Appendix B: The District Court's Opinion Below (Doc. 114)

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA

v. Case No. 8:21-cr-355-WFJ-CPT

GREGORY ALLEN WILLIAMSON
a/k/a "VLAD VALD"
_____/

REPORT AND RECOMMENDATION

Before me on referral is Defendant Gregory Allen Williamson's contested motion to suppress evidence seized from his Yahoo[1] email account and his home pursuant to two search warrants authored by a North Port Police Department Detective (NPPD), James Keller. (Docs. 44, 106). Detective Keller obtained these warrants following his review of suspected child pornographic images that Yahoo found in Mr. Williamson's email account without a warrant, and that were subsequently transmitted to the National Center for Missing and Exploited Children (NCMEC) before being forwarded to Detective Keller. *Id.*

In support of his motion, Mr. Williamson argues that Yahoo and NCMEC's warrantless seizure of the images violated the Fourth Amendment because both entities were functioning as government agents at the time. *Id.* Mr. Williamson

[1] During the relevant period, Yahoo was known as Oath Holdings Inc. d/b/a Yahoo! but will be referred to herein merely as Yahoo for the sake of simplicity.

alternatively contends that even if Yahoo and NCMEC were not state actors, Detective Keller's pre-warrant review of the images was unlawful because it exceeded the scope of Yahoo and NCMEC's private search. *Id.* And lastly, Mr. Williamson asserts that pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), the warrants contained material misrepresentations and omissions, without which they lacked probable cause and are not saved by the good faith exception under *United States v. Leon*, 468 U.S. 897 (1984). (Docs. 44, 106).

I held an evidentiary hearing on Mr. Williamson's motion, during which the Executive Director of NCMEC's Exploited Children Division, Jennifer Newman, a Yahoo legal services manager, Ashley Guizzotti, a former Yahoo employee, Jessica Hines, and Detective Keller all testified. (Doc. 99). In accordance with the Court's directive issued shortly thereafter (Doc. 97), the parties subsequently filed proposed findings of fact and conclusions of law based upon the evidence adduced at the hearing (Docs. 105, 106).[2] After careful review of those submissions, as well as the other pertinent portions of the record, I respectfully recommend that Mr. Williamson's motion be denied. Below are my findings of fact and conclusions of law that lead me to this recommendation. Unless otherwise indicated, my factual findings relate to the pertinent time frame and are predicated upon my assessment of the weight of the evidence offered by the parties, including the testimony of the witnesses.

[2] The Court's Order requiring these submissions instructed the parties that they should include in their filings all the facts and legal authority they wished the Court to consider and should not incorporate by reference any other legal memoranda. (Doc. 97)

I.

A.

Yahoo is a private corporation that provides its customers with email services, among other products. (Doc. 99 at 72); Gov't Exh. 3 at 1. NCMEC is a not-for-profit organization that Congress has tasked with operating a CyberTipline. (Doc. 99 at 11–14, 40). The CyberTipline is a national recording and reporting mechanism for child sexual exploitation and essentially serves as a conduit for child pornography-related tips made by the public and electronic service providers (ESPs) like Yahoo. *Id.* at 14–16.

The Protect Our Children Act of 2008 (Protect Act or the Act) dictates that ESPs must make a report to NCMEC of "any [known] facts or circumstances from which there is an apparent violation of" specified criminal offenses involving child pornography. 18 U.S.C. § 2258A(a)(1)–(2). NCMEC, in turn, is mandated by the Act to make each "CyberTipline" report available to federal law enforcement. *Id.* § 2258A(c). ESPs that fail to comply with the strictures of the Act face substantial fines. *Id.* § 2258A(a)(1), (e).

As with many, if not all, ESPs, Yahoo requires its customers to agree to terms of service in order to use its products. (Doc. 99 at 74–76). Among other things, these terms of service prohibit customers from using their Yahoo email accounts to engage in unlawful behavior or to "harm minors in any way . . . ." Gov't Exh. 5 at 2. Yahoo's terms of service also contain an acknowledgement by its customers that the company may pre-screen, access, and/or disclose the contents of their communications under

certain defined circumstances. *Id.* at 3–4. These contractual provisions reflect, at least in part, Yahoo's interest in protecting both its customers and its own reputation by not serving as a "host [for] abusive material, especially [that which causes] harm to minor[s]." (Doc. 99 at 76); *see also id.* at 91. Conduct that falls within this category includes "sharing or distributing . . . imagery or videos of a minor in an abusive way or a sexual way." *Id.* at 76.

To enforce its terms of service, Yahoo scans all sent emails for images[3] of child pornography or, as it is sometimes called, child sexual abuse material (CSAM). *Id.* at 76–80. This process involves an automated comparison of a unique identifier akin to a digital fingerprint associated with each image—known as a hash value[4]—to the hash values of previously identified CSAM files. *Id.* at 20–22, 78–80, 169–70. Yahoo, NCMEC, and other ESPs maintain lists of such hash values for this purpose. *Id.* at 21–23, 77–78, 170.

If there are no matches between a sent image's hash value and those of known CSAM, Yahoo's process generally ends and no further action is taken. *Id.* at 77–78. On the other hand, if there is a "hash match," Yahoo's system places the photograph into a queue for examination by one of its human moderators, who are called trust and safety agents. *Id.* at 77–80. These agents are housed in Yahoo's legal department and

[3] To avoid being repetitious, I will employ the terms image, photograph, and file interchangeably throughout my report and recommendation.

[4] Hash values are also known as PhotoDNA. (Doc. 99 at 79–84).

are continually trained on how to recognize CSAM. *Id.* at 80–81.[5] As a legal services manager, Ms. Guizzotti is involved in managing the work performed by trust and safety agents, including the detection and review of CSAM. *Id.* at 71–72.

One of the roles of a trust and safety agent is to inspect a hash-matched file to ascertain whether it, in fact, contains CSAM. *Id.* at 79–80. If the file includes CSAM, an agent will archive all images in the customer's email account and then analyze those photographs to discern whether they constitute CSAM as well. *Id.* at 79–80, 114–15, 117–22. After consulting with legal counsel about any images that fall into a gray area, the agent will generate a CyberTipline report regarding the CSAM photographs to be submitted to NCMEC. *Id.* at 81–84.

CyberTipline reports sent to NCMEC must identify both the incident type (e.g., child pornography, sex tourism, child molestation, etc.) and the time of the incident. *Id.* at 16–18, 20; Gov't Exh. 1 at 3; Def. Exh. A at 3. ESPs may, but are not mandated to, provide additional information in their CyberTipline reports. (Doc. 99 at 20). In the case of Yahoo, it typically includes such supplemental information as the hash value, file name, and the images it deems to be CSAM, along with the customer's name, email address, and IP address. *Id.* at 81–83; Gov't Exh. 1 at 1–5; Def. Exh. A at 1–5.

[5] An agent's training includes studying the parameters of CSAM, shadowing experienced agents, and participating in monthly "calibrations" with both their manager and Yahoo legal counsel to review images that are borderline CSAM. (Doc. 99 at 79–81, 103–05).

To designate the CSAM photographs for their reports, Yahoo agents must manually select those images from a display screen and then verify that they examined the images by checking a box "yes" in response to the question, "Did Reporting ESP view the entire contents of uploaded file?" (Doc. 99 at 82, 84–86, 101–04, 134–37, 140–41).[6] Once Yahoo forwards a CyberTipline report to NCMEC for further investigation, it disables the customer's account. *Id.* at 86, 126–27. Yahoo uses an internal Excel spreadsheet to track its review of suspected CSAM images and its submissions of CyberTipline reports to NCMEC. *Id.* at 104–05, 111–26.

Upon its receipt of a CyberTipline report, NCMEC conducts an independent comparison of the hash values of the specified images with its own hash list. *Id.* at 21–25. NCMEC divides its hash list into categories based upon the nature of the photographs. *Id.* These categories include apparent child pornography, child pornography unconfirmed, child clothed, child unclothed, and anime. *Id.* at 24–25, 35–36, 66. Pertinent to the issues before the Court, NCMEC applies the label of apparent child pornography to an image when it believes the activity depicted in the photograph "meets the federal definition of child pornography" and it is "overtly clear" a child is involved in that activity. *Id.* at 66. By contrast, NCMEC employs the label of child pornography unconfirmed when it believes "the activity depicted . . . appears to meet the federal definition of child pornography" but "there may be [a]

[6] Ms. Guizzotti and Ms. Hines credibly testified that Yahoo's agents do not check the "yes" box unless they have personally reviewed the images being forwarded to NCMEC. (Doc. 99 at 85, 134–37).

question of the age of the individual seen in that particular image."[7] *Id.* at 35; *see also id.* at 39–40. NCMEC only places an image on its CSAM hash list if the file was reviewed by at least two of its analysts and the analysts reached the same conclusion. *Id.* at 21–24.

