UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

GOOGLE LLC, Petitioner, v. UNITED STATES OF AMERICA, Respondent.	Case No. 23-mc-67-MJS

MEMORANDUM OPINION AND ORDER

On January 6, 2021, two pipe bombs were discovered outside the headquarters of the Republican National Committee ("RNC") and the Democratic National Committee ("DNC"), mere blocks away from the U.S. Capitol. Nearly four years later, no charges have been brought against any suspect(s). But not for lack of trying, at least as far as this Court can tell.

The United States has pursued multiple search warrants aimed at identifying the perpetrator(s). Petitioner Google LLC ("Google") was the recipient of several of those warrants, including the one being challenged here.[1] After complying with the prior warrants, Google now moves to quash the latest one on various grounds. First, and primarily, Google argues that the warrant impermissibly authorizes a "general search" in violation of the Fourth Amendment. Google takes this argument a step further by contending that the First Amendment implications of the information being demanded should trigger even stronger Fourth Amendment scrutiny. Second, Google argues that the warrant should be quashed under Section 2703(d) of the Stored

[1] *See generally* Search and Seizure Warrant, *In The Matter of the Search of Information Associated with Google Accounts, Cookie IDs, and IP Addresses That Conducted Google Searches That Are Stored at Premises Controlled by Google LLC Pursuant to 18 U.S.C. § 2703 for Investigation of 18 U.S.C. § 2332a And 26 U.S.C. § 5861(D)*, No. 21-sc-542, ECF No. 16 (the "Warrant").

Communications Act (SCA), 18 U.S.C. § 2703(d), because the records requested are assertedly too voluminous and because compliance would impose an undue burden on Google.

Google's challenges largely fail. U.S. Supreme Court precedent forecloses the sort of pre-execution Fourth Amendment challenge that Google mounts here, and the scope of the warrant—at least as narrowed by the Government in its briefing—does not demand records that are unusually voluminous or that otherwise impose an undue burden on Google. Consequently, the Court will **DENY** Google's Motion, except to **PARTIALLY GRANT** the Motion insofar as it seeks to quash the request for "technically connected user" information (which the United States withdraws).

BACKGROUND

For some time now, the United States has been in pursuit of the perpetrator(s) responsible for placing two pipe bombs outside the RNC and DNC buildings on January 5, 2021. At least some of those efforts have focused on obtaining potentially relevant information from Google.

In January and February 2021, the United States obtained three reverse search warrants directing Google to produce user information to help identify the suspect(s). The first set included two "geofence" warrants aimed at identifying Google users whose devices were within a specific geographic area near the RNC and DNC buildings during the relevant timeframe. (ECF No. 1 ("Mot.") at 5–6.) Next, the United States obtained a keyword reverse search warrant for anonymized information about users who: (1) conducted Google searches between January 1 and 5, 2021 related to the location of the RNC and DNC headquarters and their security; and (2) conducted searches on January 5 and 6, 2021 for news about the detonation or discovery of bombs *before* the incidents became public knowledge. (ECF No. 8 ("Opp'n") at 1–2; Mot. at 6–

8.) Google complied; it produced thousands of responsive searches along with anonymized user data for an estimated 1,341 users who made the responsive searches. (Mot. at 8; Opp'n at 8–9.)

After receiving the results of the keyword warrant, the United States next obtained a supplemental warrant in March 2021 seeking identifying information for the anonymized users who made approximately 293 of the thousands of responsive searches. (Mot. at 8, 10; Opp'n at 9.) Google complied; it disclosed identifying information for an estimated 251 users. (*Id.*) The United States then sought a second supplemental warrant in October 2022, but Google was reportedly unable to comply because it had purged the files identifying the responsive searches. (Mot. at 8; Opp'n at 10–11.) The United States withdrew that warrant. (*Id.*)

Now to the warrant at hand. On April 19, 2023, the United States applied for another search warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703.[2] Upon review, the Court found probable cause and issued the warrant. *See* ECF No. 14, Application, No. 22-sc-542 (Apr. 19, 2023); ECF No. 16, Search and Seizure Warrant, No. 22-sc-542 (Apr. 19, 2023).

This warrant is another reverse search warrant that directs Google to produce three categories of user information relating to approximately 537 responsive searches that Google previously identified in response to the 2021 keyword warrant (recall that the information produced in response to the earlier warrant anonymized the user details). This warrant seeks information about two classes of users: (1) those who made the responsive searches—a group the parties call the "querying users"—as well as (2) those who shared devices or identifiers with a querying user—a group the parties call the "technically connected users." (Mot. at 10–11.)

