IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE SEARCH WARRANT NO. 16-960-M-1 TO GOOGLE	:	MJ NO. 16-960
IN RE SEARCH WARRANT NO. 16-1061-M TO GOOGLE	:	MJ NO. 16-1061

MEMORANDUM

Juan R. Sánchez, J. **August 17, 2017**

Google Inc. seeks review of United States Magistrate Judge Thomas J. Rueter's February 3, 2017, Order granting the government's motions to compel Google to fully comply with two warrants issued pursuant to § 2703 of the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712. The warrants require Google to disclose to the Federal Bureau of Investigation electronic communications and other records and information associated with four Google accounts belonging to United States citizens in connection with two domestic wire fraud investigations. Google objects to the Order insofar as it requires Google to produce data the company has elected to store on servers located outside of the United States, asserting that enforcing the warrants as to such data would constitute an unlawful extraterritorial application of the SCA, as the Second Circuit Court of Appeals held in *In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016) [hereinafter *Microsoft*], *reh'g en banc denied*, 855 F.3d 53 (2d Cir. 2017) [hereinafter *Microsoft Reh'g*]. Although Google and each of the account holders in question are based in the United States, Google contends it is the physical location of the data to be retrieved—which Google, not the account holder, controls, and which Google can change at any time for its own business purposes—that determines whether the statute is being applied extraterritorially. Because this Court agrees with the government that it is the location of the provider and where it will disclose

the data that matter in the extraterritoriality analysis, and because Google can retrieve and produce the outstanding data only in the United States, the Court agrees with the Magistrate Judge's conclusion that fully enforcing the warrants as to the accounts in question constitutes a permissible domestic application of the SCA. The Order granting the government's motions to compel will therefore be affirmed.

BACKGROUND

Google is a United States-based technology company that offers a variety of different online and communications services, including email. *See* Stip. ¶ 1. Although Google's corporate headquarters are located in California, the company stores user data in a number of different locations both within and outside of the United States. *Id.* ¶¶ 1-2. Google operates a "state-of-the-art intelligent network" that automatically moves some types of data, including some of the data at issue in this case, from one network location to another "as frequently as needed to optimize for performance, reliability and other efficiencies." *Id.* ¶ 4. In addition, for some types of data—for example, a Word document attached to an email—the network breaks individual user files into component parts, or "shards," and stores the shards in different network locations in different countries at the same time.[1] *Id.* ¶ 3, Tr. 4. As a result, at any given point in time, data for a particular Google user may be stored not only outside of the country in which the user is located, but in multiple different countries, and the location of the user's data may change at any time based on the needs of the network. *See* Stip. ¶¶ 3-4. Thus, for example, the network

[1] When applied to some types of files, this "sharding" process generates individual shards that are incomprehensible on their own and become comprehensible only when the file is fully reassembled. *See* Oral Arg. Tr. 4-5, Apr. 18, 2017 [hereinafter cited as "Tr. __"] (explaining shards are "not like pieces of a puzzle, where if you got six of the seven pieces, you could make out six-sevenths of the documents"; rather, "[y]ou can't make out anything comprehensible unless you have all seven").

may change the location of data between the time a warrant is sought and the time it is served on Google. *See id.* ¶ 4.

In August 2016, Judge Rueter issued the first of the two warrants in question in this case. The warrant directs Google to provide the FBI with copies of communications and certain other categories of information associated with three Google accounts "stored at premises controlled by Google," and then authorizes the government to seize certain material from the information received. The government sought the warrant as part of an ongoing wire fraud investigation, whose target is both a citizen and resident of the United States, and all three Google accounts to which the warrant pertains belong to citizens and residents of the United States. The victim of the fraud under investigation is likewise located in the United States. In issuing the warrant, Judge Rueter found the government had demonstrated there was probable cause to believe that evidence of the fraud exists in the Google accounts.