NCMEC, however, does not view its designations to be definitive, nor does it consider itself "the determiner[ ] of what is illegal or legal content." *Id.* at 9–10, 25–26. As explained by Ms. Newman, who has worked at NCMEC for twenty-one years, including as a CyberTipline analyst, NCMEC's classification of an image amounts to "an educated and informed impression of what is being depicted," and NCMEC relies on law enforcement to do its own independent "investigation and assessment" of a file. *Id.* at 9–10, 25.

If NCMEC's hash value analysis results in a match, NCMEC will assign the same designation (i.e., apparent child pornography, child pornography unconfirmed, etc.) to the reported images as that ascribed to the identical photographs found in its own list. *Id.* at 22–25, 55–56. If there is no hash match, a NCMEC analyst will review the reported images, determine whether they constitute CSAM, and—if so—affix the proper label. *Id.* at 21–25, 35, 55–58, 66–68; Gov't Exh. 1 at 6; Def. Exh. A at 6. A NCMEC analyst, however, will not inspect any image file unless the ESP affirmatively indicates in its CyberTipline report that it "view[ed] the entire contents of the uploaded

[7] NCMEC also refers to these images as "age indeterminate" or "age difficult." *Id.* at 35, 39.

file" or states that the "entire contents of [the] uploaded file [were] publicly available." (Doc. 99 at 65).

When NCMEC decides that a CyberTipline report warrants further investigation by the police, it will employ an opensource tool called MaxMind to learn the geographical location of the user's IP address so that it can make the report available through a secure online portal to the appropriate law enforcement agency or task force. *Id.* at 14, 17–18, 26–27, 61–62, 64–65; Gov't Exh. 1 at 8; Def. Exh. A at 8. The agency or task force will then receive an email notification alerting it that there is a NCMEC CyberTipline report for its review. *Id.* at 26.

B.

On September 8, 2020, Yahoo scanned an email sent to Mr. Williamson's alleged email account—vladlover50@gmail.com—that included an image which hash-matched to known CSAM. (Doc. 99 at 117); Gov't Exh. 1 at 3; Def. Exh. A at 3. After inspecting this photograph, a Yahoo agent—Jessica Hines—elected to archive 167 image files from Mr. Williamson's account. (Doc. 99 at 114–15, 117–21, 144–45). Those archived files were then examined by at least one other agent and found to include seven photographs containing CSAM. *Id.* at 117–22, 135–45. The file names for those photographs were: image.125-1.jpeg, image.118-1.jpeg, image.120-1.jpeg, image.97-1.jpeg, image.5-1.jpeg, image.4-1.gif, and image.1-1.jpeg. Gov't Exh. 1; Def. Exh. A. Two days later, on September 10, 2020, Yahoo submitted a CyberTipline report to NCMEC relative to these seven photographs, and disabled Mr. Williamson's email account in the process. (Doc. 99 at 122); Gov't Exh. 1; Def. Exh. A.

In its CyberTipline report, Yahoo identified the incident type as possession, manufacture, and distribution of child pornography, and the offense date as September 8, 2020. Gov't Exh. 1 at 3; Def. Exh. A at 3. Yahoo also included the name, phone number, email address, and IP address associated with Mr. Williamson's email account, as well as the upload date and time for each of the seven images.[8] Gov't Exh. 1 at 3–7; Def. Exh. A at 3–7. In addition, Yahoo responded in the affirmative to the question "Did [it] view entire contents of uploaded file?" *Id.*

After receiving Yahoo's CyberTipline report, NCMEC compiled its own report which indicated that a hash match was obtained for all seven images but that no analysts reviewed the files. Gov't Exh. 1 at 6; Def. Exh. A at 6. At the hearing, however, NCMEC's Executive Director, Ms. Newman, clarified that her analysis of the relevant information in advance of her testimony revealed only one of the photographs—image.4-1.gif—hash-matched with NCMEC's list and the remaining six files were examined by one or more of NCMEC's analysts as part of its handling of Yahoo's report.[9] (Doc. 99 at 28–30, 34, 54–61, 66–70). In the end, NCMEC classified two of the files—image.118-1.jpeg and image.1-1.jpeg—as apparent child pornography; four of the files—image.125-1.jpeg, image.97-1.jpeg, image.5-1.jpeg,

[8] According to the report, image.125-1.jpeg was uploaded on November 8, 2019, images.118-1.jpeg and.120-1.jpeg were both uploaded on December 6, 2019, image.97-1.jpeg was uploaded on January 16, 2020, image.5-1.jpeg was uploaded on September 1, 2020, image.4-1.gif was uploaded on September 2, 2020, and image.1-1.jpeg was uploaded on September 8, 2020. Gov't Exh. 1 at 3–7; Def. Exh. A at 3–7.

[9] Ms. Newman explained that this error was caused by a "transition in workflow as a result of [the] COVID" pandemic. (Doc. 99 at 28–29); *see also id.* at 57–60.

and image.4-1.gif—as "CP (unconfirmed)" (i.e., child pornography unconfirmed); and one of the files—image.120-1.jpeg—as "child clothed."[10] Gov't Exh. 1 at 6; Def. Exh. A at 6.

A NCMEC analyst subsequently used MaxMind to geolocate the customer's IP address listed by Yahoo and determined that it was situated in North Port, Florida. (Doc. 99 at 61–62); Gov't Exh. 1 at 8; Def. Exh. A at 8. Once that information was added to NCMEC's report along with the data reflected above, the report was directed first to the Central Florida Internet Crimes Against Children Task Force (CFICAC),[11] and then to the NPPD, where it was assigned to Detective Keller in mid-November 2020. (Doc. 99 at 27, 31, 60–62, 152–56); Gov't Exh. 1 at 10; Def. Exh. A at 10.

By that point in his career, Detective Keller had been with NPPD for approximately eight years and had been tasked with investigating sex crimes for over a year-and-a-half. (Doc. 99 at 153); Gov't Exh. 2; Def. Exh. B. During the latter time frame, Detective Keller was assigned to both CFICAC and the FBI's Child Exploitation and Human Trafficking Task Force and attended multiple training sessions regarding the investigation and identification of CSAM. (Doc. 99 at 152–54); Gov't Exh. 2; Def. Exh. B. He also received forty hours of instruction regarding

[10] With respect to the child clothed photograph, Ms. Hines stated there are sometimes files depicting child sexual exploitation where the minor is not nude which an agent may include in a CyberTipline report depending upon the agent's evaluation of the file. (Doc. 99 at 142).

[11] CFICAC is a subdivision of a national task force—ICAC—that is headed by the Federal Bureau of Investigation (FBI). (Doc. 99 at 153).

CyberTipline reports in particular and additionally worked on multiple cases involving such reports. (Doc. 99 at 154–57); Gov't Exh. 2; Def. Exh. B.

Detective Keller opened NCMEC's CyberTipline report through the on-line portal, reviewed the document, and inspected the seven images provided by NCMEC. (Doc. 99 at 154–60). Following these steps, Detective Keller issued a subpoena to the Internet Service Provider associated with the IP address identified in the report and learned that the subscriber of that IP address was an individual with the initials A.W. residing at 2575 Rolling Road, North Port, Florida. *Id.* at 156, 159–61; Gov't Exh. 2; Def. Exh. B. Detective Keller then consulted the Florida Driver and Vehicle Information Database and discovered that A.W. shared this address with Mr. Williamson. Gov't Exh. 2; Def. Exh. B.

Based upon this information, Detective Keller applied to a state court judge on December 1, 2020, for a search warrant for Mr. Williamson's Yahoo email account. (Doc. 99 at 159–61); Def. Exh. C. Detective Keller included as part of his supporting affidavit a detailed description of the contents of each of the above seven photographs, as well as an attestation that he personally examined the images. (Doc. 99 at 160–63, 180–85); Def. Exh. C. Relying on Florida's definition of CSAM and his own training and experience, Detective Keller also stated that he deemed four of these photographs—image.125-1.jpeg, image.97-1.jpeg, image.4.1.gif, and image.1-1.jpeg —to be CSAM involving prepubescent and minor females; two of the photographs—image.118-1.jpeg and image.5-1.jpeg—to be "age difficult" (i.e., it was difficult for Detective Keller to determine the approximate ages of the subjects in the images); and

the remaining file—image.120-1.jpeg—to be child erotica. (Doc. 99 at 180–85); Def. Exh. C. The state court judge authorized the warrant the same day. Def. Exh. C. In response to this warrant, Yahoo produced, among other items, the photographs that it sent to NCMEC as part of its CyberTipline report, as well as an activity log listing the dates and times that the Yahoo customer logged into the email account. (Doc. 99 at 87–90, 127); Gov't Exh. 1; Def. Exh. A.

