suppress. A Yahoo witness who testified at the hearing could not identify the identity of the person who allegedly reviewed the images. Another witness who was a manager at Yahoo during the relevant time period testified at trial that the failure to rate the files flagged from the "Vlad" account likely indicated that the moderator did not consider the files to be the "worst of the worst." Yahoo had never received any complaints nor tips of criminal activity concerning the email account at issue.

Law enforcement later received a report from Yahoo concerning the seven images. The images were from the email address Vladlover50@Yahoo.com, which was registered to "Vlad Vlad." The approximate geolocation for the associated IP address was North Port, Florida.

The case agent found the internet provider for the IP address to be Comcast. He went on to issue an investigative subpoena to Comcast. The agent learned from

that subpoena that the internet subscriber was Aliona Williamson with a service address in North Port, Florida. That address would be determined to be the residence of the Williamson family. The agent also learned that the 1469 phone number connected to the IP address was registered to a woman in Venice, Florida. That number had been a prior phone number of Mr. Williamson.

In the course of the investigation, law enforcement also sought and obtained from a state court a search warrant for all data from email account Vladlover50@Yahoo.com. The agent later testified at trial to various sexually explicit emails sent from the Vlad email account to an account that would later be connected to Mr. Williamson's stepdaughter, D.A. The agent found that certain exhibits attached to various of the emails constituted child pornography.

After reviewing the email search warrant return, the case agent sought and obtained a search warrant from a state court for the residential address in North Port associated with the IP address.

On January 27, 2021, the North Port Police Department executed the search warrant at the residence. The residence was the home of Mr. Williamson, his wife Aloina Williamson, their three children, and D.A. (the stepdaughter of Mr. Williamson and biological daughter of Mrs. Williamson). During the search, law enforcement collected, among other items, a Gateway all-in-one computer and a Samsung cellular phone that were located in the garage of the residence. Two hard drives, several USB drives, and other digital media were seized from a bedroom

connected to Mr. Williamson. An Apple iPhone was collected from the stepdaughter's bedroom.

When law enforcement executed the search warrant, it interviewed D.A. Law enforcement specifically asked D.A. if Mr. Williamson had ever touched her inappropriately. D.A. answered that he had not. A few months later, D.A. was again interviewed in connection with the investigation. The interviewer again asked D.A. if Mr. Williamson had ever touched her inappropriately. D.A. again responded that Mr. Williamson had never touched her inappropriately. D.A. did not thereafter make any allegation that Mr. Williamson ever touched her inappropriately until 2022 when she first spoke with the prosecutor and the case agent together.

A forensic examiner employed in law enforcement later testified at trial to examinations he performed on the seized items. He testified that child pornography files were found on the Gateway computer. The examiner additionally testified that an Acer tower computer that was seized from Mr. Williamson's shared bedroom was found to contain four images that were deemed child pornography and two images that were deemed "age difficult."

Following the execution of the search warrant, the agent reviewed an extraction of the Samsung phone. In that extraction, the agent saw several photographs and videos that appeared to be taken from what he believed to be a hidden camera located in D.A.'s bedroom. Certain emails located in the Samsung phone extraction contained attachment images from the camera that depicted D.A. in various stages of undress. Those emails apparently were sent to and from the same

email address. The agent then returned to the home to discuss the findings with Mrs. Williamson. While he was doing so, D.A. approached him and handed him a USB charger that had a camera inside of it.

Mr. Williamson was arrested at the time of the execution of the search warrant. He was later indicted in the Middle District of Florida, Tampa Division, on one count of Coercion and Enticement of a Minor to Engage in Sexual Activity; one count of Attempted Production of Child Pornography; two counts of Production and Attempted Production of Child Pornography; three counts of Distribution of Child Pornography; and one count of Possession of Child Pornography.

The Initial Motion to Suppress

Prior to trial, Mr. Williamson filed a motion to suppress all evidence seized from the search warrants issued for Yahoo email account and for his residence. The motions asserted that Yahoo and NCMEC were effectively serving as government agents when they searched, seized, and reported to law enforcement the emails and images that initiated the investigation. The motion additionally asserted that, regardless of whether Yahoo and NCMEC were government agents, the case detective's review of the materials provided to him prior to obtaining a search warrant exceeded the scope of any purported private entity searches that Yahoo and NCMEC might have conducted. The motion further set out that the search warrant affidavits included material misrepresentations and omissions that negated the existence of any purported probable cause.

The district court held an evidentiary hearing on October 11, 2022. The Government presented as witnesses an Executive Director of the NCMEC, a former content moderator for Yahoo, a former E-crimes investigator and senior manager for trust and safety at Yahoo, and the case agent.

In addition to evidence set forth above that was presented trial, the evidence established that the Protect our Children Act of 2008 requires email service providers (ESPs) such as Yahoo to report any suspected violations of laws pertaining to child pornography. The Act requires any such suspected violations to be reported to the NCMEC. The NCMEC, in turn, is a non-for-profit organization that Congress empowered to operate a “CyberTipline” to receive the reports from ESPs. The NCMEC then makes those reports available to law enforcement.