Later the same month, United States Magistrate Judge M. Faith Angell issued the second warrant in question, requiring Google to produce to the FBI communications and other records and information associated with a single Google account belonging to the domestic target of a separate wire fraud investigation with a United States-based victim. Like the earlier warrant, this later warrant directs Google to provide the government with copies of certain categories of information associated with the account "located on [Google's] e mail servers" and authorizes the government to seize from Google's production certain files, documents, and communications. In issuing the warrant, Judge Angell found the government had shown there was probable cause to believe the target's Google account contains evidence of the fraud.

Both warrants were directed to Google at its headquarters in California, and Google's responses to the warrants were handled by the company's Legal Investigations Support team in

California. *See* Stip. ¶ 6; Tr. 32. Support team members are the only Google personnel authorized to access the content of user communications in order to produce such materials in response to legal process, and all support team members are located in the United States. *See* Stip. ¶ 5. In response to each warrant, Google searched for and retrieved from its network all responsive information stored at locations in the United States, a process that involves sending a series of queries from Google's headquarters in California to the company's data centers, directing the servers in those data centers to identify, isolate, and retrieve responsive material for Google to produce to the government. *See* Tr. 6-7, 30-31. All of the Google personnel involved in this process are located in California. *See id.* at 32. While Google produced to the government all of the responsive information it confirmed was stored in the United States, it did not produce data not known to be located in the United States. *See* Stip. ¶¶ 7-8. Rather, Google withheld such data based on the *Microsoft* decision in which the Second Circuit held "the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States." 829 F.3d at 222.[2]

The government thereafter moved to compel Google to fully comply with each warrant, and the matters were consolidated for argument and disposition. On February 3, 2017, Judge Rueter issued a Memorandum of Decision and Order concluding that requiring Google to fully comply with the warrants did not constitute an extraterritorial application of the SCA and granting the government's motions to compel. Google objects to this Order, taking issue with

[2] Prior to the *Microsoft* decision, when responding to a warrant, Google would query its network without regard to where on the network responsive information was located. *See* Tr. 7. Following the *Microsoft* decision, however, Google began limiting its queries to data centers located in the United States. *See id.* at 7-8.

the Magistrate Judge's extraterritoriality analysis. Following briefing of the issue by the parties and amici,[3] this Court held oral argument in this matter on April 18, 2017.

DISCUSSION[4]

The warrants in question were issued pursuant to the SCA, and it is the reach of the SCA's warrant provision that is at issue in this case; hence, the Court's analysis starts with the statute itself. Enacted as part of the Electronic Communications Privacy Act of 1986 (ECPA), the SCA grew out of congressional concern about the lack of privacy protection under existing

[3] Amicus briefs urging the Court to reject the Magistrate Judge's ruling were submitted on behalf of Yahoo, Inc. and on behalf of Microsoft Corporation, Amazon.com, Cisco Systems, Inc., and Apple Inc.

[4] Because these matters were never referred to a magistrate judge by a judge of this court, as contemplated by 28 U.S.C. § 636(b)(1)(A) or (b)(1)(B), the Order granting the government's motions to compel Google's full compliance with the SCA warrants is best understood as an exercise of the Magistrate Judge's jurisdiction under 28 U.S.C. § 636(b)(3), which permits a magistrate judge to be assigned "such additional duties," beyond those that may be assigned under § 636(b)(1)(A) or (b)(1)(B), "as are not inconsistent with the Constitution and laws of the United States." *See In re Search of Info. Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757, 2017 WL 3445634, at *4 (D.D.C. July 31, 2017). Unlike § 636(b)(1)(A) and (b)(1)(B), § 636(b)(3) does not specify a standard of review. Rather, the applicable standard depends upon whether the matter more closely resembles a pretrial motion that may be referred under § 636(b)(1)(A), in which case it is subject to review under § 636(b)(1)(A)'s "clearly erroneous or contrary to law" standard, or whether it more closely resembles one of the eight categories of motions excepted from § 636(b)(1)(A), in which case it is subject to de novo review under § 636(b)(1)(B). *See NLRB v. Frazier*, 966 F.2d 812, 816 (3d Cir. 1992). In *Frazier*, the Third Circuit Court of Appeals held that a motion to enforce a subpoena to require a witness to testify in a proceeding before an administrative agency was analogous to a dispositive motion and therefore subject to de novo review, *id.* at 817-18, and the case thus provides some support for the conclusion that the de novo standard is applicable here. The Court need not decide the issue, however, as this case turns on a question of law, and even under the clearly erroneous or contrary to law standard, such questions are subject to plenary review. *See Haines v. Liggett Grp. Inc.*, 975 F.2d 81, 91 (3d Cir. 1992) (holding the "contrary to law" standard in § 636(b)(1)(A) "indicates plenary review as to matters of law"); *see also Blunt v. Lower Merion Sch. Dist.*, 767 F.3d 247, 264 n.30 (3d Cir. 2014) (discerning "no difference between the plenary and de novo standards of review").

