

Appendix C: The District Court's Opinion Below (Doc. 173)

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 second motion to suppress evidence seized from his Oath Holdings, Inc. d/b/a Yahoo! (Yahoo) email account pursuant to a search warrant authored by North Port Police Department (NPPD) Detective James Keller. (Doc. 134).¹ Detective Keller obtained this warrant following his review of suspected child pornographic images that Yahoo found in Mr. Williamson's email account. (Docs. 114, 144, 145). Detective Keller learned of these images after Yahoo transmitted them to the National Center for Missing and Exploited Children (NCMEC), which then forwarded them to Detective Keller. *Id.*

In support of his motion, Mr. Williamson argues that Detective Keller's warrant violated the Fourth Amendment's particularity requirement because it was not properly limited in time or scope, and that the warrant cannot be saved by the good

¹ Mr. Williamson's first suppression motion was denied following an evidentiary hearing. (Docs. 114, 144, 145).

faith exception enunciated by the Supreme Court in *United States v. Leon*, 468 U.S. 897 (1984). (Doc. 134). The government opposes Mr. Williamson's motion. (Doc. 138).

I heard oral argument on the matter, after which the parties filed supplemental submissions addressing the issue of severability. (Docs. 169, 171). Based upon my review of the parties' filings and other pertinent portions of the record, I respectfully recommend that Mr. Williamson's second suppression motion be denied.

I.

The background of this case is set forth in detail in a prior Order of the Court (Docs. 114, 144, 145) and therefore need only be summarized here with some supplementation. Yahoo is a private corporation that offers email services to its customers, among other products. (Doc. 114 at 3). NCMEC is a not-for-profit organization that Congress has tasked with operating a CyberTipline. *Id.* 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 like Yahoo. *Id.*

On September 8, 2020, Yahoo learned that an email sent from the email account "vladlover50@gmail.com"² included an image³ believed to constitute child sexual abuse material (CSAM). *Id.* at 8. Upon further investigation, Yahoo discovered that the vladlover50 account contained a total of seven CSAM photographs. *Id.* Two days

² The vladlover50 email account will be referred to herein as the vladlover50 account.

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

later, on September 10, 2020, Yahoo submitted a CyberTipline report to NCMEC relative to these files, and disabled the vladlover50 account in the process. *Id.* Yahoo also included in its report the name, phone number, email address, and IP address associated with the vladlover50 account, as well as the upload date and time for each of the seven images.⁴ *Id.* at 9.

After receiving Yahoo's submission, NCMEC compiled its own report in which it classified two of the files as apparent child pornography, four of the files as "CP (unconfirmed)" (i.e., unconfirmed child pornography), and one of the files as "child clothed." *Id.* at 9–10. NCMEC additionally determined that the geolocation of the IP address for the vladlover50 account was situated in North Port, Florida. *Id.* at 10. As a result of this information, NCMEC's report was provided to the NPPD, where it was assigned to Detective Keller in mid-November 2020. *Id.*

By that point in his career, Detective Keller had been with NPPD for approximately eight years and had been charged with investigating sex crimes for over a year-and-a-half. *Id.* During the latter time frame, Detective Keller was a member of both the Central Florida Internet Crimes Against Children Task Force (CFICAC)⁵ and the FBI's Child Exploitation and Human Trafficking Task Force, and had attended multiple training sessions regarding the investigation and identification of CSAM. *Id.* at 10–11.

⁴ According to the report, the CSAM images were uploaded between November 8, 2019, and September 8, 2020. (Doc. 114 at 9 n.8).

⁵ CFICAC is a subdivision of a national task force—ICAC—that is headed by the Federal Bureau of Investigation (FBI). (Doc. 114 at 10 n.11).