The evidence additionally established that Yahoo required email users to agree to terms of service. The terms of service included an agreement that users will “not use Yahoo Services to upload, post, email, transmit, or otherwise make available any Content that is unlawful, harmful, . . . abusive, . . . obscene, . . . invasive of another’s privacy, . . . or otherwise objectionable; [or] harm minors in any way . . .” The terms further state:

...Yahoo may or may not pre-screen Content, but that Yahoo and its designees shall have the right (but not the obligation) in their sole discretion to pre-screen, refuse, or remove any Content that is available via the Yahoo Services. . . . [The customer also] acknowledge[s], consent[s,] and agree[s] that Yahoo may access, preserve[, and disclose [the user’s] account information and Content if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary to: (i) comply with legal process;[or] (ii) enforce the [terms of service] . . .

As an initial finding, the district court held, over the Government’s objection, that Mr. Williamson had a reasonable expectation of privacy in his email accounts and had standing to assert the Fourth Amendment challenges he raised in the motion.

The court then found, however, that Yahoo and NCMEC were private entities and that the Fourth Amendment challenges failed under the private search doctrine. In so holding, the court reasoned:

It is evident from the record that Yahoo was not a government actor. Starting with the first prong, I recognize at the outset that—as Mr. Williamson maintains—ESPs like Yahoo are mandated by the Protect Act to report online sexual child exploitation to NCMEC “as soon as reasonably possible after obtaining actual knowledge of any . . . apparent violations” of certain child pornography statutes. See 18 U.S.C. § 2258A(a)(1)(A)(i), (2)(A). I also recognize that an ESP’s knowing and willful failure to fulfill this obligation subjects it to sanctions. *Id.* § 2258A(e).¹⁹ Mere compliance with that law, however, does not constitute state action by a private entity. *United States v. Rosenow*, 50 F.4th 715, 730 (9th Cir 2022) (noting that “a private actor does not become a government agent simply by complying with a mandatory reporting statute”) (citations omitted)). Moreover, the Protect Act only imposes an obligation upon ESPs to report child pornography that is known to them and expressly states that ESPs are not required to search for it. 18 U.S.C. § 2258A(f)...

...Further, there is no evidence that the government instigated or cooperated with Yahoo’s review of Mr. Williamson’s emails. In fact, quite the opposite is true. According to Ms. Guizzotti’s testimony, which I credit, Yahoo undertook its analysis of these communications without any encouragement from the government.

App. B at 30-32. The court additionally found that the evidence established that “Yahoo proactively searches sent emails because it has an interest in safeguarding both its users and its reputation.” App. B at 32.

The court then rejected an assertion of Mr. Williamson that Yahoo was serving as a government agent because it relied on a directive titled “Compliance Guide for Law Enforcement.” The court recognized that the Guide “is designed to assist law enforcement in understanding Yahoo’s policies and practices with regard to retention and disclosure of electronic information and to provide answers to frequently asked questions related to subpoenas and other legal process.” App. B at 33. It further acknowledged that the Guide specifically states that Yahoo had worked with law enforcement and the NCMEC to develop its practices for reporting suspected child pornography. The court concluded, nonetheless, that Yahoo’s development of protocols “has no bearing on the company’s intent when it searches customer’s emails.” App. B. at 34.

Later in its opinion, the court rejected Mr. Williamson’s contention that Yahoo’s search did not fall outside of the private search doctrine because Yahoo could not identify the individuals who reviewed the flagged files at Yahoo. The court reasoned that “[a]ll that needs to be established is that a private entity previously inspected the same images as NCMEC and Detective Keller subsequently reviewed.” App. B at 36. The court recognized, nonetheless, that a circuit split exists as to the “the application of the private search doctrine when no human reviews the underlying CSAM images. App. B at 36-37, 37 n.21 *citing United States v. Montijo*, 2022 WL 93535 at *1 n.2 (M.D. Fla. Jan. 10, 2022) *comparing United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021) *and United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016)

with United States v. Miller, 982 F.3d 412 (6th Cir. 2020) and *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018).)

After addressing Yahoo, the court then turned to the question of whether the NCMEC was a government actor and noted that that was a “far closer question.” The court, however, declined to make a finding as to whether NCMEC was a government actor because it found that NCMEC’s search did not exceed the scope of Yahoo’s search. The court essentially found that NCMEC performed an examination of emails that Yahoo had performed prior. The court then reasoned that the case agent likewise “simply looked at the images himself...to confirm they contained CSAM” and did not therefore exceed the scope of Yahoo’s search. App. B at 35-36. The court made a finding that the case agent “uncovered no new, critical information from the photographs.” App. B at 35.

Finally, the court held that the search warrants would survive Fourth Amendment scrutiny under the good faith exception to the exclusionary rule.

The Motion to Suppress the Fruits of the Yahoo Search Warrant

Mr. Williamson additionally filed a motion to suppress the email account search warrant, asserting that the warrant violated the Fourth Amendment’s particularity requirement because it was overbroad in time and scope. Mr. Williamson asserted that the email account warrant sought virtually unlimited data and lacked any temporal restrictions. While the warrant sought seven categories of information, it also sought “account activity from creation to 11/24/20.”