[2] Given the combined sources of authority for the requested warrant (both Rule 41 and 18 U.S.C. § 2703), it "is not a traditional search warrant, but instead a distinct procedural mechanism that imports some—but not all—of the requirements of Rule 41, including, *most importantly, the probable cause requirement*." *In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*, 2017 WL 3445634, at *21 (D.D.C. July 31, 2017) (emphasis added).

For the "querying users," a group estimated to encompass between 283 and 311 accounts,[3] the warrant calls for the same set of identifying information about those accounts as did the March 2021 supplemental warrant. (Mot. at 10; Warrant at 54.) The warrant further demands all records pertaining to any devices associated with the accounts of the "querying users," such as device serial numbers and mobile network information. (Mot. at 10; Opp'n at 12; Warrant at 55.)

For the "technically connected users"—defined as "any Google account (including both current and historical accounts) ever linked to" a querying user account by "(1) common e-mail address (such as a common recovery e-mail address), or (2) a common telephone number, (3) means of payment (e.g., credit card number), (4) registration or login IP addresses, registration or login cookies or similar technologies, or (5) any other unique device or user identifier"—the warrant seeks basic records and subscriber history described in 18 U.S.C. § 2703(c)(2). (Warrant at 55.) According to Google, these "technically connected users" would range from family members and coworkers to "strangers who, at some time (and not necessarily at the *same* time) logged in to their Google Accounts via the same public Wi-Fi access point." (Mot. at 11.)

The warrant directed Google to produce responsive information on or before May 14, 2023, but, before that date, Google informed the Government it would be unable to comply by the warrant's deadline. (Mot. at 12; Opp'n at 13.) Following further discussions about timing and scope, the parties were unable to reach agreement, and Google filed this Motion to Quash in July 2023. (*Id.*) The matter was recently reassigned to the undersigned in October 2024.

[3] The United States says the warrant requests the information of approximately 283 users. (Opp'n at 34.) Google claims that the search will produce approximately 311 users. (Mot. at 10.) Ultimately, the Court need not focus on this modest discrepancy because the magnitude is not material to the Court's analysis.

DISCUSSION

Google mounts two lines of attack against the warrant. First, Google principally argues that it violates the Fourth Amendment rights of its users to be free from unreasonable searches and seizures. And second, Google invokes 18 U.S.C. § 2703(d) to argue that the warrant seeks overly voluminous records that would impose on Google an undue burden to collect and produce. The Court takes each argument in turn.

I. Google's Fourth Amendment Challenge.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by establishing that "no [w]arrants shall issue, but upon probable cause … and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

Google argues that the warrant violates this bedrock principle because it "authorizes a general search that would infringe upon users' Fourth and First Amendment rights." (Mot. at 14.) As Google puts it, the government is trying to "seiz[e] the haystack to find the needle." (*Id.*) For its part, the Government rejoins that controlling precedent precludes this sort of pre-execution Fourth Amendment challenge to a warrant. (Opp'n at 16–19.) The Government is correct.

In *United States v. Grubbs*, the U.S. Supreme Court explained that "[t]he Constitution protects property owners not by giving them license to engage the police in a debate over the basis for the warrant, but by interposing, ex ante, the 'deliberate, impartial judgment of a judicial officer ... between the citizen and the police' and by providing, ex post, a right to suppress evidence improperly obtained and a cause of action for damages." 547 U.S. 90, 99 (2006) (ellipses in original) (quoting *Wong Sun v. United States*, 371 U.S. 471, 481–482 (1963)). Said another way, "the Fourth Amendment does not provide a chance to litigate the validity of a warrant before that warrant has been executed by the government." *In re Search of Recs., Info., & Data Associated*

with 14 Email Addresses Controlled by Google, LLC, 438 F. Supp. 3d 771, 776 (E.D. Mich. 2020). Instead, the necessary Fourth Amendment "check" against "unreasonable searches and seizures" occurs: (1) before a warrant's issuance, when an impartial judicial officer confirms probable cause, as happened here; and (2) after a warrant's execution, by way of a "motion to suppress during a criminal case or an after-the-fact civil rights lawsuit." *In re Search of Info. Associated With One Acct. Stored at Premises Controlled by Facebook, Inc.*, 2021 WL 2302800 at *1, 2 (D.D.C. June 4, 2021) (cleaned up) (quoting *United States v. Info. Associated with Email Acct. (Warrant)*, 449 F. Supp. 3d 469, 474–75 (E.D. Pa. 2020)). There is no third window for such challenges between a warrant's issuance and its execution, as Google attempts here.