With this information in hand, Detective Keller applied for a state search warrant for Mr. Williamson's residence on January 27, 2021. Gov't Exh. 2; Def. Exh. B. Detective Keller's supporting affidavit for this warrant was similar in all material respects to the one he authored for the Yahoo search warrant with the following exceptions. *Compare id. with* Gov't Exh. 1; Def. Exh. A. The detailed descriptions of the images in Detective Keller's residential affidavit included the approximate ages of the minors depicted in, and the labels NCMEC assigned to, those photographs in its CyberTipline report. (Doc. 99 at 160–63, 189–91); Gov't Exh. 2; Def. Exh. B. In addition and of significance here, Detective Keller represented that the four CSAM photographs described above involved a seven to eight year old girl in image.1-1.jpeg; an eleven to twelve year old girl in image.125-1.jpeg; a twelve to thirteen year old girl in image.97-1.jpeg; and a twelve to fifteen year old girl in image.4-1.gif.[12] (Doc. 99 at 160–63, 182, 190–92); Gov't Exhs. 1, 2; Def. Exhs. A, B. Detective Keller also

[12] Detective Keller testified that the estimated age ranges he provides in warrants are based upon his training and experience and are "very conservative" so that he can avoid "any issues . . . with the approximation of ages." (Doc. 99 at 156–57).

represented that NCMEC categorized three of these files—image.125-1.jpeg, image.97-1.jpeg, and image.4-1.gif—as "[c]hild [p]ornography." (Doc. 99 at 160–63, 182, 190–92); Gov't Exhs. 1, 2; Def. Exhs. A, B. As it turns out, however, Detective Keller's characterization of these three NCMEC classifications was different than how NCMEC identified them, as NCMEC had designated the three images, along with another photograph, image.5-1.jpeg, as child pornography *unconfirmed*. *Id.* When asked about this discrepancy at the hearing, Detective Keller explained that as a general matter, he treats NCMEC's labels only as a suggestion and that he views himself as the one responsible for making the final determination of whether an image is truly CSAM. (Doc. 99 at 160–65, 170–73, 182–85). He additionally testified that he did not know until the hearing that NCMEC defined child pornography "unconfirmed" the same way he defined "age difficult." *Id.* at 170–73, 180–83.

Detective Keller executed the residential search warrant on the same day that it was authorized by the state court judge. Gov't Exh. 2; Def. Exh. B. During the course of the search of Mr. Williamson's home, agents seized a variety of electronic equipment, including cell phones, computers, compact discs, digital video discs, hard drives, and disk cards. (Doc. 106-2).

II.

A.

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. The Amendment's protections, however, extend only to items

or places in which a person has a "reasonable expectation of privacy." *California v. Ciraolo*, 476 U.S. 207, 211 (1986) (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).[13] The question of "whether an individual has a reasonable expectation of privacy in the object of [a] challenged search[ ] has come to be known colloquially . . . as Fourth Amendment 'standing.'" *United States v. Ross*, 963 F.3d 1056, 1062 (11th Cir. 2020) (en banc).

In this case, Mr. Williamson asserts that he had a reasonable expectation of privacy with respect to both his residence and his Yahoo emails. (Doc. 106). Although the government does not dispute that Mr. Williamson has Fourth Amendment standing to contest the search of his home, it maintains that he has no such standing relative to his emails. (Doc. 105). Given the threshold nature of this issue, I begin with that question.

To establish Fourth Amendment standing, a person must have "both a subjective and an objective expectation of privacy" in the item or place searched. *United States v. King*, 509 F.3d 1338, 1341 (11th Cir. 2007) (citation and quotation omitted). "The subjective component requires that a person exhibit an actual

[13] The Supreme Court in *United States v. Jones* held that government conduct can also constitute a Fourth Amendment search when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing for the purpose of obtaining information. 565 U.S. 400, 404–08 (2012). Mr. Williamson does not assert a trespass theory here and has thus waived any such claim. *See Hamilton v. Southland Christian Sch., Inc.*, 680 F.3d 1316, 1319 (11th Cir. 2012) ("[T]he failure to make arguments and cite authorities in support of an issue waives it."); *Mendoza v. U.S. Att'y. Gen.*, 327 F.3d 1283, 1286 n.3 (11th Cir. 2003) (finding an issue to be abandoned where no argument was made) (citations omitted). The Court need not address the matter in any event if it accepts my conclusion—described *infra*—that Mr. Williamson had a reasonable expectation of privacy in his Yahoo emails.

expectation of privacy, while the objective component requires that the privacy expectation be one that society is prepared to recognize as reasonable." *Id.* The individual challenging a search bears the burden of satisfying both of these elements. *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978) ("The proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure."); *United States v. Cooper,* 133 F.3d 1394, 1398 (11th Cir. 1998) ("The individual challenging [a] search bears the burdens of proof and persuasion.") (citation omitted).

Both parties rely on Yahoo's terms of service agreement with Mr. Williamson in arguing their respective positions as to whether he had a reasonable expectation of privacy in his Yahoo emails. As referenced previously, that agreement provides, in relevant part, that Yahoo's customers may "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 . . . ." Gov't Exh. 5 at 2. The agreement also states that a customer:

> [A]cknowledge[s] that 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] . . . .

Id. at 3.

The parties interpret these provisions to arrive at diametrically opposing outcomes as it relates to Mr. Williamson's alleged use of his email account to send and receive child pornography. Mr. Williamson insists Yahoo's terms of service "do not provide for any other action to be taken [aside from disabling his account] and certainly do not make clear that information will be disclosed to any other party or law enforcement." (Doc. 106 at 21). The government counters that by voluntarily creating a Yahoo account and stipulating to its terms of service, Mr. Williamson "agree[d] to Yahoo accessing, preserving, and disclosing his account information and content" and "waive[d] any reasonable expectation of privacy that he may have had in his Yahoo account." (Doc. 105 at 6–7).

Mr. Williamson and the government rely on different cases to buttress their terms of service claims. Mr. Williamson primarily predicates his argument on the Sixth Circuit's *en banc* decision in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). (Doc. 106 at 19–22). In that case, the defendant—Mr. Warshak—had an email account with NuVox Communications (NuVox), which was also his internet service provider. *Warshak*, 631 F.3d at 288. Mr. Warshak agreed to NuVox's terms of service, which included the condition that "NuVox may access and use individual Subscriber information in the operation of [NuVox] and as necessary to protect [NuVox]." *Id.* at 287.

As part of its investigation of Mr. Warshak's business operation for fraud and other offenses, the government used a subpoena and court order issued under the

Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.* to obtain thousands of Mr. Warshak's emails from NuVox, at least several of which were apparently of evidentiary value. *Warshak*, 631 F.3d at 281–83, 292 n.22. Mr. Warshak moved the trial court to exclude these emails on the grounds that the government's warrantless seizure of such communications violated the Fourth Amendment. *Id.* at 281–82. The court denied the motion, and Mr. Warshak was ultimately convicted of a number of crimes following a jury trial. *Id.* at 281.

On appeal, the Sixth Circuit commenced its analysis with the issue of Mr. Warshak's Fourth Amendment standing to contest the government's acquisition of his emails. *Id.* at 283–84. The court found Mr. Warshak "plainly manifested" a subjective expectation that these transmissions "would be shielded from outside scrutiny" given that they contained his "entire business and personal life," including matters that were "often sensitive and sometimes damning" to him. *Id.* The court also determined that Mr. Warshak's subjective expectation of privacy was one that society was prepared to recognize as reasonable notwithstanding his terms of service agreement with NuVox. *Id.* at 284–88. The court reasoned:

> As an initial matter, it must be observed that the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy. In *Katz*, the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator to listen in. Similarly, the ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country. Therefore, the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy.

> Nor is the *right* of access. . . . [A]t the time *Katz* was decided, telephone companies had a right to monitor calls in certain situations. Specifically, telephone companies could listen in when reasonably necessary to protect themselves and their properties against the improper and illegal use of their facilities. In this case, the NuVox subscriber agreement tracks that language, indicating that "NuVox may access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service." Thus, under *Katz*, the degree of access granted to NuVox does not diminish the reasonableness of [Mr.] Warshak's trust in the privacy of his emails.