The district court made a detailed analysis of the warrant and found it to be adequately particularized. The court reasoned that “the warrant contemplated a two-step procedure whereby Yahoo was initially compelled to turn over all requested records pertaining to the vladlover50 account regardless of whether they were evidence, contraband, or instrumentalities of the stated crime, it confined the subsequent search of those documents to the above-referenced seven distinct categories of information.” Those seven categories were account information, evidence of user attribution, calendar, contacts, Yahoo email, photos, and search history. With respect to the lack of any temporal limitation, the court agreed that the warrant lacked any such limitation but reasoned that the omission did not render the warrant invalid. The court went on to recognize that the “warrant (like most warrants) could have been better drafted.” App. C at 18. In the end, however, the court reasoned that it did not need to decide whether the warrant violated the particularity requirement because it was making a finding that the warrant fell into the good-faith exception to the exclusionary rule. The court held that the Government met its burden of proving that the warrant was not so facially deficient that the detective could not have reasonably assumed it was lawful.

Mr. Williamson later proceeded to a jury trial. The jury went on to render verdicts of guilty on all counts. The district court imposed sentences of life imprisonment on Count One; concurrent terms of 360 months of imprisonment on Counts Two, Three, and Four; a concurrent term of 240 months imprisonment on

Counts, Five, Six, and Seven; and a concurrent 120 months imprisonment on Count Eight.

Mr. Williamson then appealed to the Eleventh Circuit. On June 30, 2026, the Eleventh Circuit issued an opinion affirming the convictions. App. A. The court found that the district court did not clearly err in finding that Yahoo acted a private citizen rather than a government agent when it searched the email account. *Id.* at 14. In so holding, it reasoned that “[t]he 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.” *Id.* at 15 citing *United States v. Simpson*, 904 F.2d 607, 609-10 (11th Cir. 1990).

The court additionally held that law enforcement did not exceed the scope of Yahoo’s search. *Id.* at 19-20. It agreed with the district court that the Government did not fail to establish the scope of the search by not presenting testimony from the Yahoo employee who reviewed the images. *Id.* at 19-20. It relied on the fact that a Yahoo employee testified, generally speaking, “that the company’s agents review all images that are submitted in a NCMEC report” and that the investigating detective testified that “he looked only at images that were first re-viewed by Yahoo and NCMEC before seeking the search warrants.” *Id.* at 19. The Eleventh Circuit further provided, Mr. Williamson “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." *Id.* at 19-20.

With respect to the overbreadth of the Yahoo warrant, the court seemingly believed that the warrant may have been overbroad but found that the good faith exception precluded the need to reach that question:

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.

Id. at 23. With respect to whether the warrant was so facially deficient that the executing officers could not have reasonably relied on it, the court found that it did not fail to "particularize the place to be searched or the things to be seized" because it "identified the place to be searched (the Yahoo account) and the things to be seized (information from the account)." *Id.* at 24-25 (internal citations omitted). The court did not address the fact that the affiant of the search warrant was also the executing officer.

This petition follows.

REASONS FOR GRANTING THE PETITION

I. The Question of Whether Email Service Providers and the NCMEC Act as Government Entities When They Search Private Email Accounts

The evidence presented in the lower court clearly established that *both* Yahoo and NCMEC were acting as government agents within the purview of the Fourth Amendment. In the application for the search warrant for Mr. Williamson's residence, law enforcement relied almost exclusively on the information that Yahoo and the NCMEC obtained from the warrantless searches they performed.

"A search by a private person does not implicate the Fourth Amendment unless he acts as an instrument or agent of the government." *United States v. Steiger*, 318 F.3d 1039, 1045 (11th Cir. 2003). This Court has provided that the question of whether a private entity is acting as an agent of the state will vary depending on the circumstances of the case, with no one factor being determinative in every scenario. *See Lugar v. Edmondson*, 457 U.S. 922, 939, 102 S.Ct. 2744, 73 L.Ed.2d 482 (1982); *Brentwood Acad. v. Tennessee Secondary Sch. Athletic Ass'n*, 531 U.S. 288, 295-96, 121 S.Ct. 924, 148 L.Ed.2d 807 (2001).

The Eleventh Circuit has set out more defining standard, holding that a private person or entity acts as a government agent if (1) "the government knew of and acquiesced in the intrusive conduct, and (2) "the private actor's purpose was to assist law enforcement efforts rather than to further his own ends." *United States v. Allen*, 854 Fed. Appx. 329, 333 (11th Cir. 2021).

In searching private email accounts such as the “vladlover” accounts, Yahoo acted as an agent for the government. To be sure, the government clearly knew of Yahoo’s search and reporting activities. Federal law, indeed, required Yahoo to report any findings of suspected child pornography to the NCMEC. If Yahoo fails to do so, the law subjects Yahoo to fines of up to \$150,000 for a first, single violation and up to \$300,000 for each subsequent violation. 18 U.S.C. § 2258A(e). Furthermore, when Congress enacted the Protect our Children Act of 2008, it specifically intended for Yahoo and other such ESPs to essentially act in a law enforcement role. *See* Legislative History of Protect our Children Act of 2008, 154 Cong. Rec. H10241-02, H10250, 2008 WL 4373171 (stating “Internet companies will need to do their part too. When we begin to hold Web sites accountable for the images that they host, we’ve taken the first step towards supporting parents in their efforts to protect children. Our combined efforts will help make the Internet a safer place.”).