Plenty of cases have applied *Grubbs* to reach this same conclusion. *Matter of Search of Info. Associated With One Email Acct. That is Stored at Premises Controlled by Google, Inc.*, 677 F. Supp. 3d 580, 584 (E.D. Tex. 2023) (applying *Grubbs* to foreclose an ability to move to quash a warrant based on the Fourth Amendment); *In re Anthony Marano Co.*, 647 F. Supp. 3d 643, 651 (N.D. Ill. 2022) ("In the criminal context, the Supreme Court definitively has rejected the notion that a target of a search warrant has a right to make a pre-execution court challenge to that warrant.") (collecting cases); *United States v. Crumpton*, 2023 WL 3611554, at *1–2 (M.D. Ga. May 23, 2023) (collecting cases holding that pre-execution challenges to search warrants are "foreclosed by clear Supreme Court precedent" in *Grubbs*).[4] *Grubbs* controls here, and it forecloses Google's pre-execution Fourth Amendment challenge.

[4] *See also, e.g.*, *Warshak v. United States*, 532 F.3d 521, 528 (6th Cir. 2008) (holding that Fourth Amendment challenges to warrants are properly limited to "two discrete, *post-enforcement* settings: (1) a motion to suppress in a criminal case or (2) a damages claim under [civil actions]"); *In re Search of Elec. Commc'ns in the Acct. of chakafattah gmail.com at Internet Serv. Provider Google, Inc.*, 802 F.3d 516, 528 n.39 (3d Cir. 2015) ("A subpoena … may be challenged prior to compliance. In stark contrast, a search warrant is properly challenged after it is executed."); *Info. Associated with Email Acct. (Warrant)*, 449 F. Supp. 3d at 474–75 (E.D. Pa. 2020) ("If [a user] has reason to conclude that the warrant was issued without probable cause or that the Government acted in an unconstitutional manner while executing the warrant, he

Google ignores *Grubbs* altogether. Its briefing fails to even acknowledge the Supreme Court's decision, let alone attempt to argue why it should not control. Instead, Google cites a handful of distinguishable and non-binding cases to argue that it has a "right to be heard before it is compelled to expend resources or bear other burdens assisting in the execution of an unlawful warrant." (ECF No. 9 ("Reply") at 3.) None of Google's cases bears on the Court's analysis.

For starters, most predate the Supreme Court's on-point ruling in *Grubbs* by decades. Moreover, none of the cases even mentioned—much less approved—the sort of pre-execution Fourth Amendment challenge to a warrant implicated here. They all addressed due-process challenges premised on claims of undue burden by the third-party communications provider being asked to comply with the warrant. *In re Application of the United States of America*, 610 F.2d 1148, 1157 (3d Cir. 1979) ("We conclude that *due process* requires a hearing *on the issue of burdensomeness* before compelling a telephone company to provide tracing assistance.") (emphases added); *Mountain States Tel. & Tel. Co.*, 616 F.2d 1122, 1132–33 (9th Cir. 1980) (similar); *In re Order Requiring [XXX], INC. to Assist in the Execution of a Search Warrant Issued by This Court by Unlocking a Cellphone*, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014) ("[D]ue process requires that a third party … be afforded a hearing on the issue of *burdensomeness*[.]") (emphasis added); *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, 149 F. Supp. 3d 341, 370 (E.D.N.Y. 2016) (similar). Whatever the broader implications of those cases, they do not support Google's position here—and certainly not in the

---

has within his defensive arsenal the option of filing a motion to suppress the evidence."); *United States v. Richards*, 2020 WL 5893974, at *1 (D. Utah Oct. 5, 2020) ("In this case, Ms. Richards has had the benefit of having a magistrate judge review and approve the United States' search warrant ex ante. Later, if evidence is improperly obtained from her, she then may seek, ex post, suppression of that evidence."); *Matter of 381 Search Warrants Directed to Facebook*, 132 A.D. 3d 11, 13 (N.Y. App. Div. 2015) (holding Facebook had "no constitutional or statutory right to challenge an alleged defective warrant before it is executed"), *aff'd on other grounds*, N.Y.3d 331 (2017).

face of specific precedent from the U.S. Supreme Court.[5] As noted, when it comes to the Fourth Amendment, the constitutional protections required before a warrant's enforcement are entrusted to "the deliberate, impartial judgment of a judicial officer," who ensures that probable cause exists (and that sufficient particularity is specified) before the warrant issues. *Info. Associated with Email Acct. (Warrant)*, 449 F. Supp. 3d at 474 (quoting *Grubbs*, 547 U.S. at 99).