Id. at 286–87 (internal quotation marks and citations omitted).[14]

Although deciding that "some degree of routine access is hardly dispositive with respect to the privacy question," the court did state that it was "unwilling to hold that a subscriber agreement will *never* be broad enough to snuff out a reasonable expectation of privacy." *Id.* at 287. The court noted, for example, that "if [a service provider] expresses an intention to audit, inspect, and monitor its subscriber's emails, that might be enough to render an expectation of privacy unreasonable." *Id.* (internal quotation

---

[14] In arriving at this conclusion, the court recognized "the prominent role that email has assumed in modern communication," observing:

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.

Warshak, 631 F.3d at 284; *see also id.* at 286 ("Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age.").

marks and citations omitted). The court added, however, that where "there is no such statement, the [provider's] control over the [emails] and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy." *Id.* (internal quotation marks and citations omitted). The court further cautioned that in "most situations," a subscriber agreement will not "be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account." *Id.* at 286.

The government does not address *Warshak* and instead cites two other decisions—*United States v. Montijo*, 2022 WL 93535 (M.D. Fla. Jan. 10, 2022) and *United States v. DiTomasso*, 56 F. Supp. 3d 584, 595 (S.D.N.Y. 2014)—to bolster its position. (Doc. 105 at 7). In the first case, the defendant—Mr. Montijo—sent a child pornographic video to another person during a chat on Facebook's instant messaging program. *Montijo*, 2022 WL 93535, at *1–3. Facebook was monitoring the chat (or at least the files circulated at the time) and, upon discovering the video, notified law enforcement. *Id.* The video was thereafter sent to a local police officer, who viewed the video without a warrant and then used the video's contents to obtain search warrants for Mr. Montijo's home and car. *Id.* Mr. Montijo was eventually charged with producing and possessing child pornography following the execution of those warrants. *Id.*

In response to a subsequent motion by Mr. Montijo to suppress this search warrant evidence, the government contended, *inter alia*, that Mr. Montijo did not have

a reasonable expectation of privacy in his Facebook messenger chat. *Id.* at *3. In addressing that issue, the court examined Facebook's terms of service governing Mr. Montijo's use of the platform. *Id.* at *6–7. Those terms of service advised Facebook customers, in pertinent part:

> We employ dedicated teams around the world and develop advanced technical systems to detect misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community. If we learn of content or conduct like this, we *will* take appropriate action—for example, . . . [by] *contacting law enforcement*.
>
> * * *
>
> And we develop automated systems to improve our ability to detect and remove abusive and dangerous activity that may harm our community and the integrity of our Products.

Id. at *7 (emphasis added and in original).

Along with these terms of service, Facebook's Community Standards set forth written guidelines as to what customers could share on Facebook. Gov't Exh. 2 at 12. One of those standards—entitled "Child Sexual Exploitation, Abuse and Nudity"—read, "[w]e do not allow content that sexually exploits or endangers children, [and w]hen we become aware of apparent child exploitation, *we report it to . . . NCMEC[,] in compliance with applicable law*." *Id.* (emphasis added).

In light of this language, the court determined that Mr. Montijo did not have a reasonable expectation of privacy in his messenger communications. *Id.* It explained that Facebook provided him with "fair warning" that "he risked being reported to law

enforcement or NCMEC if Facebook discovered that he sent, received, or distributed apparent child pornography." *Id.*

In the second case, the defendant—Mr. DiTomasso—had an American Online (AOL) email account to which another party sent two emails containing child pornography. *DiTomasso*, 56 F. Supp. 3d at 587. AOL's monitoring programs detected this illicit content and reported it to NCMEC. *Id.* During roughly the same time frame, Mr. DiTomasso also used a separate online platform—Omegle.com—to engage in an anonymous chat with another individual, which Omegle discovered included evidence of child pornography. *Id.* at 588. Omegle likewise reported these chats to NCMEC. *Id.*

Mr. DiTomasso was later charged with the production and transportation of child pornography and moved to suppress the evidence obtained from both AOL and Omegle. *Id.* at 586. In response, the government argued that Mr. DiTomasso did not have a reasonable expectation of privacy in his AOL or Omegle communications because, *inter alia*, both providers cautioned him by way of their user agreements with him that they might be monitoring his activity. *Id.* at 592. Among other things, AOL's privacy policy and customer agreement "forbade users from 'post[ing] content that contain[ed] explicit or graphic descriptions or accounts of sexual acts,'" informed its users that "'AOL reserve[d] the right to take any action it deem[ed] warranted' in response to illegal behavior, including 'cooperat[ing] with law enforcement;'" and stated that "AOL itself may disclose to others—including law enforcement—'information relevant to a crime that has been or is being committed.'" *Id.* at 588.

Omegle's privacy policy advised its customers, in pertinent part, that it kept "'record[s] of the IP addresses involved in every chat' . . . 'for the purpose of law enforcement,'" among other reasons, and that it "captured" and "monitor[ed]" webcam videos on an ad hoc basis "for misbehavior." *Id.* at 588–89 (citation omitted).

The court in *DiTomasso* rejected the government's reasonable expectation of privacy argument, choosing instead to follow the lead of the Sixth Circuit in *Warshak* and the Ninth Circuit in *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008), *rev'd on other grounds,* 560 U.S. 746 (2010). *DiTomasso*, 56 F. Supp. 3d at 592 n.62 (citations omitted). In *Quon*, the Ninth Circuit held that users of text messaging services had a reasonable expectation of privacy in their texts stored on their service provider's network even though the service provider may have been able to access the contents of the messages for its own purposes. *Quon*, 529 F.3d at 904. The *DiTomasso* court reasoned:

> [I]t would subvert the purpose of the Fourth Amendment to understand its privacy guarantee as "waivable" in the sense urged by the government. In today's world, meaningful participation in social and professional life requires using electronic devices—and the use of electronic devices almost always requires acquiescence to some manner of consent-to-search terms. If this acquiescence were enough to waive one's expectation of privacy, the result would either be (1) the chilling of social interaction or (2) the evisceration of the Fourth Amendment. Neither result is acceptable.

Id. at 592.

In reaching this determination, the court in *DiTomasso* looked to the Supreme Court's Fourth Amendment jurisprudence involving what it believed to be analogous

situations. The court noted, for instance, that "the Supreme Court has held that employees, including public employees, enjoy an expectation of privacy in their workplace desks—and that th[is] expectation stays intact vis-a-vis law enforcement even if it would be unreasonable, given the 'operational realities' of the workplace, for employees to expect the same privacy protection from their supervisors." *Id.* at 593, 593 n.64 (citing *O'Connor v. Ortega*, 480 U.S. 709, 717–18 (1987)). The court also observed that the Supreme Court has similarly ruled that a hotel guest's granting of access to his room for "limited purposes," such as housekeeping or an emergency, "neither vitiates [the guest's] expectation of privacy in the room nor authorizes hotel employees to consent to a search by the government on behalf of the guest." *Id.* 593, 593 n.65 (citing *Stoner v. California*, 376 U.S. 483 (1964)).[15]

The *DiTomasso* court went on to conclude:

> Both of these holdings cut against the government's position. In essence, the government argues that by consenting to have his emails and chats searched by AOL and Omegle—as [Mr.] DiTomasso arguably did when he agreed to their respective terms of use—he also consented to permitting the government to search. Fourth Amendment privacy, however, is a context-sensitive question of societal norms. In some domains, people expect information to stay shielded from law enforcement even as they knowingly disclose it to other parties. As the Supreme Court has recognized, workplace desks and hotel rooms are two such domains. In the digital age, electronic communication is another.

[15] The court additionally cited *Chapman v. United States*, 365 U.S. 610 (1961), in which the Supreme Court reached the same conclusion with respect to an apartment.

Id. at 593. In short, the court held that Mr. DiTomasso had a reasonable expectation of privacy in both his AOL emails and Omegle chats. *Id.* at 592–96.

Against this backdrop, I find that Mr. Williamson's Fourth Amendment standing argument has merit. I note at the outset that, as the above discussion reveals, *DiTomasso* undermines rather than buttresses the government's contention that Mr. Williamson did not have a reasonable expectation of privacy in his Yahoo emails. As a result, the government's Fourth Amendment standing argument rests solely on *Montijo* and the court's finding in that case that Mr. Montijo did not have a reasonable expectation of privacy in his Facebook messenger communications given Facebook's terms of service and its Community Standards. While I do not agree with Mr. Williamson's assertion that there is "*no* evidence" Yahoo's subscriber agreement "permitted [it] to disclose information to law enforcement or anyone else" (Doc. 106 at 21) (emphasis added), Yahoo's terms of service do not include the type of language contained in Facebook's user contract or its community standards described in *Montijo*.