Contrary to the lower courts’ findings, the statutes created in the Protect our Children Act compel Yahoo and other ESPs to proactively search for child pornography. *See e.g. United States v. DiTomasso*, 81 F. Supp. 3d 304 (S.D.N.Y. 2015). Even if the Act does not require ESPs to specifically implement procedures for searching out suspected child pornography, the imposition of substantial penalties for the failure to report suspected child pornography would compel any reasonable entity to implement procedures for seeking out any such material so as to avoid any potential criminal liability. Nonetheless, a private entity can still be an agent of the government even if it is not compelled to act on behalf of the government.

For instance, this Court has found that when an individual volunteers to assist law enforcement with a police function, with law enforcement's knowledge, the individual is a government actor. *See United States v. Henry*, 447 U.S. 264, 100 S.Ct. 2183, 65 L.Ed.2d 115 (1980). The Court addressed in *Henry*, a situation where law enforcement requested a confidential informant who was in custody with other inmates to "be alert to any statements made by the federal prisoners, but not to initiate any conversation with or question" the defendant in that case with respect to a bank robbery he was charged with. *Id.* at 266. Under those circumstances, the Court found that the informant was an agent of the government for Sixth Amendment purposes even though law enforcement did not instruct the informant to proactively seek out incriminating information from the defendant. *Id.* at 274-75. The situation at issue in the instant case is effectively the equivalent of the scenario the Court considered in *Henry*. As in *Henry*, Yahoo was asked to be alert for certain information and to report any such information it learned of. In both scenarios, the governmental requests rendered those otherwise private parties agents of the government.

In addition, contrary to the reasoning of the lower courts, the fact that the government did not cooperate with Yahoo in the investigation of Mr. Williamson's emails should be of no consequence. The Government had knowledge of and acquiesced in Yahoo's searching of email accounts. Beyond that, as set forth above, the Government effectively compelled Yahoo to do so. Suggesting that Yahoo could not be a government actor because the government did not actively participate in Yahoo's actions would nullify the long line of cases that address when and how private

entities can act as government agents. Indeed, this Court has held that “surely [it] cannot be that government, state or federal, is able to evade the most solemn obligations imposed in the Constitution by simply resorting to the corporate form.” *Lebron v. Nat’l R.R. Passenger Corp.*, 513 U.S. 374, 375, 115 S.Ct. 961, 130 L.Ed.2d 902 (1995). Consistent with that reasoning, if the government needed to actively participate in a private entity’s actions in order for the private entity to be deemed a government actor, then law enforcement and other government entities could simply sidestep the doctrine by enlisting private entities to do their bidding and then simply turn a blind eye to the private entities’ actions.

Given the circumstances of this case, the statutes discussed above effectively deputize ESPs such as Yahoo as federal agents. Indeed, the entire federal enforcement scheme relies on ESPs such as Yahoo to function as discussed above. For those reasons, the question presented is one of great importance that is likely to arise in numerous cases in the future.

**A. Yahoo Performed a Public Function that is Traditionally Reserved
for Law Enforcement**

As set forth above, Yahoo was acting pursuant to its obligations under federal law. In addition, Yahoo employs an entire division to serve the purpose of searching emails for possible child pornography. The evidence presented at the hearing in the district court did not even suggest that Yahoo profits from the work of that division. It is implausible to believe that the work of that division could, in any way, turn a profit for Yahoo. On the contrary, the searching of emails and reporting to NCMEC

serves only to comply with federal regulations and to assist law enforcement in the course thereof.

Furthermore, in carrying out its obligations under the Protect Our Children Act, Yahoo is permitted to possess child pornography. Any person or non-law enforcement entity that possessed such material would be committing serious crimes. Federal law thereby confers immunity on ESPs such as Yahoo that are typically only extended to law enforcement. By effectively requiring Yahoo to search out and report suspected child pornography, and conferring immunity on the company in carrying out those functions, the government has compelled Yahoo to perform a public function that is traditionally reserved for law enforcement.

**B. The Government has Insulated Itself into a Position of
Interdependence on ESPS such as Yahoo**

Yahoo and the NCMEC are clearly in such a “symbiotic relationship.” *Id.* As discussed above, federal law requires Yahoo to report to NCMEC. 18 U.S.C. § 2258A. And, again, Yahoo is subject to serious penalties if it fails to adhere to the reporting mandates. *Id.* Furthermore, while Yahoo is not specifically required by statute to search its email accounts for child pornography, Yahoo does so as a matter of course in an effort to comply with the statutory reporting requirements. The NCMEC, in turn, relies on the reports of ESPs such as Yahoo to carry out its function. The NCMEC’s existence would be futile without the help of ESPs such as Yahoo.

As further evidence of the symbiotic relationship, Yahoo (through its owner Verizon) touts its partnership with NCMEC. Verizon’s corporate policy describes having a “close partnership” with NCMEC. *See* Verizon Digital Safety Policy,

available at <https://www.verizon.com/about/ourcompany/company-policies/digital-safety>. Verizon, moreover, is a “Protector level” sponsor of NCMEC and has donated millions of dollars to NCMEC to “further support NCMEC’s mission...[and] to amplify NCMEC’s voice.” *Id.* Yahoo and the NCMEC clearly work hand-in-hand in a symbiotic relationship carrying out the statutorily mandated functions of the NCMEC.

