UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF: ENCRYPTED DATA PROVIDED BY THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN FOR NINETEEN RELATED CYBER TIPLINE REPORTS

Case No. 20-sw-321 (ZMF)

ORDER

In March 2021, the government submitted an Application for a Search Warrant ("Application") to view video files provided to law enforcement by Google. Google's private search revealed that the files were a hash match to known child pornography. For the reasons below, this Court denies the requested Application.

I. BACKGROUND

Providers[1] are not obligated to affirmatively monitor for child pornography. *See* 18 U.S.C. § 2258A(f). However, once a Provider discovers child pornography, it must submit a report "to the CyberTipline operated by [the National Center for Missing and Exploited Children ("NCMEC")]." 18 U.S.C. § 2258A(a)(1)(B). NCMEC then forwards the report to law enforcement. *See* 18 U.S.C. § 2258A(c).

[1] 18 U.S.C. § 2258 defines "provider" as "an electronic communication service provider or remote computing service." 18 U.S.C. § 2258E(6).

A. Google's Voluntary Identification of Child Pornography

"Google's Terms of Service, which a user must accept as part of registering a Google Account," prohibit using their platform to violate the law. *See* ECF No. 2 (Decl.) at 1.[2] Google reserves the right to "take down" content that either violates applicable law or "could harm [] users, third parties, or Google," the prime example of which is "child pornography." *Id.* Google has an avowed "strong business interest in enforcing [its] Terms of Service and ensuring that [its] products are free of illegal content, and in particular, [child pornography].[3] Accordingly, [Google] independently and voluntarily take[s] steps to monitor and safeguard [its] platform." *Id.*

Thus, based on "private, non-government interests, Google has undertaken voluntary efforts to remove and report [child pornography] on a large scale." *Id.* To do this, and consistent with Google's Privacy Policy, Google has employed reviewers and created software to search customer content. *See id.* at 2. The Google reviewers "are trained on the federal statutory definition of child pornography and how to recognize it on [Google's] products and services." *Id.* Google reviewers identify and catalogue child pornography images and videos differently (as described below). *See id.*

[2] Google has submitted a sworn declaration at the request of the court, which details Google's internal policies.

[3] Google uses the more accurate term of "child sexual abuse material" also known as "CSAM." However, this Court describes the offending content as "child pornography" to mirror the statutory definition. 18 U.S.C. § 2256(8).

Google's review is twofold: finding both new and previously identified child pornography. Google finds "never-before-seen [child pornography] imagery" using algorithms, a subject with which the world's most powerful search engine has *some* familiarity, "machine learning," and human review. Kristie Canegallo, *Our efforts to fight child sexual abuse online*, Google: The Keyword (Feb. 24, 2021) available at https://blog.google/technology/safety-security/our-efforts-fight-child-sexual-abuse-online/. Once found, a Google reviewer views the content before it is marked for addition to Google's repository of known child pornography. *See* Decl. at 2. Google finds previously identified child pornography by running automated searches for matches to images and videos in its repository. *See id.* When a match occurs, Google will either automatically send the data to the CyberTipline or in some instances, a Google reviewer will conduct a spot check and re-review the content to confirm its illicit nature. *See id.* In 2020 alone, "Google submitted 547,875 CyberTip reports to NCMEC [including] over 4.4 million pieces of content." *Id.* at 1.

B. Hash Match

Google uses "hash" matches to identify child pornography images and videos. Hash values are "unique digital fingerprints," Canegallo, created by taking "a large amount of data, such as a file or all the bits on a hard drive, and us[ing] a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data," Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38 (2005). The chance of two different files creating the same hash value is "astronomically small." *Id.* at 39. Indeed, the government opines "it can be concluded that two files that share the same hash value are identical with a precision that exceeds 99.9999 percent certainty." ECF No. 1 (Appl.) at 8.