Recall that the relevant part of Yahoo's customer agreement authorized it to pre-screen and remove content that violated its terms of service and to access or disclose user content only if it was "required" to do so by law or because it had a good faith belief that such steps were reasonably necessary "to comply with legal process" or to enforce the terms of service. Gov't Exh. 5. As Ms. Guizzotti testified on cross-examination, these terms of service do not indicate to Yahoo's customers that their

"information *will* be disclosed to law enforcement," at least absent some compulsion. (Doc. 99 at 126) (emphasis added).

By contrast, as discussed in *Montijo*, Facebook's terms of service and Community Standards expressly stated that Facebook will proactively reach out to law enforcement and NCMEC when it discovers "harmful conduct towards others" (including—no doubt—harmful conduct involving children) or "situations where [it] may be able to help . . . protect [the] community" (including—again obviously—safeguarding children). *Montijo*, 2022 WL 93535, at *7 ("If [Facebook] learn[s] of [harmful conduct], we *will* take appropriate action . . . [by] contacting law enforcement") (emphasis added and omitted); *id.* ("[Facebook does] not allow content that sexually exploits or endangers children, [and w]hen we become aware of apparent child exploitation, *we report it to . . . NCMEC*[,] in compliance with applicable law.") (emphasis added). Yahoo's user contract, on the other hand, conspicuously makes no mention of aiding or collaborating with the police and, in fact, does not even reference "law enforcement" at all. As a result, I conclude that Mr. Williamson had a reasonable expectation of privacy in his Yahoo emails.[16] A survey of other decisions addressing

[16] Notably, the government does not raise, much less brief, the separate argument that Mr. Williamson consented to the search of his emails based upon Yahoo's terms of service. As the court stated in *DiTomasso*, "[e]ven if a search would otherwise be invalid . . . because it encroaches unreasonably on one's expectations of privacy[,] 'an individual may [nonetheless] consent to a search, thereby rendering it'" permissible under the Fourth Amendment. 56 F. Supp. 3d at 590 (quoting *United States v. Garcia*, 56 F.3d 418, 422 (2d Cir. 1995) and citing *Schneckloth v. Bustamonte*, 412 U.S. 218, 222 (1973)). Because the government does not assert this theory, it has waived the right to do so. *See Hamilton*, 680 F.3d at 1319; *Mendoza*, 327 F.3d at 1286 n.3.

Even if the government is deemed not to have waived this contention, it is difficult to see how it could succeed on a consent theory under the circumstances presented. In *DiTomasso*, the court held

Fourth Amendment standing based upon an ESP's terms of service provides support for this conclusion. *See, e.g.*, *Matter of Search of Encrypted Data Provided by Nat'l Ctr. For Missing & Exploited Children*, 2021 WL 2100997, at *4 (D.D.C. May 22, 2021) (stating that the defendant had a reasonable expectation of privacy in his Google email account even though Google's terms of service "prohibit[ed customers from] using [its] platform to violate the law" and reserved the right for Google to "'take down'" content—such as child pornography—which either violated applicable law or "'could harm [ ] . . . third parties,'" and even though Google "independently and voluntarily [took] steps to monitor and safeguard [its] platform") (citing *United States v. Miller*, 982 F.3d 412, 426 (6th Cir. 2020)); *United States v. Coyne*, 387 F. Supp. 3d 387, 395–96 (D. Vt. 2018) (rejecting the government's contention that the user agreements for Yahoo and Microsoft, among others, vitiated any expectation of privacy despite language in

---

that where, as here, a defendant's constitutional claim is based upon the proposition that an ESP was "acting as [a] government agent[ ] when [it] monitored his electronic communications, the [ESP's] policies only defeat [that] constitutional claim if, by agreeing to them, [the defendant] was consenting to a search by [the ESP] *as* [a] government agent[ ]." 56 F. Supp. 3d at 596. The court went on to find that Mr. DiTomasso consented to AOL's search of his emails but not to Omegle's review of his chats. *Id.* at 596–97. Akin to the court's thinking in *Montijo* on the matter of Fourth Amendment standing, the *DiTomasso* court grounded its consent finding relative to AOL on the fact that AOL's terms of service made it apparent to AOL's users it would *affirmatively* help the police ferret out any wrongdoing by them. As the court observed:

> Not only does [AOL] explicitly warn [its] users that criminal activity is disallowed, and that [it] monitors for such activity[, its] policy also explains that "AOL reserves the right to take any action it deems warranted" in response to illegal behavior, including . . . "cooperat[ing] with law enforcement." The policy also makes clear that AOL reserves the right to reveal to law enforcement information about "crimes[s] that [have] been or [are] being committed." [In short,] AOL's policy makes clear that [it] intends to *actively assist law enforcement*.

Id. at 597 (emphasis added and citations omitted).

As noted above, Yahoo's terms of service do not include the kind of language contained in AOL's policy.

those contracts notifying customers that—in the case of Yahoo—"Yahoo's automated systems analyze[d] all communications content . . . for . . . abuse protection" and—in the case of Microsoft—Microsoft had the right to "access, transfer, disclose, and preserve personal data, including [the customer's] content . . . when [it] ha[d] a good faith belief that doing so [was] necessary to (1) comply with applicable law or respond to valid legal process").[17]

B.

The government argues that irrespective of whether Mr. Williamson has Fourth Amendment standing with respect to his Yahoo emails, his challenge to the subsequent review of his communications by Yahoo, NCMEC, and Detective Keller fails under the private search doctrine. (Doc. 105); *see generally United States v. Jacobsen*,

[17] The Eleventh Circuit's unpublished decision in *United States v. Jones*, 149 F. App'x 954 (11th Cir. 2005) (per curiam)—which neither party references in their respective submissions—does not require a different result. In *Jones*, the court ruled that co-conspirators in a drug ring did not have a reasonable expectation of privacy in the texts messages sent or received by one of their cohorts, who later elected to cooperate with the government and testify against them. *Id.* at 959. In arriving at this determination, the court stated that "an individual sending an e-mail loses 'a legitimate expectation of privacy in an e-mail that had already reached its recipient.'" *Id.* (quoting *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001)).

The problem with applying *Jones* here is two-fold. First, the government does not mention *Jones* or assert the Fourth Amendment standing theory upon which *Jones* relies. As such, the government has waived any such claim. *Hamilton*, 680 F.3d at 1319; *Mendoza*, 327 F.3d at 1286 n.3. This result appears to be especially apt since one of the cases the government does cite—*DiTomasso*—explicitly rejects this line of argument. *DiTomasso*, 56 F. Supp. 3d at 591–92 (characterizing as "baseless" the government's assertion that "by exchanging emails and chats with other people[, Mr.] DiTomasso relinquished his expectation of privacy in those statements").

Second, while it seems undisputed that one of the seven images at issue was included in an email sent by Mr. Williamson, the other six photographs were not, as they were retrieved from Mr. Williamson's archived emails.

466 U.S. 109, 113 (1984); *Walter v. United States*, 447 U.S. 649, 653–59 (1980). Mr. Williamson asserts the opposite. (Doc. 106). I turn to this issue now.

It is well settled that "[a] search by a private [entity] does not implicate the Fourth Amendment unless [it] acts as an instrument or agent of the government." *United States v. Steiger,* 318 F.3d 1039, 1045 (11th Cir. 2003); *see also Skinner v. Ry. Labor Execs. Ass'n*, 489 U.S. 602, 614 (1989) ("Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the [g]overnment."). A corollary to this long-established principle is that where an individual's expectation of privacy in particular information has been "frustrated" by a non-state actor, law enforcement may later lawfully use that information without a warrant. *United States v. Sparks*, 806 F.3d 1323, 1334 (11th Cir. 2015) (citation omitted), *overruled on other grounds by Ross*, 963 F.3d at 1056. As a result, a warrantless search performed by the government following a private search violates the Fourth Amendment only to the extent "it is broader than the scope of the previously occurring private search." *Id.* (citations omitted). A government search crosses this threshold when it "meaningfully exceeds" the parameters of the private search, *United States v. Harling*, 705 F. App'x 911, 816 (11th Cir. 2017), such as when an officer "learn[s] new, critical information" from his examination of the materials at issue, *Montijo*, 2022 WL 93535, at *4–5.