After reviewing NCMEC's CyberTipline report, Detective Keller determined that the user of the vladlover50 account uploaded multiple files containing CSAM. *Id.* at 11–12. Detective Keller then 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 of S.B. residing at 2575 Rolling Road in North Port, Florida.⁶ *Id.* at 11; (Doc. 134-1 at 5). Based upon this information, Detective Keller applied to a state court judge on December 10, 2020, for a search warrant directed to Yahoo for the vladlover50 account.⁷ (Doc. 134-1 at 10). In his warrant application, Detective Keller sought the seizure of several defined categories of data which either constituted evidence or contraband of possession of child pornography in violation of Florida Statute § 827.071(5), or which was used in the commission of that offense. *Id.* at 8–9; *see also id.* at 11–12. These categories were as follows:

1. Account Information—User name, primary email address, secondary email addresses, connected applications and sites, and account

⁶ In a later warrant to search this North Port residence, Detective Keller stated that the initials of the individual at that address were A.W. (Doc. 114 at 11). I refer to those initials here as “S.B.” because that is how Detective Keller described them in his Yahoo warrant. (Doc. 134-1).

⁷ The Court's decision resolving Mr. Williamson's first suppression motion indicated that the vladlover50 warrant was submitted and signed on December 1, 2020. (Doc. 114 at 11). The Court derived this date from the warrant that was admitted into evidence at the evidentiary hearing on the first suppression motion. *Id.* (citing Def. Exh. C). It now appears, however, that this warrant was the first of two warrants Detective Keller requested for the vladlover50 account. It seems that the first warrant incorrectly listed the target email address as “vladlover5@yahoo.com” (Doc. 134 at 2 n.1), and that after Yahoo informed Detective Keller of this error, he submitted the second warrant (which is the one I rely upon here) with the correct email address. *Id.* These facts do not appear to be contested by the parties.

activity from creation to 11/24/20, including account sign in locations, browser information, platform information, and [IP] addresses;

2. Evidence of user attribution—accounts, [e]mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s);

3. Calendar—All calendars, including shared calendars and the identities of those with whom they are shared, from creation to 11/24/20, calendar entries, notes, alerts, invites, and invitees;

4. Contacts—All contacts stored by Yahoo[] . . . including name, all contact phone numbers, emails, social network links, and images;

5. Yahoo[] Email—All email messages from [insert date] to [insert date], including by way of example and not limitation . . . inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information[,] such as the date, time, [IP] address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the ‘cc’ (carbon copy) or the ‘bcc’ (blind carbon copy), the message content or body, and all attached files;

6. Photos—All images, graphic files, video files, and other media files stored by Yahoo[] . . . associated with the listed account; [and]

7. Search History—All search history and queries from creation to 11/24/20, including by way of example and not limitation, . . . World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance[.]

Id. at 8–9.

In support of his request to obtain this information, Detective Keller set forth a detailed description of the contents of each of the above seven images tied to the vladlover50 account and attested that he personally reviewed these photographs. *Id.* at 4–5. Relying on Florida’s definition of CSAM and his own training and experience, Detective Keller also stated that he deemed four of these files to be CSAM involving prepubescent and minor females; two of the files to be “age difficult” (i.e., it was difficult for Detective Keller to discern the approximate ages of the subjects in the images); and the remaining file to be child erotica. *Id.*

As pertinent here, Detective Keller additionally referenced the need to identify the user of the vladlover50 account and explained that this objective necessitated that the scope of the warrant, including the time frame, be more expansive. Specifically, he advised:

Yahoo[] . . . may not verify the true identity of an account creator, account user or any other person who accesses a user’s account using login credentials. For these reason[s,] *it is necessary to examine particularly unique identifying information that can be used to attribute the account data to a certain user.* This is often accomplished by analyzing associated account data, usage, and activity through communication, connected devices, locations, associates, and other accounts. For these reasons[,], it may be necessary to search and analyze data from *when the Yahoo[] . . . account was initially created to the most current activity.*

Id. at 6 (emphasis added).

As an example of the type of identifying information he sought, Detective Keller further advised:

Yahoo[] maintains information about their customers[,] including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Yahoo[] . . . account or use the user's Yahoo[] . . . account as a password login, and account login activity[,] such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the [IP] address they logged in from. . . . *The IP can be resolved back to a physical address[,] such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers.*

Id. (emphasis added).