Moreover, Yahoo also satisfies the “nexus” test due to its close relationship with NCMEC, which is itself a state actor. *See e.g. United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) (holding NCMEC to be a governmental entity or agency for Fourth amendment purposes). Section 2258A delegates to the NCMEC powers mandating that NCMEC is the sole collaborator with state and federal law enforcement in carrying out its duties. *Id.* at 1296. Likewise, the NCMEC alone maintains the CyberTipline that ESPs such as Yahoo must report to. Those ESPs, moreover, are obligated to make reports to that tipline, not to law enforcement. The NCMEC, in turn, makes the reports to law enforcement. The statutory framework that imposes the relevant obligations on ESPs and the NCMEC is a well-oiled machine that seeks out and initiates law enforcement investigations into child pornography. The government clearly relies on and is dependent on ESPs and the NCMEC in investigating and prosecuting those serious crimes. Yahoo and the NCMEC are therefore acting as state actors.

As the cases cited herein demonstrate, virtually every ESP has conducted searches of email accounts. As such, the instant issue impacts every person who has

an email account – the vast majority of the entire population. As a result, the instant question is one of great public importance that will have far reaching effects. Indeed, the question will impact every case in which suspected contraband is found in email accounts. The question is only going to arise with ever increasing frequency in the future. It is, consequently, imperative for the lower courts to have greater guidance on the question presented.

II. The Question of Whether the Private Search Doctrine Applies when no Human Reviews the Alleged Contraband Contained in a Private Email Account

In the instant case, the Government did not, and seemingly could not, present testimony from any witness at Yahoo who would have viewed the images at issue. It similarly failed to present any reliable testimony to establish that the NCMEC actually viewed the images at issue. The NCMEC originally claimed it did not view the images, only to change that position later. Regardless, the NCMEC does not know who allegedly viewed the images, or when they were allegedly viewed. The NCMEC also did not know whether the “hash matches” corresponding to six of the images in the CyberTipline Report had been previously categorized by NCMEC. Therefore, with respect to the searches conducted by *both* Yahoo and the NCMEC, the Government presented no evidence of what *actually* occurred.

The district court and the Eleventh Circuit below found that those facts were immaterial. The courts rejected Mr. Williamson’s contention that Yahoo’s search did not fall outside of the private search doctrine because Yahoo could not identify the individuals who reviewed the flagged files at Yahoo. The courts found it sufficient

that the Government proved that, generally speaking, Yahoo has a policy that the company's agents review all images that are submitted in a NCMEC report and the detective claimed that he looked "only at images that were first reviewed by Yahoo and NCMEC before seeking the search warrants." App. A at 19. It also specifically held that "there is no requirement that the government present testimony from the person who reviewed the files." *Id.* In the end, however, the Government presented no evidence that Yahoo actually followed its policies when it searched the email accounts. The Yahoo representative who testified at the motion hearing, initially testified that a certain former Yahoo employee personally reviewed the images at issue, but later admitted that she did not know whether any employee of Yahoo actually even viewed the images at all. Therefore, while evidence was presented that images purportedly must be viewed before the images are submitted to the CyberTipline, the Government presented no evidence to show that that actually occurred in the instant case.

Even if one assumes for purposes of argument that Yahoo carried out searches of the email accounts as a private entity, the question remains whether law enforcement's subsequent search exceeded whatever the scope of the private search was. The Government may replicate a private search, "as long as government officials constrain their search to the parameters of the search conducted by the private individual." *United States v. Harling*, 705 Fed. Appx. 911, 916 (11th Cir. 2017) *citing* *United States v. Young*, 350 F.3d 1302, 1306–07 (11th Cir. 2003); *see also* *United States v. Jacobsen*, 466 U.S. 109, 115, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984); *Walter*

v. United States, 447 U.S. 649, 100 S.Ct. 2395, 65 L.Ed.2d 410 (1980). Consequently, law enforcement violates the Fourth Amendment if it conducts a search that is broader in scope than the previously occurring private search. *Id.* The lawfulness of law enforcement’s actions thereby turns on the scope of the earlier private search.

The district court recognized that a circuit split exists as to the “the application of the private search doctrine when no human reviews the underlying CSAM images.” App. B *citing United States v. Montijo*, 2022 WL 93535 at *1 n.2 (M.D. Fla. Jan. 10, 2022) *comparing United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021) *and United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) *with United States v. Miller*, 982 F.3d 412 (6th Cir. 2020) *and United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018).)