In this case, Mr. Williamson maintains that both Yahoo and NCMEC were functioning as government agents when they engaged in their warrantless review of

his emails and that this intrusive conduct therefore contravened the Fourth Amendment. (Doc. 106). Mr. Williamson also contends that the unlawful searches conducted by Yahoo and NCMEC render Detective Keller's subsequent warrants for his Yahoo email account and his residence fatally infirm. *Id.* After careful review, I find that Mr. Williamson's state actor argument directed at Yahoo fails and that the remainder of his private search challenge necessarily fails as well.

Determining whether a private entity was operating as an instrument or agent of the government centers "on the degree of the [g]overnment's participation in the private party's activities, a question that can only be resolved in light of all the circumstances." *Skinner*, 489 U.S. at 614–15 (internal quotation marks and citations omitted). Courts in this Circuit employ a two-prong test in resolving this issue: (1) whether the government knew of and acquiesced in the challenged conduct, including by openly encouraging or cooperating in the search; and (2) whether the private entity's motive was to assist law enforcement's efforts rather than to advance its own ends. *Id.*; *United States v. Emile*, 618 F. App'x 953, 955 (11th Cir. 2015) (quoting *United States v. Ford*, 765 F.2d 1088, 1090 (11th Cir. 1985); *United States v. Smythe,* 84 F.3d 1240, 1243 (10th Cir.1996)); *see also U.S. v. Propst*, 369 F. App'x 42, 45 (11th Cir. 2010) (citing *Steiger,* 318 F.3d at 1045).[18] The burden of establishing that a private actor is a government agent rests with Mr. Williamson. *United States v. Allen*, 2019 WL 5842684, at 7 (M.D. Fla. Oct. 7, 2019) (citing *United States v. Gumerlock*, 590 F.2d 794, 799 (9th

[18] Unpublished opinions are not considered binding precedent but may be cited as persuasive authority. 11th Cir. R. 36-2.

Cir. 1979)), *report and recommendation adopted*, 2019 WL 5802657 (M.D. Fla. Nov. 7, 2019), *aff'd*, 854 F. App'x 329 (11th Cir. 2021); *United States v. Hearst*, 2022 WL 16832834, at *10 (N.D. Ga. Mar. 10, 2022) (citing *United States v. Ginglen*, 467 F.3d 1071, 1074 (7th Cir. 2006)). On appeal, a district court's determination as to whether a private entity is an arm of the state is reviewed for clear error. *Allen*, 854 F. App'x at 333 (citing *Ford*, 765 F.2d at 1090).

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);

[19] Some courts have viewed the penalties for failing to report child pornography as providing an incentive for ESPs *not* to search for such illicit content so that they can claim willful ignorance. *See, e.g., United States v. Ringland*, 966 F.3d 731, 736 (8th Cir. 2020).

Rosenow, 50 F.4th at 730 (drawing a distinction under the Protect Act between "mandated *reporting*" and "mandated *searching*"); *United States v. Meals*, 21 F.4th 903, 907 (5th Cir. 2021) (observing that while the Protect Act insists ESPs report child exploitation to NCMEC, the Act "neither compels nor coercively encourages internet companies to search actively for such evidence"). Yahoo is thus "free to choose not to search [its] users' data" and, when it does search, it "do[es] so of [its] own volition." *Rosenow*, 50 F.4th at 730. Multiple courts that have confronted this issue—including with respect to Yahoo—have reached the same conclusion. *See, e.g., id.* at 731 (holding "that federal law did not transform Yahoo's . . . private searches into governmental action"); *United States v. Cameron*, 699 F.3d 621, 636–38 (1st Cir. 2012) (holding that Yahoo's statutory duty under the Protect Act to report to NCMEC "did not impose any obligation to search for child pornography," but "merely an obligation to report child pornography of which Yahoo[ ] became aware"); *Phillips v. United States*, 2021 WL 1342301, at *4 (M.D. Fla. Apr. 9, 2021) ("Yahoo[ ] is a private actor, which conducted a private search of the [defendant's] email account.") (citing *Cameron*, 699 F.3d at 637–38); *see also Meals*, 21 F.4th at 907 (rejecting the defendant's argument that the Protect Act transformed Facebook into a government agent); *Miller*, 982 F.3d at 424 (declining to find Google to be a state actor based upon the Protect Act, reasoning that the Act directs "providers only to report child pornography that they know of; it does not compel them to search for child pornography of which they are unaware")

(collecting cases);[20] *Ringland*, 966 F.3d at 736 (same); *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013) (refusing to adopt the defendant's argument that AOL's hash-detection program which automatically reported child pornography to NCMEC in accordance with the Protect Act amounted to state action); *United States v. Richardson*, 607 F.3d 357, 364–67 (4th Cir. 2010) (same); *United States v. Hart*, 2021 WL 2412950, at *8 (M.D. Pa. June 14, 2021) (determining that Kik was not a government actor when it searched a user's account and reported suspected child pornography to NCMEC pursuant to the Protect Act).

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. (Doc. 99 at 91).

Nor does Mr. Williamson prevail on the second prong. Ms. Guizzotti made clear during her testimony that Yahoo proactively searches sent emails because it has an interest in safeguarding both its users and its reputation. *Id.* at 76. Courts have found similar testimony to be unexceptional and consistent with an ESP's expected business interests. *See, e.g.*, *Ringland*, 966 F.3d at 736 (deeming Google not to be a government agent, in part, because it "acted out of its own obvious interests in

[20] As the court pointed out in *Miller*, courts have similarly held that laws mandating teachers or doctors to report child abuse also "do not transform private parties into government actors for purposes of various constitutional provisions." *Miller*, 982 F.3d at 424 (citing *Mueller v. Auker*, 700 F.3d 1180, 1191–92 (9th Cir. 2012); *Brown v. Newberger*, 291 F.3d 89, 93–94 (1st Cir. 2002)).

removing child sex abuse from its platform"); *Cameron*, 699 F.3d 637–38 (stating that although "it is certainly the case that combating child pornography is a government interest[,] this does not mean that Yahoo[ ] cannot voluntarily choose to have the same interest," and adding that a private party will not be deemed to be a government agent "simply because the government has a stake in the outcome of a search") (internal quotation marks and citation omitted); *United States v. Wolfenbarger*, 2019 WL 6716357, at *11–12 (N.D. Ca. Dec. 10, 2019) (concluding that "Yahoo had its own legitimate, independent motivation" for endeavoring to remove child pornography from its services, including "creati[ng] a safe place for its users—many of whom [were] minors themselves") (internal quotation marks omitted); *Coyne*, 387 F. Supp. 3d at 397 ("The ESPs have been very clear about their purpose in identifying child pornography, which is commercial and not primarily altruistic. Obviously the ESPs involved in this case share a moral repugnance for child pornography, but their efforts to detect child pornography and close subscriber accounts involved in its transmission are strongly motivated by business concerns.").

Mr. Williamson's reliance on Yahoo's "Compliance Guide for Law Enforcement" (Guide) in this respect is unavailing. (Doc. 106 at 28); Def. Exh. H. It is true, as he observes, that the Guide provides at the beginning that it "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." Def. Exh. H at 6. It is also true, as Mr. Williamson further notes, that the Guide additionally has a section

specifically devoted to Yahoo's procedures for making reports to NCMEC, in which it states that Yahoo has "worked with law enforcement and [NCMEC] to develop practices for reporting instances of apparent child pornography . . . as required by [the Protect Act]." *Id.* at 12.

That said, the mere fact that Yahoo has developed protocols to facilitate its interactions with the government has no bearing on the company's intent when it searches its customer's emails. *Rosenow*, 50 F.4th at 735 ("[A] private party's otherwise legitimate, independent motivation is not rendered invalid just because law enforcement assistance may further its interests."). At most, it evidences that Yahoo is aware of its obligations under the Protect Act to report known instances of child pornography, not to affirmatively search for such content, and that Yahoo has an understandable interest in ensuring that law enforcement is educated as to its policies and procedures to prevent any confusion on the matter. In sum, I find that Mr. Williamson does not meet his burden of establishing that Yahoo was a state actor when it searched his emails.

Mr. Williamson's NCMEC state actor argument, on the other hand, presents a far closer question. In fact, several courts have found NCMEC to be a government entity or agent for Fourth Amendment purposes. *See, e.g., United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016) (Gorsuch, J.); *Coyne*, 387 F. Supp. 3d at 400 (collecting cases). The Court need not reach that issue here, however, because even assuming *arguendo* that NCMEC was operating as an arm of the state when it inspected Mr. Williamson's emails, its examination did not exceed the scope of Yahoo's review

of those communications. *Montijo*, 2022 WL 93535, at *3 (noting that under the private search dotrine, the government is permitted "to replicate a prior private search [without a warrant] provided it stays within the same parameters") (citing *Sparks*, 806 F.3d at 1334).