Along with the above identifying information, Detective Keller articulated the basis for seizing the other requested data as well. *Id.* at 6–8. Detective Keller explained, *inter alia*, that this additional information could likewise be used to tie the vladlover50 account to the suspect, witnesses, associates, and victims, and could constitute evidence or contraband of the crime itself. *Id.* For instance, as to the sought-after calendar entries, contacts, email messages, photos, videos, and search history for the vladlover50 account, Detective Keller stated: (a) Yahoo's calendar feature, which "allows users to schedule events" and which "may include dates, times, notes[,] and descriptions," could assist law enforcement in identifying the user's co-conspirators and/or witnesses, as well as potentially "corroborative evidence;" (b) the user's contacts, including names, phone numbers, and email addresses, could also help law enforcement ascertain the names of co-conspirators and witnesses; (c) the user's email messages, whether read, unread, sent, saved, or placed in a trash folder, could similarly

reveal the identities, motives, and plans of associates and co-conspirators; (d) the user's photos and videos could "depict[] the suspect, his/her associates[,] and others performing incriminating acts, and victims," as well as further facilitate the discovery of residences and other "geographic locations" relevant to the investigation; and (e) the user's search history and queries, including "specialty searches where the results" focus on a "particular group," could equally reveal information pertinent to the investigation. *Id.*

Detective Keller's warrant contemplated that it be executed in two steps. *Id.* at 5, 8, 11–12. The first step required Yahoo to provide him with all the records for the vladlover50 account, while the second step involved Detective Keller searching those records and seizing only that information covered by one or more of the above seven categories. *Id.*

The state court judge authorized the warrant on December 11, 2020. *Id.* at 13. In response to the warrant, Yahoo produced the images that it sent to NCMEC as part of its CyberTipline report and other items. (Doc. 134 at 14 n.5).

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."⁸ U.S. Const. amend. IV. A search warrant must therefore "particularly

⁸ The Court has already determined that Mr. Williamson has standing to challenge a search of the vladlover50 email account. (Docs. 114, 144, 145).

describ[e] the place to be searched, and the persons or things to be seized.’” *United States v. Alford*, 744 F. App’x 650, 652 (11th Cir. 2018) (per curiam) (quoting U.S. Const. amend IV) (alteration in original). “The ‘specific evil’ [this] 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 v. New Hampshire*, 403 U.S. 443, 467 (1971)). Such rummaging was allowed in the colonial era by the “general warrant,” which was “an instrument ‘abhorred by the colonists.’” *Id.* (quoting *Coolidge*, 403 U.S. at 467).

While recognizing the importance of the particularity requirement, the Eleventh Circuit has instructed that it should be applied with “a practical margin of flexibility” and that warrants need only be as “specific as the circumstances and nature of the activity under investigation permit[].” *Alford*, 744 F. App’x at 653 (citing *United States v. Bradley*, 644 F.3d 1213, 1259 (11th Cir. 2011); *United States v. Moody*, 977 F.2d 1425, 1432 (11th Cir. 1992)). Put another way, a search warrant will survive a particularity challenge under governing Eleventh Circuit precedent if it sufficiently connects the items to be searched and seized to the crime(s) under investigation. *United States v. Wheat*, 2022 WL 16851663, at *7 (N.D. Ga. Nov. 10, 2022) (citing *Blake*, 868 F.3d at 973).

Here, Mr. Williamson asserts that Detective Keller’s warrant for the vladlover50 account was constitutionally infirm because the nature of the data it sought was “virtually unlimited,” and because it also did not have a meaningful temporal restriction. (Docs. 134, 171). To buttress this contention, Mr. Williamson

relies on the Eleventh Circuit's decision in *Blake*, among other case authority. *Id.* The government counters that Detective Keller's warrant was not impermissibly overbroad and—in addition to distinguishing *Blake*—cites the Eleventh Circuit's opinion in *Alford* to bolster its position. (Docs. 138, 169).

In *Blake*, the defendants—Dontavious Blake and Tara Jo Moore—were convicted after a trial of various sex trafficking-related offenses that stemmed from their management of a prostitution ring involving underage girls. 868 F.3d at 966. During the course of its investigation of this ring, the FBI discovered that the defendants were using a specific email address belonging to Ms. Moore (the S.B. email address) to post ads on a classified website known as Backpage.com. *Id.* The FBI subsequently arrested Mr. Blake and Ms. Moore and, of relevance here, served a search warrant on Microsoft and two on Facebook pertaining to the defendants. *Id.* The Microsoft warrant had no temporal limitation but was confined to certain categories of emails from two of the defendants' email accounts (including the S.B. email account) that were linked to the sex trafficking crimes. *Id.*

The Facebook warrants, on the other hand, sought “virtually every type of data that could be located in a Facebook account.” *Id.* at 966. By way of example, the warrants requested that Facebook disclose:

[E]very private instant message [Ms.] Moore had ever sent or received, every IP address she had ever logged in from, every photograph she had ever uploaded or been “tagged” in, every private or public group she had ever been a member of, every search on the website she had ever conducted, and every purchase she had ever made through “Facebook Marketplace,” as well as her entire contact list.

