UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

IN THE MATTER OF THE SEARCH OF CONTENT THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE	Case No. 16-mc-80263-LB **AMENDED ORDER** [Re: ECF No. 3]

INTRODUCTION

The government applied for, and the court issued, a search warrant under 18 U.S.C. § 2703(a), the Stored Communications Act ("SCA"), directing Google to produce stored content related to certain email accounts.[1] Google moved to quash on two grounds: (1) the government cannot compel Google to disclose content that it stores outside the United States; and (2) the search warrant asks for content that does not exist in the locations that the government specified (such as "Dasher Policy" or "GA Plus").[2] The court addressed the second issue in an earlier order; if the parties disagree about whether there is responsive data (and they likely do not), they will submit

[1] Warrant – ECF No. 4-1. Record citations refer to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of documents.

[2] Motion to Quash – ECF No. 3 at 3.

any discovery disputes in a joint letter brief.[3] The remaining dispute is whether Google must produce content that it stores outside of the United States.

Google has a distributed system where algorithms determine how it sends and stores data — in packets or component parts — in aid of overall network efficiency. In this case, the result is that Google has content that is responsive to the search warrant and is stored wholly outside of the United States. The legal issue is whether § 2703(a) reaches content stored outside of the United States. Citing the Second Circuit, Google contends that the government cannot compel it to disclose the extraterritorial content.[4] *See In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), *reh'g denied en banc*, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017). The government counters that the SCA authorizes production of data retrievable from the United States.[5]

The SCA regulates disclosure of data in a service provider's possession. The service provider — Google — is in the district and is subject to the court's jurisdiction; the warrant is directed to it in the only place where it can access and deliver the information that the government seeks. This disclosure is a domestic application of the SCA. The court thus orders Google to produce all content responsive to the search warrant that is retrievable from the United States, regardless of the data's actual location.

STATEMENT

1. Facts

Google — headquartered in the United States and incorporated in Delaware — has its principal place of business in California.[6] It offers its users different online and communication services, including email.[7] It stores its data in different locations, some in the United States and

[3] Order – ECF No. 31.

[4] Motion to Quash – ECF No. 3 at 5.

[5] Opposition – ECF No. 15 at 12.

[6] Stipulation of Facts ("SF") – ECF No. 37, ¶ 1

[7] *Id.*

some outside the United States.[8] User files may be broken into component parts, and different parts of a single file may be stored in different locations (including different countries).[9] Google operates what the parties term a "state-of-the-art intelligent network."[10] "[T]o optimize performance, reliability, and other efficiencies," the network moves data — including data responsive to the search warrant — automatically from one location to another (including different countries).[11] The data's location can change during the time period from when legal process (such as a search warrant) is authorized and when it is served.[12]

Google has a legal team in the United States — the Legal Investigations Support team — that produces information in response to search warrants and other requests for legal process.[13] All Google personnel on the team are in the United States, and only Google personnel on the team are authorized to access and produce the content of communications.[14]

The search warrant — signed on June 30, 2016 — authorized production of information from specific Google email accounts regarding subscriber information, evidence of specified crimes, and information about the account holders' true identities, locations, and assets.[15] Google produced the following information. One, for all Google accounts (except for one that did not exist), Google produced records "confirmed to be stored in the United States," including subscriber information, Google Contacts, files, location history, search history, Maps, and Photos metadata.[16] Two, for all but two accounts, Google "produced email content and header information" but "did not produce any attachments to those emails because they were not

---

[8] *Id.* ¶ 2.
[9] *Id.* ¶ 3.
[10] *Id.* ¶ 4.
[11] *Id.*
[12] *Id.*
[13] *Id.* ¶ 5.
[14] *Id.*
[15] Warrant – ECF No. 4-1 at 3–8.
[16] SF ¶ 7.

confirmed to be stored in the United States."[17] Three, for the remaining two accounts, Google "did not produce any Gmail content, non-content[,] or attachments" because "all such information for those accounts was stored exclusively outside of the United States."[18] As of November 18, 2016, Google "asserts that it had disclosed all responsive information" (as described in this paragraph) "that Google had confirmed at the time to be stored in the United States."[19]

2. Procedural History

Google moved to quash or amend the search warrant; the government opposed the motion.[20] The court held a hearing on February 21, 2017,[21] and directed (1) the parties to submit a joint stipulation of undisputed facts relevant to the extraterritoriality analysis and (2) Google to provide information about its current ability to identify whether information is stored in the United States, given its representation at the hearing that it was finalizing a tool to identify whether or not content was stored in the United States.[22] The parties provided additional information on March 13, 14, and 16.[23]