Google's hash-matching system varies slightly between images and videos. *See* Decl. at 1-2. Once a Google reviewer has confirmed that an image depicts child pornography, Google assigns it a hash value. *See* Decl. at 2. Google scans its platform for hash matches to these child pornography images. *Id.*

The process for video identification begins the same, a Google reviewer watches the video "to the extent necessary to confirm" it depicts child pornography. *Id.* at 3. Once identified as such, Google then creates a unique digital "fingerprint" for the video.[4] *Id.* at 2. This "fingerprint" is then added to Google's repository after human review. *Id.* Google automatically searches the repository "us[ing] a technology called CSAI Match, which is a fingerprint matching technology" to detect other such videos on its platform. *Id.* CSAI Match "was the first technology to use hash-matching to identify known [child pornography] videos." *Fighting child sexual abuse online*, Google, available at https://protectingchildren.google/intl/en/. CSAI Match "uses fingerprints that are resistant to manipulation and obfuscation, allowing Google to detect exact matches, matches intermingled with non-offending content, and slightly modified versions of the previously fingerprinted video." Decl. at 2. For example, a child pornography video that Google has fingerprinted will still match with the same video that has been covered by a watermark in an attempt to evade detection. *Id.* at 2–3. In this way, CSAI Match is more sophisticated than a traditional hash-matching search used for images.

[4] "When Google becomes aware of new [child pornography] contained in a video, it may calculate the fingerprint of the portion of the video that contains the [child pornography], possibly including some portion of the video before and after the portion confirmed as apparent [child pornography]." *Id.* at 2.

D. Instant Application

Between October 3 and October 5, 2020, Google submitted several reports to the CyberTipline. *See* Appl. at 10. The reports contained videos a user uploaded to their Google Drive which produced a CSAI Match to child pornography. *See id.* The report stated the files were not manually re-reviewed by Google reviewers concurrent with submission, *see* ECF No. 3 (Suppl. Br.) at 6; however, the files were a match to previously identified child pornography that a Google reviewer would have reviewed, *see id.*; Decl. at 2. After receipt, NCMEC forwarded the files to law enforcement. *See* Suppl. Br. at 6. The government then submitted an Application to this Court to view the files contained in the report. *See* Appl.

Although the government believed a search warrant "should not be necessary," they submitted an application to search the CyberTip reports. *See* Suppl. Br. at 2. To the Court's and the government's knowledge, this was one of the first requests in this District for a warrant to search a CyberTip report. The Court held two hearings to further understand the government's request and the process by which Google identified child pornography. Google attended both hearings through its counsel. Both the government and Google filed supplemental materials.

On March 23, 2021, the Court denied the government's application, even though it "established probable cause" to view the data in question. Minute Order March 23, 2021. The Court relied on its "inherent authority to manage its docket" to make this ruling. Id. (citing *Beale v. Dist. of Columbia*, No. 04-cv-959, 2005 WL 8178299, at *2 (D.D.C. Sept. 30, 2005)). "In the interest of addressing largely-unexplored issues that will certainly arise again, the undersigned takes th[is] opportunity to consider further the request and appropriate vehicles for such authorizations." *In re Use of a Cell-Site Simulator to Locate a Cellular Device Associated with One Cellular Tel. Pursuant to Rule 41*, No. 20-sc-3276, 2021 WL 1133838, at *2, n.4 (D.D.C.

Mar. 25, 2021) (cleaned up). Unnecessary search warrants fall into a self-perpetuating blind spot: a court-approved search largely inoculates the government from a later motion to suppress. The alternative is risky: conducting the review without a warrant and hoping the court will not suppress the fruits when it is later contested. The government will continue to choose the former option and get unnecessary warrants as insurance. But in so doing, evasion of review looms as no court will be presented with suppression litigation which would give an opportunity to speak to why a warrant was not needed. And all the while, the number of applications to search will proliferate.

The two questions before the court are: (1) does a judge have the authority in managing her docket to reject an unnecessary warrant application even though the government established probable cause to search; and (2) was a search warrant unnecessary given that Google had conducted a prior private search?

II. DISCUSSION

A. Court's Authority To Review Search Warrants

A magistrate judge is not an automaton considering probable cause in a vacuum. "In authorizing [a] Warrant, the [Court] implicitly decide[s] upon the necessity of it in the first place." *In re Use of a Cell-Site Simulator*, 2021 WL 1133838, at *2, n.4. When considering a warrant application, "[i]t is no answer to [simply] argue . . . that probable cause existed in [the] case. The same could be said in any case in which the court finds probable cause but holds the warrant too general." *United States v. Buck*, No. 84-cr-220, 1986 WL 14296, at *5 (S.D.N.Y. Dec. 4, 1986), *rev'd on other grounds*, 813 F.2d 588 (2d Cir. 1987). Prohibiting magistrate judges from denying unnecessary search warrants cedes to the executive branch the power to define the boundaries of Fourth Amendment protections. This is a role reserved for the courts. "The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. . . . [T]hose charged with [] investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks." *United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 317 (1972).