Id. at 966–67.

The Facebook warrants asked for this wide swath of information even though the FBI already knew the Facebook account was Ms. Moore’s because it was associated with both her S.B. email address and her phone number. *Id.* at 966. The warrants also were not confined to the time frame in which Ms. Moore managed the prostitution ring and instead were essentially unbounded temporally. *Id.* at 967. The potential saving grace was that the Facebook warrants required a second step that restricted law enforcement to seizing only data “constitut[ing] fruits, evidence[,] and instrumentalities” of sex trafficking. *Id.*

In response to Ms. Moore’s argument that the Microsoft and Facebook warrants violated the Fourth Amendment’s particularity requirement, the Eleventh Circuit found that the Microsoft warrant was “appropriately limited in scope because it sought only discrete categories of emails that were connected to the alleged crimes.” *Id.* at 973, 973 n.7. As a result, the court determined that the absence of a time delimiter alone did not render the warrant unconstitutional. *Id.*

The court, however, criticized the breadth of the Facebook warrants, stating that they “unnecessarily” called for the disclosure of nearly “every kind of data that could be found in a social media account.” *Id.* at 974 (citation omitted). Relative to the sought-after instant messages, for example, the court noted that the warrants could have cabined this “request to messages sent to or from persons suspected at that time of being prostitutes or customers” and to “data only from the period of time during

which [Ms.] Moore was suspected of taking part in the prostitution conspiracy.” *Id.* The court commented that such restrictions “would have undermined any claim that the Facebook warrants were the internet-era version of a ‘general warrant.’” *Id.* (citing *Coolidge*, 403 U.S. at 467; *Riley v. California*, 134 S. Ct. 2473, 2488–91 (2014)).

The court was skeptical that the cases relied upon by the government—which involved a two-step search process whereby hard drives seized in a defendant’s home were later searched at the government’s offices—could be applied to the Facebook warrants. *Id.* (citations omitted). The court pointed out that hard drive searches entail “time-consuming electronic forensic investigation with special equipment” and that conducting such a “search in the defendant’s home would be impractical, if not impossible.” *Id.* By contrast, the court stated that “when it comes to Facebook account searches, the government need only send a request with the specific data sought and Facebook will respond with precisely that data.” *Id.* (citation omitted). The court added that it did not appear this one-step procedure would have been “impractical for Facebook or for the government” to utilize in the case given the record before it. *Id.* (citation omitted).

Despite these criticisms, the court declined to resolve the issue of whether the Facebook warrants were insufficiently particularized for purposes of the Fourth Amendment. *Id.* Instead, relying on *Leon*, it held that even if the warrants were impermissibly overbroad, the “district court did not err in allowing the government to use evidence gathered as a result of them.” *Id.* (citing *United States v. Herring*, 492 F.3d 1212, 1215 (11th Cir. 2007)).

In *Alford*, which was decided almost a year after *Blake*, the defendant challenged his conviction for the receipt of child pornography on, among other grounds, that a search warrant issued to Google during the investigation was not adequately particularized. *Alford*, 744 F. App'x at 652–53. This Google warrant apparently related to a nighttime phone call in September 2014 from an anonymous Google Voice phone number to a K-Mart in Hamilton, Montana, in which the caller claimed his daughter was being victimized. *Id.* The warrant directed Google to provide:

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

Id. at 652 (alteration in original) (emphasis added).