ANALYSIS

The warrant here issued under 18 U.S.C. § 2703(a), which is part of the Stored Communications Act ("SCA"). Section 2703 sets forth the legal processes that the government must use to require service providers such as Google to produce customer communications and records. For example, only an administrative subpoena is needed for basic subscriber information and transactional information. 18 U.S.C. § 2703(c)(2). The government can obtain a court order

[17] *Id.*
[18] *Id.*
[19] *Id.* ¶ 8.
[20] ECF Nos. 3, 15, and 16.
[21] Minute Order – ECF No. 28; Reporter's Transcript ("RT") – ECF No. 35.
[22] Order – ECF No. 31 at 2–3.
[23] ECF Nos. 37, 38, 39, and 41.

without notice to the customer for other non-content records if it "offers specific and articulable facts showing that there are reasonable grounds" that the records "are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d). Other user content can be obtained by subpoena or a 2703(d) order with notice to the subscriber or customer. *Id.* § 2703(b)(1)(A). To obtain stored communications, the government must obtain a "warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." *Id.* § 2703(a). The SCA defines a "court of competent jurisdiction" as (1) a U.S. district or appeals court that has jurisdiction over an offense being investigated, is in the service provider's district, or is acting on a request for foreign assistance under 18 U.S.C. § 3512, or (2) a state court of general criminal jurisdiction authorized by state law to issue search warrants. *Id.* § 2711(3). It is otherwise silent about its territorial reach or the reach of its warrant procedures.

The procedures for obtaining a search warrant are in Federal Rule of Criminal Procedure 41 — titled "Search and Seizure." Rule 41(b)'s venue provision limits its territorial reach to federal districts, generally providing for warrants for persons or property in the issuing court's district and sometimes allowing warrants for persons or property outside the district (but still in a federal district) in specified contexts, such as (1) the persons and property were in the district when the warrant issued, (2) investigations involving domestic or international terrorism, and (3) tracking devices installed in the district. Fed. R. Crim. P. 41(b)(1)–(4). Rule 41(b)(5) allows the issuance of a warrant for property outside the jurisdiction of any state or district but in (1) "a United States territory, possession, or commonwealth," (2) "a United States diplomatic or consular mission in a foreign state," or (3) a residence "owned or leased by the United States and used by United States personnel assigned to the United States diplomatic or consular mission in a foreign state." Rule 41(b)(6) allows warrants to issue in one district for searches of computer and media in other districts under certain circumstances.

The SCA does not specify whether it or its warrant provisions apply outside the United States. The court thus presumes that they do not under the canon of statutory construction known as the presumption against extraterritoriality. *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090,

2100 (2016); *Morrison v. Nat'l Australia Bank, Ltd.*, 561 U.S. 247, 255 (2010). "Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." *RJR Nabisco*, 136 S. Ct. at 2100 (citing *Morrison*, 561 U.S. at 255).

There are several reasons for the presumption. *Id.* "Most notably, it serves to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries." *Id.* "[I]t also reflects the more prosaic commonsense notion that Congress generally legislates with domestic concerns in mind." *Id.* (quotation omitted). "We therefore apply the presumption across the board, 'regardless of whether there is a risk of conflict between the American statute and a foreign law.'" *Id.* (quoting *Morrison*, 561 U.S. at 255).

Three recent Supreme Court decisions establish a two-part framework to analyze whether a statute applies extraterritorially. *RJR Nabisco*, 136 S. Ct at 2101; *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1665–69 (2013); *Morrison*, 561 U.S. at 261–70. "At the first step, we ask whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially." *RJR Nabisco*, 136 S. Ct at 2101. "We must ask this question regardless of whether the statute in question regulates conduct, affords relief, or merely confers jurisdiction." *Id.* "If the statute is not extraterritorial, then at the second step we determine whether the case involves a domestic application of the statute, and we do this by looking to the statute's 'focus.'" *Id.* "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory." *Id.*

The parties do not dispute that at step one, section 2703 and its warrant provisions do not contemplate or permit extraterritorial application.[24] The inquiry thus moves to step two: whether the case involves a domestic application of the statute, which in turn depends on whether the conduct relevant to the SCA's focus took place in or outside the United States. *Id.*

[24] United States' Opposition – ECF No. 15 at 18; Google's Reply – ECF No. 16 at 7–9.