Under circumstances similar to those of the instant case, the Ninth Circuit, in *United States v. Wilson*, *supra*, 13 F.4th 961, found that law enforcement’s actions exceeded the scope of an earlier private search. In that case, Google made a report of suspected child pornography to the NCMEC CyberTipline. Google had set forth in a declaration that it did not view the images prior to submitting them to NCMEC. *Id.* at 965. The NCMEC passed Google’s report on to law enforcement. The investigating agent, like the case agent in the instant case, had a policy that “called for inspecting the images without a warrant whether or not a Google employee had reviewed them.” *Id.* at 965. The Ninth Circuit found under the circumstances that the government did not carry its burden to prove that law enforcement’s warrantless search of the images was valid. *Id.* at 971. The court held that the “government’s actions here

exceed the limits of the private search exception as delineated in *Walter and Jacobsen* and their progeny.” *Id.*

The Ninth Circuit drew on the Tenth Circuit’s earlier decision in *United States v. Ackerman*, *supra*, 831 F.3d 1292. In that case, AOL came upon suspected child pornography sent in an email and forwarded the email the NCMEC. The Tenth Circuit addressed whether the NCMEC qualified as a government agency. It stated at the outset that “the problem of drawing a line between public and private entities is an old and difficult one.” *Id.* at 1295. Relying on, *Trustees of Dartmouth College v. Woodward*, 17 U.S. (4 Wheat.) 518, 668–69, 4 L.Ed. 629 (1819), it reasoned that “the calling card of a governmental entity is whether it is ‘invested with any portion of political power, partaking in any degree in the administration of civil government, and performing duties which flow from the sovereign authority.’” *Id. quoting id.* The court then discussed the structure of the NCMEC, the tasks it performed, and the authority under which it operated. It noted that “in the face of so much law and evidence suggesting NCMEC qualifies as a governmental entity, the government offers almost no reply.” *Id.* at 1298. The Tenth Circuit ultimately held that NCMEC is a government actor and that NCMEC conducted a search. It went on to reverse the denial of a motion to suppress but remanded the case to the district court for further findings. In doing so, it stated:

Surely hard questions remain to be resolved on remand, not least the question whether the third-party doctrine might preclude Mr. Ackerman's claim to the Fourth Amendment's application, a question the government has preserved and the district court and we have reserved. But about one thing we can be very certain. There can be no doubt that NCMEC does important work and that its work can continue

without interruption. After all, it could be that the third-party doctrine will preclude motions to suppress like Mr. Ackerman's. Or that changes in how reports are submitted or reviewed might allow NCMEC to access attachments with matching hash values directly, without reviewing email correspondence or other attachments with possibly private, noncontraband content—and in this way perhaps bring the government closer to a successful invocation of the private search doctrine. Or it may be possible that the government could cite exigent circumstances or attenuation doctrine or special needs doctrine or the good faith exception to excuse warrantless searches or avoid suppression in at least some cases. But even if not a single one of these potential scenarios plays out—and we do not mean to prejudge any of them—we are confident that NCMEC's law enforcement partners will struggle not at all to obtain warrants to open emails when the facts in hand suggest, as they surely did here, that a crime against a child has taken place.

Id. at 1308-09.

In contrast to the Ninth and Tenth Circuits, and more consistent with the Eleventh Circuit below, the Fifth Circuit held in *Reddick, supra*, 900 F.3d 636, that a detective's search of forwarded images from the NCMEC did not violate the Fourth Amendment. In *Reddick*, the defendant uploaded digital files to a Microsoft cloud hosting service. *Id.* at 637-38. Microsoft utilized a program that scanned the hash values of files in the cloud to locate any suspected known CSAM files. *Id.* The program located such suspected files in the defendant's account and sent a CyberTips report to the NCMEC, which forwarded the report to law enforcement. *Id.* at 638. A detective then viewed the files and determined that they were CSAM. *Id.* After the defendant was later charged with associated federal offenses, he argued that the detective's warrantless search of the files violated the Fourth Amendment. *Id.* When the case reached the Fifth Circuit on appeal, it reasoned “[t]he question presented here, then, is whether, by the time Detective Ilse viewed the suspect image files,

Reddick's expectation of privacy in his computer files had already been thwarted by a private third party.” *Id.* Relying on *Jacobsen*, the Fifth Circuit held “when Detective Ilse opened the files, there was no 'significant expansion of the search that had been conducted previously by a private party' sufficient to constitute ‘a separate search.’” *Id.* at 639 quoting *Walter*, 447 U.S. 649 at 657. The court noted that, in that case, “there is no allegation that Detective Ilse conducted a search of any of Mr. Reddick’s files other than those flagged as child pornography.” *Id.* Based on that fact, it distinguished its holding from *Ackerman*, where “an investigator conducted a search of an email and three attachments whose hash values did not correspond to known child pornography images.” *Id.* at 640 citing *Ackerman*, 831 F.3d at 1306.

Two years later, in *Miller*, *supra*, 982 F.3d 412, the Sixth Circuit adopted the Fifth Circuit’s reasoning. In that case, Google scanned the defendant’s Gmail files for hash-value matches of suspected CSAM, found suspected CSAM, and sent a report with the files to the NCMEC. *Id.* at 417. No Google employee viewed the files. *Id.* at 420. A detective later viewed those same files and connected the files to the defendant. *Id.* at 417-18. The defendant argued that the detective’s warrantless search violated the Fourth Amendment. The court reasoned that a pertinent question was “whether the detective’s manual search would disclose anything more than what Google’s hash-value search showed.” *Id.* at 418. The court went on to follow *Reddick* and found that no Fourth Amendment violation occurred.