Following a review of its decision in *Blake*, the Eleventh Circuit in *Alford* characterized the Google warrant as “fall[ing] somewhere between the Microsoft and Facebook warrants in *Blake*.” *Id.* at 652–53. It stated that “like the Facebook warrants, [the Google warrant] 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.* Employing a “practical margin of flexibility,” the court ruled that notwithstanding the breadth of the Google warrant, it was “as specific as the circumstances and nature of

the activity under investigation permitted.” *Id.* (citing *Blake*, 868 F.3d at 973–74; *Bradley*, 644 F.3d at 1259; *Moody*, 977 F.2d at 1432). To support this finding, the court emphasized that the applicant seeking the warrant “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 [the] potential victim” and that “*all* of the evidence seized” could have helped law enforcement ascertain who owned the Google account. *Id.* (citing *Blake*, 868 F.3d at 973) (emphasis added). The *Alford* court also ruled that the Google warrant fell within the ambit of *Leon*’s good faith exception in any event. *Id.* at 653–54 (citing *Blake*, 868 F.3d at 975).

Applying the teachings of *Blake* and *Alford* here, Detective Keller’s vladlover50 warrant appears to be adequately particularized. I begin by noting that although 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. (Doc. 134-1 at 5, 8, 11–12). This materially differentiates Detective Keller’s warrant from the Facebook warrants at issue in *Blake*. Detective Keller’s warrant is further unlike the Facebook warrants in *Blake*, insofar as he explicitly explained it was necessary to employ the bifurcated search protocol he proposed because Yahoo had “no reasonable means to distinguish evidence of the crimes from other records contained within the [vladlover50] account.” *Id.* at 5.

Detective Keller's warrant also bears a number of similarities to the Google warrant in *Alford*. Akin to the Google warrant, for example, much, if not virtually all, of the data requested in Detective Keller's warrant arguably pertained to the identity of the user of the vladlover50 account. *Id.* at 6–9, 11–12. This is evident by the fact that the information Detective Keller referenced in the “user attribution” category in his warrant included many of the items he listed elsewhere in the warrant. *Id.* at 8–9, 12.

It bears highlighting in this respect that, in contrast to *Blake* where the Facebook warrants were executed towards the end of the investigation after law enforcement had already developed “extensive evidence” against the account holder, Ms. Moore, *Blake*, 868 F.3d at 966, Detective Keller's investigation directed at the user of the vladlover50 account was still in its relative infancy at the time the Yahoo warrant was sought (Doc. 134-1 at 4–5). The record before the Court indicates, for example, that law enforcement did not know a great deal about the user of the vladlover50 account at that juncture, clearly not enough to prove a case against him. *See id.* Nor was much apparently known about the associate(s) or victim(s) affiliated with the emails containing the CSAM that Yahoo discovered during its review of the vladlover50 account. *See id.* As discussed previously, the vast majority of the data requested by Detective Keller in the Yahoo warrant was potentially relevant to these issues. Notably, a number of the types of information Detective Keller asked for in the vladlover50 warrant—like user names, IP addresses, email addresses, photos, videos, email content, and search history—were deemed by the Eleventh Circuit in *Alford* to

be pertinent to the issue of the target's identity in that case. *Alford*, 744 F. App'x at 652.

Besides the data bearing on the identity of the vladlover50's account user, a fair portion of the sought-after information in Detective Keller's warrant also constituted possible evidence of the account user's possession of child pornography, particularly since—as Detective Keller articulated in his affidavit—the user of this account had emailed CSAM to other(s) in the past. (Doc. 134-1 at 4–5). The information that fell into this grouping consisted of, *inter alia*, records and data linking the user of the vladlover50 account to CSAM, photos or videos containing CSAM, emails and other communications containing or relating to CSAM, and third parties who sent CSAM to or received CSAM from the vladlover50 account user. As Detective Keller stated in his affidavit:

[Your affiant knows t]hrough [his] experience and training . . . that Yahoo[] . . . stores files for their subscribers. *These files can be stored as an attachment in an email which was either received, sent, or attempted to be sent in the past, or have been saved.* An analysis of these saved files is necessary to the investigating officers in order to further establish evidence of the crime.

Id. at 6 (emphasis added).