This analysis resolves the bulk of Google's arguments. Because the Court cannot—and will not—consider a pre-execution Fourth Amendment challenge to the warrant as a general matter, the Court need not resolve the parties' more specific disagreements over whether Google has standing to vicariously raise a Fourth Amendment challenge on behalf of its users (Opp'n at 14–15; Reply at 7-14), or whether Google's users lost any Fourth Amendment rights to the information by voluntarily revealing it to a third party (Opp'n at 28-32; Reply at 15). These questions are secondary to the antecedent question of whether *any* pre-execution Fourth Amendment challenge is proper at this juncture; it is not. Separately, although Google's briefing invokes the First Amendment in a few places, those arguments are really nothing more than another gloss on Google's core Fourth Amendment challenging to the warrant—*i.e.*, that because the warrant ostensibly "targets information that may be protected by the First Amendment … the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude.'" (Mot. at 28.) The presence of particularized First Amendment implications (or not) does nothing to change the fact that Google's overall Fourth Amendment challenge founders under clear precedent.

As a final point, the Court returns briefly to the "due process" arguments that Google raises in reply. Google argues that it holds an independent "due process right to be heard before it is

[5] Google's reliance on the Third Circuit's decades-old decision in *In re Application* is particularly perplexing because that court has issued at least two (and far more recent) rulings endorsing the very principle from *Grubbs* that forecloses Google's challenge. *United States v. Wright*, 777 F.3d 635, 641 (3d Cir. 2015); *United States v. Jackson*, 2024 WL 2874364, at *3 n.8 (3d Cir. June 7, 2024).

compelled to expend resources or bear other burdens assisting in the execution of an unlawful warrant." (Reply at 3-6.)[6] For at least two reasons, this argument misses the mark. First, Google's failure to raise the argument until its reply brief provides a threshold basis to disregard it. *See, e.g.*, *Benton v. Laborers' Joint Training Fund*, 121 F. Supp. 3d 41, 51 (D.D.C. 2015) ("It is a well-settled prudential doctrine that courts generally will not entertain new arguments first raised in a reply brief."). But even treating the argument as properly raised, Google ignores that the SCA—at least based on how the parties have approached this case—affords Google an ability to challenge the warrant based on undue burden and voluminousness, *see* 18 U.S.C. § 2703(d), through a procedure that is essentially tantamount to the type of due process that Google seeks.

For these reasons, Google's Fourth Amendment challenge to the warrant fails.

II. Google's Section 2703(d) Arguments.

Separate and apart from its constitutional challenge(s), Google moves to quash the warrant on other grounds under the SCA, 18 U.S.C. § 2703(d). This statutory provision authorizes a court to quash or modify an order under Section 2703 "if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider."[7] Google says these grounds require relief here.

On this front, the contested issues have been narrowed considerably by the Government's "affirmative[] waive[r]" of Google's need to comply with the warrant's demand for "technically

---

[6] Google invokes the Fourteenth Amendment in support of this argument. But it is the Fifth Amendment that applies to federal actors (and the District of Columbia). *English v. District of Columbia.* 717 F.3d 968, 972 (D.C. Cir. 2013). Ultimately, the distinction is immaterial for present purposes because "the procedural due process protections under the Fifth and Fourteenth Amendments are the same." *Id.*

[7] Other courts have acknowledged a lack of clarity as to whether Section 2703(d) applies to *search warrants* (as here) rather than *orders*. *In re Search of Info. Associated With One Acct. Stored at Premises Controlled by Facebook*, 2021 WL 2302800 at *3 n.8. But the Government does not argue that Google's Section 2703(d) is improper on this basis—in fact, the Government expressly concedes that Google can challenge the warrant under 2703(d). (Opp'n at 34.). Accordingly, the Court assumes without deciding that Section 2703(d) can be invoked to challenge a warrant issued under Section 2703.

connected user" information. (*See* Opp'n at 3.) The Government now seeks execution of the warrant *only* as to the information related to the "querying users." For its part, Google balks at that concession somewhat because the Government has not "returned, withdrawn, or sought modification of the warrant, so the demand for technically connected users remains operative." (Reply at 7.) The Court understands Google's concern to some degree, given the arguable impermanence of the Government's offer, but the Court can remedy that concern by quashing as uncontested those aspects of the warrant the Government agrees to waive. The Court will do so.