Most recently, the Fourth Circuit addressed the issue and noted the circuit split that existed between *Maher*, *Wilson*, *Miller*, and *Reddick*. *United States v.*

Lowers, 170 F.4th 134, 151 (4th Cir. 2026). The Fourth Circuit joined the position of the Second and Ninth Circuits:

We further hold that, unless someone visually inspects the contents of a file containing apparent CSAM prior to law enforcement doing the same, the defendant maintains a reasonable expectation of privacy in the file and the private search doctrine is inapplicable. In reaching this holding, we align ourselves with the Second and Ninth Circuits, which have reached the same conclusion. *United States v. Maher*, 120 F.4th 297 (2d Cir. 2024); *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021).

Id. at 156.

As the cases above explicitly note, a circuit split exists on the question of whether law enforcement's review material sent by an ESP or the NCMEC violates the Fourth Amendment, particularly when the Government does not present evidence of an actual human being reviewing the suspected contraband that is sent to law enforcement. As with the preceding question, the instant question will have far reaching effects. Again, nearly every email account serviced by a United States provider is regularly being searched. The searches are likely to occur with ever increasing frequency in the future. At least six circuits have addressed the instant questions or questions related thereto and have essentially split evenly in their holdings. The lower courts are clearly in need of guidance on the instant case. The review of the instant question could likewise resolve a clear split of decisions among the courts of appeal. For those critical reasons, the Petitioner respectfully requests this Court to take up the question presented.

III. The Question of Whether the Good Faith Exception can Apply to Save a Facially Overbroad Search Warrant when the Same Law Enforcement Officer is Both the Affiant and the Executing Officer

The Eleventh Circuit seemingly recognized that the search warrant for the Yahoo account was unconstitutionally overbroad. The search warrant compelled Yahoo to provide law enforcement with all “account activity from creation to 11/24/20.” The search warrant was not tailored in any way whatsoever to the suspected activity that was under investigation. Instead, the warrant was a general warrant that sought virtually all information connected to the account for the history of the account’s existence. The failure to make any reasonable efforts to particularize the information sought in the warrant violated Mr. Williamson’s right to be free from unreasonable searches and seizures. Nonetheless, despite the facial overbreadth of the warrant, the Eleventh Circuit found that the good faith exception to the exclusionary rule would operate to save the fruits of the unconstitutional search warrant.

A. The Yahoo Search Warrant Violated the Fourth Amendment’s Particularity Requirement

The protections of the Fourth Amendment dictate “searches deemed necessary should be as limited as possible.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). “The ‘specific evil’ that limitation targets ‘is not that of intrusion per se, but of a general, exploratory rummaging in a person’s belongings.’” *United States v. Blake*, 868 F.3d 960, 973 (11th Cir. 2017) *quoting Coolidge*, 403 U.S. at 467. “That type of rummaging was permitted during the colonial era by the ‘general warrant,’ an instrument ‘abhorred by the colonists.’” *Id.*

quoting id. “The Fourth Amendment is intended to preclude ‘general warrants’ by ‘requiring a ‘particular description’ of the things to be seized.” *Id. quoting id.*

The analysis of the instant issue revolved around two opinions from the Eleventh Circuit, *Blake, supra*, 868 F.3d 960, and *United States v. Alford*, 744 F. App’x 650 (11th Cir. 2018). In *Blake*, the Eleventh Circuit considered whether two warrants - one issued to Microsoft and the other issued to Facebook - violated the particularity requirement of the Fourth Amendment. *Blake*, 868 F.3d at 973-74. Both warrants sought information pertaining to the investigation of a prostitution ring. *Id.* With respect to the Microsoft warrant, the court found that the warrant “limited the emails to be turned over to the government, ensuring that only those that had the potential to contain incriminating evidence would be disclosed.” *Id.* at 973. The court further reasoned, however, that “it is somewhat troubling that the Microsoft warrant did not limit the emails sought to emails sent or received within the time period of Moore’s suspected participation in the conspiracy.” *Id.* at 973 n.7. It concluded, nonetheless, that the warrant was not unconstitutional because it was limited in scope to only “only discrete categories of emails that were connected to the alleged crimes.” *Id.* The court only went so far as to hold that the warrant “was okay.” *Id.* at 973.

As to the Facebook warrant, on the other hand, the court found that the warrant “required disclosure to the government of virtually every kind of data that could be found in a social media account.” *Id.* at 974. The court found the all-encompassing scope of that warrant unnecessary. *Id.* The court went on to provide

examples of how the warrant could have been more narrowly tailored to comply with the particularity requirement. *Id.* It noted that, “[w]ith respect to private instant messages, for example, the warrants could have limited the request to messages sent to or from persons suspected at that time of being prostitutes or customers.” *Id.* It further provided that the warrants should been limited to requesting only data from the time period that the defendant was suspected of participating in the conspiracy. *Id.* The court found that such “limitations might then have provided probable cause for a broader, although still targeted, search of Moore’s Facebook account.” *Id.* It further held that “[t]hat procedure would have undermined any claim that the Facebook warrants were the internet-era version of a ‘general warrant.’”¹ *Id. citing Coolidge*, 403 U.S. at 467; *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473, 2488–91, 189 L.Ed.2d 430 (2014).