Judges have an obligation to manage their dockets to conserve limited resources because "judicial economy plays a paramount role in trying to maintain an orderly, effective, administration of justice." *In re Vistaprint Ltd.*, 628 F.3d 1342, 1346 (Fed. Cir. 2010). The public "interest in the dispensation of justice that is not unreasonably delayed has great force." *United States v. Poston*, 902 F.2d 90, 96 (D.C. Cir. 1990) (quoting *United States v. Burton*, 584 F.2d 485, 489 (D.C. Cir. 1978)). "The public [also has] a compelling interest in judicial economy—not only in seeing speedy administration of justice, but also in ensuring that clogged dockets don't render courts inaccessible." *Auto. Techs. Int'l, Inc. v. Delphi Corp.*, No. 08-11048, 2011 WL 13209069, at *2 (E.D. Mich. June 16, 2011).

Courts have the "inherent power to manage the docket and promote judicial economy." *United States v. Halgat*, No. 13-cr-239, 2017 WL 736872, at *3 (D. Nev. Feb. 23, 2017); *see also Shrader v. Biddinger*, No. 10-cv-1881, 2011 WL 843931, at *2 (D. Colo. Feb. 10, 2011) (finding it appropriate to administratively close a case "in the interest of judicial economy and within the discretion of [the] court to manage its own docket efficien[tly] and effectively"), *rev'd on other grounds*, 2011 WL 841314 (D. Colo. Mar. 8, 2011); *Beale v. D.C.*, No. 04-cv-959, 2005 WL 8178299, at *2 (D.D.C. Sept. 30, 2005) (stating "the court has the inherent authority to manage its docket" and limiting the scope of discovery in the "interests of judicial economy"). Even the exercise of certain constitutional rights "cannot be insisted upon in a manner that will obstruct an orderly procedure in courts of justice, and deprive such courts of the exercise of their inherent powers to control the same." *Poston*, 902 F.2d at 96 (cleaned up) (upholding denial of a continuance to allow new counsel to prepare for trial, even though the sixth amendment right to counsel was implicated).

In 2020, NCMEC reported receiving 21.4 million CyberTip reports from Providers. *See* Brenna O'Donell, *Rise in Online Enticement and Other Trends: NCMEC Releases 2020 Exploitation Stats*, NCMEC Blog (Feb. 24, 2021), available at https://www.missingkids.org/blog/2021/rise-in-online-enticement-and-other-trends--ncmec-releases-2020-. Authorizing a search warrant here would open the flood gates to millions of unnecessary search warrant applications. Consider this against the backdrop that a cursory review of the docket revealed less than 1,000 total search warrant requests in 2020 for this district. The exponential increase in warrant requests would swamp courts' dockets and bring the "prompt, effective, and efficient administration of justice" to a grinding halt. *Poston*, 902 F.2d at 96.

Yet, a court must "'weigh competing interests and maintain an even balance' between the court's interests in judicial economy and any possible hardship to the parties." *Belize Soc. Dev. Ltd. v. Gov't of Belize*, 668 F.3d 724, 732–33 (D.C. Cir. 2012) (quoting *Landis v. North American Co.*, 299 U.S. 248, 254–55 (1936)). To rule based on judicial economy, there must be a "clear case of hardship or inequity in being required to go forward" compared to "even a fair possibility" that acting otherwise would adversely affect a party. *CEF Energia, B.V. v. Italian Republic*, No. 19-cv-3443, 2020 WL 4219786, at *5 (D.D.C. July 23, 2020) (quoting *Landis*, 299 U.S. at 255). The hardship to the government is negligible given it believed a warrant was unnecessary here. *See See* Suppl. Br. at 2. The government had opportunities to object to the Court's finding or plead hardship, yet it did not. Presumably this is because the instant opinion mitigates any possible harm to the government by providing a good faith basis for its review to go forward. Meanwhile, the hardship to the Court and the public from court clog is real and severe. *See Poston*, 902 F.2d at

96. Because the harm to judicial economy far outweighed any hardship to the government, the Court was authorized to reject the unnecessary warrant application. *See In re Use of a Cell-Site Simulator*, 2021 WL 1133838, at *2, n.4.