In light of the above averments, there was at least a “fair probability” that the type of evidence, contraband, and/or instrumentalities of possession of child pornography detailed by Detective Keller in his warrant would be found in the vladlover50 account at the time the warrant was issued. *United States v. Orr*, 819 F. App'x 756, 765 (11th Cir. 2020) (per curiam) (“Although the government did not

attach photographs or describe specific pornographic images officers expected to find at the apartment, there is no requirement that it do so given the other details provided in the affidavit. Probable cause for child pornography offenses does not depend on law enforcement having proof that child pornography is in the defendant's possession.") (citing *United States v. Williams*, 444 F.3d 1286, 1304 n.87 (11th Cir. 2006)).

The fact that Detective Keller's warrant did not have a temporal limitation does not render it invalid. The warrant in *Alford* also did not have such a restriction. 744 F. App'x at 652. And here, as discussed earlier, Detective Keller made clear that because "Yahoo may not verify the true identity of an account creator, account user[,] or any other person who accesses a user's account[,] it is often necessary to analyze "associated account data, usage, and activity through communication, connective devices, locations, associates, and other accounts" from when the target "account *was initially created to the most current activity.*" (Doc. 134-1 at 6) (emphasis added). These attestations further evidence that Detective Keller's warrant for the vladlover50 account was as "specific as the circumstances and nature of the activity under investigation permitted." *Alford*, 744 F. App'x at 653 (citation omitted).

In short, applying "a practical margin of flexibility," *id.*, the vladlover50 warrant properly connected the items to be searched and seized to the possession of child pornography offense under investigation, *Wheat*, 2022 WL 16851663, at *7; *United States v. Montgomery*, 2022 WL 3582814, at *4-5 (M.D. Ga. Aug. 19, 2022) (upholding

a warrant where the information to be seized was limited to incriminating data even though the scope of the materials Yahoo was required to produce was broader).

That said, I do recognize that—as Mr. Williamson maintains—Detective Keller’s warrant (like most warrants) could have been better drafted. At times, for example, Detective Keller could have used more tailored language to justify the search and seizure of certain information that more neatly fit the circumstances of this case.

But the Fourth Amendment’s particularity requirement does not demand that a warrant be perfect. *United States v. Martinez-Martinez*, 777 F. App’x 441, 444 (11th Cir. 2019) (per curiam) (stating that the “particularity standard ‘does not necessitate technical perfection’”) (quoting *Bradley*, 644 F.3d at 1259); see also *United States v. Ulbricht*, 858 F.3d 71, 100 (2d Cir. 2017) (“T]he Fourth Amendment does not require a perfect description of the data to be searched and seized,” and “a search warrant does not necessarily lack particularity simply because it is broad.”), *abrogated on other grounds by Carpenter v. United States*, 138 S. Ct. 2206 (2017). Courts must instead look at search warrants as a whole and in a realistic and practical manner, and “should not invalidate [a] . . . warrant by interpreting [the supporting] affidavit in a hypertechnical, rather than a commonsense, manner.” *Illinois v. Gates*, 462 U.S. 213, 236 (1983) (internal quotation marks and citations omitted). This is because affidavits and warrants “are frequently drafted under time pressure, often by police or persons without legal training, and . . . must frequently express complex thoughts.” *Nat’l City Trading Corp. v. United States*, 487 F. Supp. 1332, 1336 (S.D.N.Y. 1980), *aff’d*, 635 F.2d 1020 (2d Cir. 1980). As a result, warrants “cannot properly be subjected to the same

standards of dissection as might befit a criminal statute, an indictment, or a trust indenture.” *Id.* Mr. Williamson’s critique of Detective Keller’s warrant, pursued with the benefit of hindsight, seemingly exceeds the standard to which the Court must hold the warrant in this case.

The Court, however, need not decide whether the vladlover50 warrant contravened the Fourth Amendment’s particularity requirement because, even if it did, it falls squarely within the good faith exception to the exclusionary rule established in *Leon*. As the Court observed in its earlier Order (Doc. 114), the Supreme Court held in *Leon* that where an officer relies on a subsequently invalidated warrant in an objectively reasonable manner, the evidence obtained as a result of the warrant should generally not be excluded. *Leon*, 468 U.S. at 897, 918. The Supreme Court also identified four instances in *Leon* where this exception would not apply, including—of relevance here—where the challenged warrant was “so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers c[ould not have] reasonably presume[d] it to be valid.” *Id.* at 923.⁹ In the end, the government bears the burden of demonstrating that the *Leon* good faith exception applies. *United States v. Morales*, 987 F.3d 966, 974 (11th Cir. 2021).