One year after *Blake*, the Eleventh Circuit decided *Alford*, *supra*, 744 Fed. Appx. 650. In *Alford*, law enforcement sought and obtained a search warrant directed to Google in connection with a child pornography investigation. *Id.* at 652. The warrant at issue in *Alford* sought a broad range of types of information but was narrowly tailored to limited information surrounding a communication made on a specific date. *Id.* The warrant was specifically confined to only information pertaining to a specific date and time, compelling Google to provide only data “which may aid in obtaining the identification and/or location of the individual whom contacted K-mart

¹ Despite those shortcomings, the court found that the warrant fell within the good-faith exception to the exclusionary rule. *Id.* at 974-75.

in Hamilton, MT via phone call [to various phone numbers] on September 16th, 2014 at approximately 2145 hours MST.” *Id.* The court found that the *Alford* warrant fell “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.” *Id.* at 653. The court further provided that the warrant affiant 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.” *Id.*

Turning to the instant case, the warrant issued to Yahoo was materially indistinguishable from the *Blake* Facebook warrant. The warrant at issue in *Blake*, like the warrant at issue in the instant case, was not limited in time or scope. The request made in the warrant to Yahoo was the functional equivalent of a general warrant. Just as the *Blake* Facebook warrant could have been tailored to data relevant to the suspected offenses being investigated, the Yahoo warrant could have been just as narrowly tailored. Law enforcement could have easily limited the data requested to only information pertaining to the accountholder’s identity and to only activity surrounding the suspected transmissions of child pornography. Those limitations would have allowed law enforcement to obtain the information it needed without delving into essentially all of the data arising from the lifetime of the email account. Just the same, law enforcement could have easily restricted account activity data to only a specific date range encompassing the suspected dates the potential

child pornography was transmitted. By instead requesting all “account activity from creation...” the warrant potentially sought decades worth of data.

The warrant at issue in the instant case was also remarkably different from the warrant this Court considered in *Alford*. The warrant at issue in *Alford* was narrowly tailored to limited information surrounding a communication made on a specific date and at a specific time. The warrant further narrowed the requested information to that which could be used to determine the identification and location of the parties to a specific communication. The warrant at issue in the instant case had no such comparable limitations whatsoever, even with respect to the seven categories of requested information.

In the end, the warrant at issue in the instant case compelled all “account activity from creation to 11/24/20.” The phrase encompassed every single email, attachment, search history, webpage visited. Virtually no information fell outside the purview of the warrant. Consequently, the warrant was not sufficiently narrowly tailored to comply with the Fourth Amendment’s particularity requirement.

B. The Good-Faith Exception did not Apply to Save the Fruits of the Unconstitutional Search Warrant

As set forth above, the Eleventh Circuit found in *Blake* that the good faith exception applied despite the overbreadth of the search warrant at issue. When the warrant at issue in *Blake* was executed, of course, the Eleventh Circuit obviously had not issued its opinion in *Blake*. Since 2017, however, *Blake* has been the law, in the Eleventh Circuit at least. The *Blake* opinion was, therefore, undoubtedly binding precedent at the time the warrant to Yahoo was issued in the instant case. Moreover,

as set forth above, the Yahoo warrant was remarkably similar to the Facebook warrant at issue in *Blake*. In light of *Blake*, no reasonable law enforcement officer could have relied on the search warrant given the warrant's obvious overbreadth.

This Court held in the landmark *Leon* opinion that the Government would not be barred from using evidence that was obtained from a faulty search warrant "by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be unsupported by probable cause." *United States v. Leon*, 468 U.S. 897, 900, 905, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984) (emphasis added).

Even when the good-faith exception might otherwise apply, this Court has recognized that four exceptions exist to the *Leon* good-faith exception:

- (1) where "the magistrate or judge in issuing a 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 magistrate wholly abandoned" his detached and neutral 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 upon 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."

United States v. Martin, 297 F.3d 1308, 1313 (11th Cir. 2002) *quoting Leon*, 468 U.S. at 923.

The warrant at issue in this case squarely fell within one of the recognized exceptions to the good-faith exception: that is 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.” *Id.* at 1313. Given the facial overbreadth of the Yahoo warrant, no reasonable law enforcement officer would have relied on it.

Of particular importance, the Eleventh Circuit did not seemingly consider or take issue with the fact that the same law enforcement officer drafted the affidavit for the search warrant and then executed the subsequently issued warrant. While that practice is not uncommon, it is pertinent to the question of whether the officer could rely in good faith on a facially overbroad search warrant. When, as here, the officer drafts a warrant that fails to particularize the place to be searched and the things to be seized in any meaningful way whatsoever, despite a case that clearly indicates the facial insufficiency of the warrant, that same officer cannot reasonably presume that a subsequently issued warrant is valid. Under the circumstances, the instant case presents a question of great importance that this Court should consider under its supervisory power. Petitioner respectfully requests this Honorable Court to exercise its supervisory powers to consider whether the Eleventh Circuit “departed from the accepted and usual course of judicial proceedings” in applying the good faith exception. SUP. CT. R. 10(a).

CONCLUSION

Based on the foregoing, the Petitioner respectfully requests that this Honorable Court grant this petition for a writ of certiorari.

Respectfully Submitted on this 28th day of September 2026,



BJORN E. BRUNVAND
Brunvand, Wise & Farinella
615 Turner Street
Clearwater, Florida 33756
Ph: (727) 446-7505
Email: bjorn@acquitter.com
Florida Bar No. 0831077
Counsel of Record for Petitioner