To see why this is so, remember that—as a matter of policy—Yahoo will not submit a CyberTipline Report to NCMEC unless one of its agents reviews and manually selects each of the images to be uploaded with the report and then specifically attests that he or she has inspected those photographs by checking a box affirming the same. (Doc. 99 at 82, 84–86, 101–04, 134–37, 140–41). And the evidence in this case demonstrates that this box was checked with respect to Yahoo's examination of Mr. Williamson's emails. The evidence also demonstrates that NCMEC—like Yahoo—ran an automated analysis of those files and had its staff examine six of the seven images reported. As such, I find that NCMEC did not go beyond the boundaries of Yahoo's prior search of Mr. Williamson's emails. *Phillips*, 2021 WL 1342301, at *4 (finding no Fourth Amendment violation where NCMEC did not exceed the scope of Yahoo's private search).

I reach the same conclusion with respect to Detective Keller's review of the images after he received them from NCMEC but he before applied for the warrants for Mr. Williamson's Yahoo email account and his home. I credit Detective Keller's testimony that he simply looked at the images himself at that juncture to confirm they contained CSAM. In doing so, he uncovered no new, critical information from the photographs. He merely saw the same files Yahoo previously analyzed and then made

his own determinations as to whether the photographs constituted CSAM. As a result, Detective Keller also did not exceed the scope of Yahoo's prior search. *See Ringland*, 966 F.3d at 737 ("Because [the officer] searched only the same files that [the ESP] searched, the [officer] did not expand the search beyond [the ESP's] private party search.") (citations omitted); *United States v. Powell*, 925 F.3d 1, 6 (1st Cir. 2018) (finding a government actor's review of screenshotted images of suspected child pornography reported by a private ESP following the ESP's search of a user account did not disclose any previously unknown facts and the government's review did not therefore require a warrant).

The fact that Yahoo may not now be able to identity the particular employees at the company who reviewed the files is not—as Mr. Williamson maintains—of any importance. All that needs to be established is that a private entity previously inspected the same images as NCMEC and Detective Keller subsequently reviewed. *See Montijo*, 2022 WL 93535, at *5 ("[The d]efendant makes much about the [g]overnment not providing evidence on the contractors' identities and how Facebook found the offending files. But Facebook and its contractors are private persons. So the who and how Facebook searches its programs do not lessen the private search doctrine's application here."). Indeed, at least one other court has found that the government's human review of an image after a private ESP performed *solely* an

automated hash analysis fell within the scope of the ESP's private search.[21] *See Miller*, 982 F.3d at 427.

C.

Mr. Williamson's final challenge is that even if the warrants for his Yahoo email account and his residence were valid under the private search doctrine, they nonetheless fail under *Franks* because Detective Keller's supporting affidavits included material misrepresentations and omissions, without which the affidavits lacked probable cause. (Doc. 106). The government counters that Mr. Williamson does not make the requisite showing necessary to sustain his *Franks* argument. (Doc. 105).[22]

It is well established that a search warrant is presumptively valid once issued. *Franks*, 438 U.S. at 171. The Supreme Court instructs, however, that (1) "where [a] defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit," and (2) "the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." *Id.* at 155–56 (emphasis added). The requirement of a *Franks* hearing also extends to situations where facts are intentionally or recklessly omitted

[21] I do note that there is apparently a circuit split about the application of the private search doctrine when no human reviews the underlying CSAM images. *See Montijo*, 2022 WL 93535, at *1 n.2 ("A seemingly straightforward issue—does the private search doctrine apply here—presents tough constitutional questions that circuit and district courts have answered differently.") (comparing *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021) and *Ackerman*, 831 F.3d at 1292 with *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020) and *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018)).

[22] To prevent the possible piecemeal litigation on the *Franks* issue, I received evidence at the hearing regarding the veracity of the challenged averments contained in Detective Keller's affidavits.

from a warrant affidavit if the "inclusion of the omitted facts would have prevented a finding of probable cause." *United States. v. Lebowitz*, 676 F.3d 1000, 1010 (11th Cir. 2012) (per curiam) (quoting *United States v. Kapordelis*, 569 F.3d 1291, 1309 (11th Cir. 2009)). A defendant must satisfy both of the prongs of the *Franks* analysis to be entitled to an evidentiary hearing. *United States v. Arbolaez*, 450 F.3d 1283, 1293 (11th Cir. 2006) (per curiam) (citing *Franks*, 438 U.S. at 155-56).

The substantial preliminary showing required by the first part of the *Franks* test "is not lightly met." *Id.* at 1294. As the Eleventh Circuit has explained:

> To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained.

Id. (quoting *Williams v. Brown*, 609 F.2d 216, 219 (5th Cir. 1979)).

If such a showing is made, a trial court must proceed to the second part of the *Franks* analysis and decide if probable cause still exists once "those portions of the affidavit which the defendant has shown are arguably false or misleading" are excised. *Kapordelis*, 569 F.3d at 1309 (citing *Franks*, 438 U.S. at 171-72). If probable cause does remain, there is no *Franks* violation and no need for a hearing. *United States v. Capers*, 708 F.3d 1286, 1296 (11th Cir. 2013) (citation omitted); *Lebowitz*, 676 F.3d at 1010–11.

If a defendant makes the requisite showing under *Franks* to secure a hearing, he must then prove an allegation of perjury or reckless disregard at the hearing by a preponderance of the evidence. *United States v. Barsoum*, 763 F.3d 1321, 1328 (11th Cir. 2014). Where a defendant meets this burden, the search warrant must be voided if, "with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause." *Franks*, 438 U.S. at 156. Under such circumstances, the fruits of the search are subject to exclusion to the same extent as if probable cause was lacking on the face of the affidavit. *Id.*

Here, Mr. Williamson posits three arguments in support of his *Franks* challenge. First, he claims Detective Keller omitted from the residential warrant affidavit the fact that one of the photographs—image 1-1.jpg—was sent on September 8, 2020, which was after the last log-in date listed in the activity logs for Mr. Williamson's email account and which "would [thus] call . . . into question" whether the image was really transmitted from that account. (Docs. 44, 106). Second, Mr. Williamson asserts Detective Keller misrepresented at one point in both of his affidavits that there were seven CSAM images uploaded by the user of Mr. Williamson's email account even though Detective Keller later found only four of the photographs met the statutory definition for CSAM. *Id.* And third, Detective Keller misstated in the residential affidavit that NCMEC classified three of the files as child pornography when NCMEC actually designated those images as "CP (unconfirmed)." *Id.* These contentions do not amount to the substantial preliminary showing required under *Franks* and certainly

do not undermine the validity of the warrants for Mr. Williamson's Yahoo email account and his home.

Beginning with the first argument, Mr. Williamson does not make the necessary initial showing, much less prove by a preponderance, that Detective Keller intentionally or recklessly omitted the challenged log-in date from his residential affidavit. I note as an initial matter that Detective Keller made clear in his affidavit that, according to the log-in data he received from Yahoo, "[September 5, 2020,] was the last time the [user] logged into his Yahoo email before the reported incident occurred on [September 8, 2020,]" which is the date that the child pornographic image referred to herein as image.1-1.jpeg was transmitted. Gov't Exh. 2; Def. Exh. B. Further, Detective Keller testified at the hearing that the fact the last log-in date on Mr. Williamson's email account was September 5, 2020, three days prior to the transmission of image.1-1.jpeg, "[h]a[d] no bearing" on the probable cause showing because he knows "[f]rom [his] training and experience, [including] dealing with many CyberTips," that users "can stay logged into [their] accounts for a significant period of time." (Doc. 99 at 164–66); *see also id.* at 186–88. This testimony was credible and consistent with the testimony tendered by Ms. Guizzotti, who stated that although "Yahoo [e]mail users must be logged into an account to send email messages," they can remain logged into Yahoo for a "couple of weeks." *Id.* at 88–90; *see also id.* at 89 ("[The] time stamp value in Yahoo's [activity logs] corresponds to the date and time when the user either logged in the reported account or extended a previous log-in session. By logging in or by extending a log in session, the user would remain logged

into the Yahoo account on the same device for a period of two weeks."). Mr. Williamson does not offer any sworn affidavits or other reliable witness statements to refute this evidence. *Franks*, 438 U.S. at 171 (noting that "[a]ffidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained" by a defendant seeking a *Franks* hearing); *see also Arbolaez*, 450 F.3d at 1294 ("There is no affidavit or otherwise sworn statement alleging that [the affiant] knowingly or recklessly included false statements in the search warrant affidavit. Accordingly, we find that [the defendant] has failed to make the necessary 'substantial preliminary showing' and that there is no error.").