⁹ The Supreme Court in *Leon* additionally held that the government cannot rely on the good faith exception where the affidavit in support of the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable. *Leon*, 468 U.S. at 914–15. While Mr. Williamson originally contended in his instant suppression motion that the vladlover50 warrant was devoid of probable cause and thus not protected by *Leon* (Doc. 134), he conceded at oral argument that this assertion is foreclosed by the Court’s ruling on his first suppression motion, which was issued after he filed this second motion (Docs. 114, 144, 145).

the warrant's fruits from suppression" because, "although there was no temporal limitation and the warrant authorized the [g]overnment to obtain all records from the email accounts, the warrant limited the [g]overnment to seizing records that evidenced the crimes under investigation"), *report and recommendation adopted*, 2019 WL 397991 (N.D. Ga. Jan. 31, 2019).

The other cases upon which Mr. Williamson principally relies (Docs. 134, 162)—*United States v. Mercery*, 591 F. Supp. 3d 1369 (M.D. Ga. 2022), *United States v. Irving*, 347 F. Supp. 3d 615 (D. Kan. 2018), and *United States v. Shah*, 2015 WL 72118 (E.D.N.C. Jan. 6, 2015)—do not dictate a different result. All of these decisions were issued by courts outside of this District and are not binding on the Court. Furthermore, they also involved facts and circumstances far different from those present in this action.

In *Mercery*, the court determined that a warrant for an Instagram account contravened the particularity requirement because it was "not tailored to evidence of the crimes under investigation, the time period during which [the defendant] allegedly committed the crimes, or the persons allegedly involved in the crimes." 591 F. Supp. 3d at 1381. Indeed, not only did the court deem the Instagram warrant to be "unnecessarily overbroad," it noted that the warrant was "even [more expansive] than the warrants described in *Blake*," with "absolutely no limitation" on what data law enforcement could seize after Instagram's wide-ranging disclosures that encompassed "eighteen broad categories of information." *Id.* In light of these infirmities, the court

in *Mercery* concluded that the warrant could not be saved by *Leon*'s good faith exception. *Id.* at 1382–83.

In *Irving*, the court found that a warrant for a Facebook account was overbroad because even though the offense under investigation only involved a registered sex offender's alleged failure to register his Facebook account, the warrant was "not defined and limited by that crime" at all. 347 F. Supp. 3d at 624. In fact, the warrant authorized "the search and seizure of [the d]efendant's entire Facebook account" with "no set limits." *Id.* Given these deficiencies and the other information before it, the *Irving* court ruled that *Leon* did not apply. *Id.* at 625–26.

In *Shah*, the court decided that a warrant for a Google account was insufficiently particularized because, although it contemplated a two-step process, the second step did not "impose any real limitation" on the breadth of the search. *Shah*, 2015 WL 72118, at *13. The court observed, for instance, that the warrant did not adequately "clarify the particular crime at issue," nor did it "offer[anything] about the time frame of the offense." *Id.* at *14. That said, the court concluded that the warrant fell within *Leon*'s good faith exception. *Id.* at *15–16.

Because Detective Keller's vladlover50 warrant is materially distinguishable from the warrants challenged in *Mercery*, *Irving*, and *Shah*, those cases are of no help to Mr. Williamson in this action. Indeed, the court's finding in *Shah* on the applicability of *Leon* undercuts Mr. Williamson's argument.

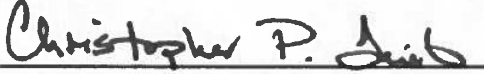
B.

In light of the above findings, the Court need not reach the severability question briefed by the parties in their supplemental submissions. (Docs. 169, 171). Leaving the resolution of that issue for another day appears to be especially appropriate given that, according to the parties' filings, there is no controlling Eleventh Circuit authority on the matter of severability and addressing it could prove quite nettlesome.

III.

Based upon the foregoing, I respectfully recommend that Mr. Williamson's second motion to suppress (Doc. 134) be denied.

Respectfully submitted this 6th day of July 2023.


HONORABLE CHRISTOPHER P. TUIE
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