B. Google Performed A Private Search

A search occurs when a reasonable expectation of privacy is infringed upon, *see Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring), or when there is a "meaningful interference with an individual's possessory interests in [] property" by a government actor, *United States v. Jones*, 565 U.S. 400, 408 n.5 (2012). The government would need a warrant to compel Google to conduct a search for child pornography in user accounts because "individuals generally have reasonable expectations of privacy in the emails that they send through commercial providers like Google." *United States v. Miller*, 982 F.3d 412, 426 (6th Cir. 2020).

Yet, the Fourth Amendment's prohibition on unreasonable search and seizure does not reach the actions of private parties, unless they act as agents of the government or with participation or knowledge of any government official. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (no search warrant needed prior to performing chemical test on white powder identified by shipping company's private search of package). Indeed, the private-silver-platter doctrine dictates that the "unreasonable[ness]" of the private party search does not impact the government's use of the disclosed information without a warrant. *See id.*; *see also United States v. Lee*, 723 F.3d 134, 139 n.3 (2d Cir. 2013) (reviewing "silver platter doctrine"). Thus, a Provider, in its role as a private actor, "can search through all of the stored files on its server and disclose them to the government without violating the Fourth Amendment." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1212 (2004).

Google's compliance with the § 2258A(a) reporting requirement, "standing alone, does not transform [it] into a government agent whenever it chooses to scan files sent on its network for child pornography." *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013). Indeed, § 2258A(a) "is silent regarding whether or how [a Provider] should scan its users' e-mail." *Id.* Transforming a Provider into a government agent requires compulsion, not silence.[5]

Google is many things, *see* Google Products, available at https://about.google/intl/en_us/products/ (a phone company, an email provider, a streaming video company, a video chatting platform, a search engine, *etc.*), but a government agent it is not. "Google is a private entity." *Miller*, 982 F.3d at 421.

Google conducts child pornography searches at its own instigation to advance its "strong business interest[s]." Decl. at 1. Specifically, Google believes that "[r]idding its products and services of [child pornography] is critically important to protecting [its] users, [its] product, [its] brand, and [its] business interests." *Id.* Moreover, Google expressed concern that its users may stop using its products and services if its platform became "associated with being a haven for abusive content" such as child pornography. *Id.* Google retains total control over how it conducts

[5] No court in this Circuit has ruled on what transforms a private actor into an agent of the government for Fourth Amendment purposes. The Eighth and Sixth Circuits examine whether: (1) the government knew of and acquiesced in the search; and (2) whether the private actor conducted the search primarily to assist law enforcement, rather than to advance its own legitimate interests. *See United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013); *United States v. Bowers*, 594 F.3d 522, 525–26 (6th Cir. 2010). The First and Ninth Circuits examine: (1) the extent of the government's role in instigating or participating in the search; (2) the government's intent and degree of control exercised over the search and the private party; and (3) the extent to which the private party aims primarily to serve its own interests versus the government's interest. *See United States v. Silva*, 554 F.3d 13, 18 (1st Cir. 2009); *United States v. Rivera-Morales*, 961 F.3d 1, 8 (9th Cir. 2020). Regardless, Google's search here does not qualify under either standard as government-compelled action that would transform it into a government actor.

these searches without any input or oversight from the government. *See* Canegallo. Thus, Google is a private entity whose search for such material is "independent[] and voluntar[y]." Decl. at 1.

B. Law Enforcement Did Not Exceed The Scope Of Google's Private Search

Without a warrant, the government's search cannot "exceed the scope of the private search." *Jacobsen*, 466 U.S. at 116. The relevant question is whether the government knows with "substantial certainty," based on the prior private search, what the government will find when it conducts its own search. *United States v. Runyan*, 275 F.3d 449, 463 (5th Cir. 2001). "Such an 'expansion' of the private search provides the police with no additional knowledge that they did not already obtain from the underlying private search and frustrates no expectation of privacy that has not already been frustrated." *Id.*; *see also Rann v. Atchison*, 689 F.3d 832, 836–38 (7th Cir. 2012) (following *Runyan* and upholding law enforcement's search of digital memory card and computer zip drive handed over by private actors after they simply stated it contained child pornography).