Mr. Williamson's suggestion that Detective Keller should have investigated "how or when Yahoo logs out accounts" (Doc. 106 at 41) is likewise deficient. Ms. Guizzotti credibly testified that Yahoo is not able "to track when an account is either manually or automatically logged out" and that no such data exists. (Doc. 99 at 128). Mr. Williamson makes no offer of proof to rebut these sworn attestations either.

I am similarly unpersuaded by Mr. Williamson's second and third contentions concerning Detective Keller's misstatements in both of his affidavits that all seven images constituted CSAM and that, in the residential affidavit, NCMEC designated three of the images as "child pornography" instead of "CP (unconfirmed)." The operative inquiry is not, as Mr. Williamson seems to intimate, whether Detective Keller's affidavits contained errors—they do—but whether the errors were made intentionally or in reckless disregard of the truth. *United States v. Sims*, 845 F.2d 1564, 1571 (11th Cir. 1988) (finding that it is not enough to show that statements in an

affidavit were wrong under *Franks*, a defendant must establish that the affiant knowingly or recklessly included such falsities and/or material omissions) (citing *Franks*, 438 U.S. at 171–72); *see also United States v. Flowers*, 531 F. App'x 975, 981 (11th Cir. 2013) (per curiam) ("*Franks* requires the defendant to offer proof that the affiant had the requisite intent.") (citing *Franks*, 438 U.S. at 171).

With this principle in mind, the problem with Mr. Williamson's arguments is that they fail to take into account the entirety of Detective Keller's averments and to view them in a common sense and realistic manner. *United States v. Joyce*, 2012 WL 7148366, at *2 (S.D. Fla. Dec. 12, 2012) (emphasizing that courts must "utilize common sense" when reviewing search warrant affidavits and must read them "in a realistic and non-technical manner" that takes into account the "affidavit as a whole"), *report and recommendation adopted*, 2013 WL 560817 (S.D. Fla. Feb. 13, 2013). Most importantly, Mr. Williamson downplays, if not ignores, the fact that immediately following these generalized misstatements made by Detective Keller, he described the seven images—often graphically—and expressly stated that, based upon his training and experience, only four actually met the statutory definition for child pornography, while the other three did not. As the government aptly observes in its submission, by setting forth such a particularized accounting of the contents of the child pornographic images, Detective Keller "provided the necessary information to allow [the] court to make a [probable cause] determination[,]" and his "detailed descriptions negated any potential confusion or error caused by [his] initial misclassification" and misstatements about the photographs. (Doc. 105 at 17).

In light of these additional qualifying attestations made by Detective Keller, it is difficult to afford much credence to Mr. Williamson's assertion that Detective Keller's mistakes were the result of any malfeasance. The fact that Mr. Williamson does not meaningfully aver, much less prove—whether through a declaration from a CSAM expert or some other equally weighty evidence—that Detective Keller's descriptions and classifications of the images were false buttresses this conclusion.

Detective Keller's testimony regarding the matter of NCMEC's classifications likewise undermines Mr. Williamson's contentions. At the hearing, Detective Keller advised that he did not place much importance on NCMEC's labels like "CP (unconfirmed)," viewing them instead to be "suggestion[s]" and believing the ultimate decision on the age of a minor, for example, to rest with him. (Doc. 99 at 162, 170–71, 184). Indeed, he testified that he typically does not incorporate NCMEC's designations in his affidavits at all, as was the case with the Yahoo warrant. *Id.* at 168–69, 189–90. Detective Keller's perspective on this issue was bolstered by Ms. Newman, who—as referenced previously—testified that NCMEC "rel[ies] on law enforcement to do their [own] independent review[,] investigation[,] and assessment of" suspected CSAM files and that NCMEC is "not the determiner[ ] of what is illegal or legal content." *Id.* at 26. While Detective Keller later found out his understanding of NCMEC's "CP (unconfirmed)" classification was wrong (as he candidly admitted under oath), my evaluation of his overall testimony and the other evidence of record does not support Mr. Williamson's claim that this misunderstanding by Detective Keller was intentional or the product of recklessness.

One other item in the record bears this out. In NCMEC's CyberTipline report forwarded to the NPPD, NCMEC labeled one of the images—image.118-1.jpeg—as "apparent child pornography." Gov't Exh. 1; Def. Exh. A. This meant that, as Ms. Newman attested, NCMEC concluded the photograph met the federal definition of child pornography and that it was "overtly clear" a child was involved in the sexual activity depicted in the file. (Doc. 99 at 66). Yet, in his affidavit, Detective Keller deemed this image to be "age difficult" and thus—in his view—having little, if any, probative value to the probable cause determination. *Id.* at 184. Stated differently, Detective Keller rejected NCMEC's designation of a photograph that would have further supported his warrant application in favor of assigning his own label that detracted from it.

In addition to failing to make the necessary showing on the first prong of the *Franks* analysis, Mr. Williamson does not meet his burden as to the second prong. *Lebowitz*, 676 F.3d at 1010 (stating "[a] defendant bears the burden of demonstrating" at "the second step" of the *Franks* analysis that had the affiant excluded the misrepresentations or included the alleged omissions, it "would have prevented a finding of probable cause"). Even were the Court to correct the affidavits to account for the omitted log-in information, Detective Keller's misstatement about the seven images constituting CSAM, and his mischaracterizations of certain of the NCMEC labels, the affidavits would still contain ample probable cause. In short, they establish that a detective well-versed in the contours of CSAM personally viewed seven images extracted from an email account tied to Mr. Williamson's residence, found a number

of them to constitute child pornography, and then detailed the contents of those photographs for the reviewing judge to make his or her own determination. (Doc. 99 at 160–63). As Mr. Williamson conceded at the July 2022 oral argument, one such image would have been sufficient to demonstrate probable cause.

D.

In conjunction with the above determinations, I also find the warrant to be valid under the good faith exception. Generally, evidence seized in violation of the Fourth Amendment is subject to suppression under the exclusionary rule, the purpose of which is "to deter future unlawful police conduct." *United States v. Calandra*, 414 U.S. 338, 347 (1974). The Supreme Court recognized in *United States v. Leon*, however, that "where the officer's conduct is objectively reasonable, excluding the evidence will not further the ends of the exclusionary rule in any appreciable way. . . ." 468 U.S. 897, 918 (1984) (internal citation omitted). As a result, the *Leon* Court concluded that where an officer has relied on a warrant in an objectively reasonable manner, the evidence obtained, even though the warrant is found to be defective, will not be excluded. *Id.*

In light of *Leon*, an officer's reliance on a warrant will not qualify as "objectively reasonable" only in situations where (1) probable cause is based on statements in an affidavit that are knowingly or recklessly false; (2) the reviewing judge fails to perform a neutral and detached function and instead merely "rubber stamps" the warrant; (3) the affidavit is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; or (4) the warrant was so facially deficient that the

executing officer could not reasonably have assumed it was valid. *Id.* at 914–15. The government bears the burden of demonstrating that none of these circumstances exist in cases where it seeks to rely on *Leon*. *United States v. Morales*, 987 F.3d 966, 974 (11th Cir. 2021).

The government has met its burden here. It is evident from his submission that Mr. Williamson only seeks to avail himself of the first circumstance described above. Yet I have already been found that Detective Keller did not make any intentional or reckless omissions or misrepresentations. Thus, the good faith exception under *Leon* applies.

III.

In light of the foregoing, I respectfully recommend that Mr. Williamson's motion to suppress (Doc. 44) be denied.

Respectfully submitted this 10th day of February 2023.

HONORABLE CHRISTOPHER P. TUITE
United States Magistrate Judge

NOTICE TO PARTIES

A party has fourteen (14) days from this date to file written objections to the Report and Recommendation's factual findings and legal conclusions. A party's failure to file written objections, or to move for an extension of time to do so, waives

that party's right to challenge on appeal any unobjected-to factual finding(s) or legal conclusion(s) the District Judge adopts from the Report and Recommendation. *See* 11th Cir. R. 3-1; 28 U.S.C. § 636(b)(1).

Copies to:
Honorable William F. Jung, United States District Judge
Counsel of record