Only the Second Circuit has considered the extraterritorial application of the SCA. In *Microsoft*, it held that the SCA did not apply outside the United States and Microsoft need not disclose user content stored in Ireland. *Microsoft*, 829 F.3d at 201–02, 216–21. Like Google, Microsoft provides web-based email. *Id.* at 202. It stores the contents of emails and other non-content information on a network of servers. *Id.* Its "service offerings" are "segmented into regions." *Id.* Most customer data (such as email, calendar entries, and documents) is stored in data centers in the region where the customer is located. *Id.* The customer self-reports the customer's location when subscribing to the Microsoft service; Microsoft does not verify user identity or location. *Id.* at 202–03. Based on the user's country code, Microsoft transfers data associated with the user to the server associated with the country code (for example, the Dublin datacenter), and (at the time) deleted most data sets in the United States. *Id.* at 203. At some offices in the United States, Microsoft could collect account data stored on its international servers. *Id.*

The Second Circuit denied the government access to the Ireland content. It determined that the statute's focus was user privacy, rejected the government's contrary argument that the SCA focused on "disclosure of content," and concluded that requiring Microsoft to disclose content stored in Ireland would be an unlawful extraterritorial application of the act. *Microsoft*, 829 F.3d at 216–21. The government sought rehearing *en banc*, which the Second Circuit denied in a four-four split decision. *See* 2017 WL 362765 (2nd Cir. Jan. 24, 2017). The court follows as persuasive the reasoning of the dissenters from the denial of rehearing *en banc* and concludes that the disclosure of information from Google's headquarters in the United States is a domestic application of the SCA. *Id.* at *5–18 (four dissenters — Circuit Judges Jacobs, Cabranes, Raggi, and Droney — each wrote a dissent; each dissenter joined the others' dissents). The statute's application here is lawful, and Google thus must provide all responsive information.

The parties stipulate that the only place to access the information is in the United States.[25] Even if the SCA's focus is privacy, the warrant requirement — with its attendant requirement of probable cause — protects privacy. *Id.* at *6 (Jacobs, J., dissenting). Moreover, an SCA warrant is

[25] SF ¶ 5.

not a search warrant in the classic sense: the government does not search a location or seize evidence. Instead, the conduct relevant to the focus — and what the SCA seeks to regulate — is disclosure of the data in the service provider's possession. *Id.* at *10 (Cabranes, J., dissenting). The service provider — Google — is in the district and is subject to the court's jurisdiction; the warrant is directed to it in the only place where it can access and deliver the information that the government seeks. "[I]f statutory and constitutional standards are met, it should not matter" where a service provider chooses to store the 1's and 0's. *Id.* at *7 (Jacobs, J., dissenting). That conclusion is especially true here. Unlike *Microsoft*, where storage of information was tethered to a user's reported location, 829 F.3d at 203, there is no storage decision here. The process of distributing information is automatic, via an algorithm, and in aid of network efficiency.

In sum, the disclosure is a domestic application of the SCA. Other courts have reached similar conclusions after a similar analysis of the *Microsoft* decision. *See, e.g.*, *In re: Information associated with one Yahoo email address that is stored at premises controlled by Yahoo*, No. 2:17-mj-1234-WED, ECF No. 1 at 6–8 (E.D. Wis. Feb. 21, 2017);[26] *In re Search Warrant to Google*, No. 2:16-mj-960-JS-1, 2017 WL 471564, at *9–14 (E.D. Pa. Feb. 3, 2017).[27]

[26] The memorandum and order addressed two miscellaneous cases: *In re Information associated with one Yahoo email address that is stored at premises controlled by Yahoo*, No. 2:17-mj-1234-WED; and *In re: Two email accounts stored at Google, Inc.*, No. 2:17-mj-1235-WED. In the *Google* case, Google objected to the magistrate judge's order, and the magistrate judge directed Google to file a motion to quash. *See* No. 17-mj-1235, ECF Nos. 3 & 4. That motion is still pending. The court was unable to access through PACER the sealed docket in the *Yahoo* case.

[27] The memorandum of decision addressed two cases: *In re Search Warrant No. 16-960-M-01 to Google*, No. 2:16-mj-960-JS-1; and *In re Search Warrant No. 16-1061-M to Google*, No. 2:16-mj-1061-JS-1. Google objected to the magistrate judge's decision. That objection is still pending.

CONCLUSION

The court denies Google's motion to quash the warrant for content that it stores outside the United States and orders it to produce all content responsive to the search warrant that is retrievable from the United States, regardless of the data's actual location.

IT IS SO ORDERED.

Dated: April 25, 2017

LAUREL BEELER
United States Magistrate Judge