There is a "substantial certainty" that child pornography identified by hash value match or CSAI Match is in fact child pornography. This matching process is at least once checked by a Google reviewer. *See* Decl. at 2. "And Google employees trained on [the] federal definition are much more likely to accurately identify child pornography than a person who comes across one disturbing image."[6] *Miller*, 982 F.3d at 431. The chances of Google's submission based on a hash match not being child pornography is "astronomically small." *See* Salgado, *supra* p.3. Indeed,

[6] Undoubtedly, "Google employees who add files to its child-pornography repository might mistake a lawful image for an illegal one. Yet that is not a type of error that matters under the private-search doctrine." *Miller*, 982 F.3d at 431. Just because a private party turns out to be wrong about the legality of an item that the party discloses to police does not mean that the police violate the Fourth Amendment when they reexamine the item. *Id.* "[T]he police [do not] conduct a Fourth Amendment 'search' if the pictures that a private party provides turn out not to be 'child pornography' under 18 U.S.C. § 2256." *Id.*

the "hash-value match's near-perfect accuracy" moves beyond a "substantial certainty" to a "virtual certainty" that the videos the government will review in this CyberTipline report are child pornography within the scope of the private search. *Miller*, 982 F.3d at 418.

In some cases, such as this, Google reports a video file that contains a hash match to child pornography without viewing the video in its entirety at any point. The question then is, does the government exceed the scope of the prior private search when it views the entire video file? It does not. *See Runyan*, 275 F.3d at 460. In *Runyan*, the private party viewed some, but not all, of the images on the defendant's disks and discovered they contained child pornography. *See id.* Law enforcement subsequently viewed specific files on the disks not viewed by the private party without obtaining a warrant. *See id.* The defendant's expectation of privacy in the entire disk was compromised when the private party viewed even a few images, and thus, law enforcement stayed within scope of the private search when they examined different images on the same disk. *Id.* at 465; *cf. United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990) (finding law enforcement search of a box containing pornography did not exceed scope of private search even though law enforcement took more time and was more thorough than the private searchers).

The government's review of the full video file from the CyberTipline is akin to examining "more items" on a disk or examining the disk more "thoroughly" than Google did. *Runyan*, 275 F.3d at 464. This is not a case in which law enforcement opened files with no hash match to suspected child pornography. *Compare United States v. Ackerman*, 831 F.3d 1292, 1306 (10th Cir. 2016) (finding law enforcement's visual inspection of three attachments in an email not identified by hash match to contain child pornography exceeded scope of private search), *with United States v. Reddick*, 900 F.3d 636, 639–40 (5th Cir. 2018) (finding law enforcement's visual inspection of files that contained hash matches to known child pornography did not exceed the scope of private search).[7]

The *Runyan* court granted a broader scope of review, allowing a search of all digital media regardless of whether the specific file had been viewed and confirmed by the private party to contain child pornography. 275 F.3d at 464-65. This order does not allow the government to look through an entire email account, or even all the attachments of a single email. Rather, the government can only view the files Google excised from the customer's account that contain a match to known child pornography.[8]

[7] As with *Miller*, the instant application is easily distinguished from *Ackerman*. In *Ackerman*, AOL sent an entire email and its four attachments to NCMEC, after only one of the files produced a hash match to child pornography. *See* 831 F.3d at 1294. The government agent subsequently viewed the full content of the email and its attachments. *Id.* This was found to exceed AOL's private search because the hash match was only to a single image. *Id.* at 1305–06. The *Miller* Court found "*Ackerman* reserved whether its holding would change if the analyst had viewed *only* the one image." 982 F.3d at 429. The *Miller* Court distinguished *Ackerman* by finding the government agent in *Miller* "viewed only files with hash-value matches." *Id.* This is identical to the instant case. Google only sent video files with hash matches to the CyberTipline. Thus, the government does not exceed the scope of the private search when it views only these files with no surplus content or attachments. *See id.*

[8] On this ground, this ruling is consistent with *United States v. Rouse*, 148 F.3d 1040 (8th Cir. 1998). In *Rouse*, law enforcement exceeded the scope of an airline employee's private search when officers examined more items in defendant's luggage than the employee examined. *See id.* at 1041. *Rouse* rejected the proposition that an entire suitcase, or an entire email account, can be searched following a single hit to illicit material. *See id.* at 1042.

III. CONCLUSION

The Fourth Amendment should not be used to place unnecessary and wasteful roadblocks between a private actor's voluntary disclosure of criminal activity and the government's lawful use of such information. *See Coolidge v. New Hampshire*, 403 U.S. 443, 488 (1971). Finding otherwise would "discourage citizens from aiding to the utmost of their ability in the apprehension of criminals." *Id.*

Zia M. Faruqui

Digitally signed by Zia M. Faruqui
Date: 2021.05.22 18:32:34 -04'00'

ZIA M. FARUQUI
UNITED STATES MAGISTRATE JUDGE