This leaves only the warrant's request for "querying user" information and Google's related arguments about voluminousness and undue burden. The Court does not find those arguments compelling. Recall that Google already responded to a prior warrant requesting essentially the same categories of identifying information for an earlier set of user accounts associated with certain search queries. That past group of accounts was admittedly a tad smaller in number—251 users, versus 283 or 311 users, depending on which side's figure one credits—and, as Google points out, the Government is now seeking identifying information *plus* a few additional categories of related data. (*See* Mot. at 10.)[8] The Court acknowledges that the warrant (like all warrants) will undoubtedly impose some operational and logistical burden on Google in responding. But the key question is whether that burden is "undue." And ultimately, the Court does not believe that the warrant's request for a slightly expanded scope of information from a slightly larger group of users suddenly crosses the threshold into "unusually" voluminous or "unduly" burdensome, as contemplated by Section 2703(d). This is borne out by the fact that most of Google's arguments on these issues focus the "technically connected user" information, which is no longer at issue.

[8] Along with identifying information, the warrant requests "records pertaining to devices associated with the [querying users] and software used to create and access [their accounts]," including "any … unique identifiers that would assist in identifying any such device(s)." (Warrant at 54.)

As a final point, Google invokes the so-called "burden of compelled compliance" based on its view that the warrant is "overbroad and unsupported by probable cause, insufficiently particular, and unreasonable." (Mot. at 32.) As Google puts it, compliance with the warrant creates a separate burden by "undermining the trust of its users," particularly since it ostensibly "targets a large number of its users based on their protected political activities and associations." (*Id.*) At bottom, this theory is little more than a replay of Google's main Fourth Amendment challenge, which the Court already rejected for the reasons explained. Google's attempt to repackage those same arguments for consideration under Section 2703(d) fares no better. Moreover, at least one other court rejected similar arguments from Google on standing grounds; Google's argument that a warrant was "overbroad" for Fourth Amendment purposes—*i.e.*, its "sincere[] belie[f]" that the warrant was "an unlawful government intrusion"—did not demonstrate "how the supposed 'burden' to Google … will cause Google any 'real detriment.'" *In re Grand Jury Subpoena to Google, LLC Dated March 20, 2019*, 2020 WL 13505395, at *5 (S.D.N.Y. Jan. 31, 2020). This Court views the matter similarly and agrees that the so-called Fourth Amendment burdens Google invokes are not the types of burdens that Section 2703(d) contemplates.[9]

For these reasons, the Court likewise rejects Google's Section 2703(d) motion to quash the "querying user" information requested by the warrant.

[9] Finally, Google suggests that the nondisclosure order ("NDO") entered in conjunction with the warrant compounds this "burden" because it "bars Google from speaking about the warrant." (Mot. at 32.) Again, the Court views this argument as another gloss on Google's flawed pre-execution Fourth Amendment challenge. Beyond that, insofar as Google is attempting to attack the terms or scope of the NDO itself, it remains free to do so through a separate and direct First Amendment challenge, as has occurred in other matters. *See, e.g.*, *In re Sealed Case*, 77 F.4th 815 (D.C. Cir. 2023) (considering such a challenge).

CONCLUSION AND ORDER

The Court **DENIES** Google's Motion to Quash, except in limited part as follows. The Court **GRANTS IN PART** the motion as to the "technically connected user" information that the Government has waived and withdrawn. The Court thereby **MODIFIES** the warrant to **STRIKE** the following language from Section I of Attachment B at Page 55:

> "c. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any Google account (including both current and historical accounts) ever linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (e.g., credit card number), registration or login IP addresses, registration or login cookies or similar technologies, or any other unique device or user identifier."

The Court otherwise **DENIES** Google's Motion to Quash.

SO ORDERED.

Dated: November 25, 2024

MATTHEW J. SHARBAUGH
United States Magistrate Judge