federal law for electronic communications in the control of third party computer operators.[5] As the Third Circuit previously observed, the SCA "was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to 'stored communications in remote computing operations and large data banks that stored e-mails.'" *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015) (quoting *Garcia v. City of Laredo*, 702 F.3d 788, 791 (5th Cir. 2012)). The SCA addressed this problem by creating "a set of Fourth Amendment-like privacy protections by statute" for electronic communications held by two types of network service providers: providers of "electronic communication service" and providers of "remote computing service."[6] *See* 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, 1212-14 (2004); *see also Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1179 (9th Cir. 2013).

The SCA's main substantive provisions appear in the first three sections of the Act. Section 2701 prohibits unauthorized access to "a facility through which an electronic

[5] *See* S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (concluding that stored wire and electronic communications—because they are "subject to control by . . . third party computer operator[s]" and thus may not be subject to constitutional privacy protection—"may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties"); *id.* at 5 (noting the lack of "Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology").

[6] For purposes of the SCA, "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). "[R]emote computing service" refers to "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2). An "electronic communications system," in turn, is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14).

communication service is provided," making it unlawful to "intentionally access[] without authorization" or to "intentionally exceed an authorization to access" such a facility and thereby to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system," and providing criminal penalties for a violation. 18 U.S.C. § 2701(a).[7] This prohibition against unauthorized access does not apply, however, "with respect to conduct authorized . . . by the person or entity providing a wire or electronic communications service." *Id.* § 2701(c)(1). Section 2701 thus does not prohibit a service provider from accessing communications stored on its own system. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 115 (3d Cir. 2004) (interpreting "§ 2701(c) literally to except from [§ 2701(a)'s] protection all searches by communications service providers"); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1026-27 (N.D. Cal. 2014) ("The SCA grants immunity to 18 U.S.C. § 2701(a) claims to electronic communication service providers . . . for accessing content on their own servers.").

Whereas § 2701(a) prohibits unauthorized access to stored communications by third parties, §§ 2702 and 2703 govern disclosure of such communications by providers of electronic communication service or remote computing service. Section 2702 prohibits providers from "knowingly divulg[ing]" the contents of stored communications and other subscriber records and information, except as specifically permitted therein, including "as otherwise authorized in section 2703." *Id.* § 2702(a), (c)(1). And § 2703 sets forth the conditions under which the government may require providers to disclose the contents of stored communications and other

[7] A separate SCA provision, 18 U.S.C. § 2707, provides a private civil cause of action for knowing or intentional violations of § 2701(a).

subscriber records and information, notwithstanding the general prohibition on disclosure in § 2702. *Id.* § 2703(a)-(c).

Section 2703 establishes three main forms of legal process by which the government may require a provider to disclose subscriber information in its possession: (1) "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)," *id.* § 2703(a), (b)(1)(A), (c)(1)(A); (2) a "court order for disclosure" (or a "§ 2703(d) order") issued based on an offer by the government of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation," *id.* § 2703(d); and (3) "an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena," *id.* § 2703(b)(1)(B)(i), (c)(2). The particular form of legal process the government must obtain depends on the type of information it seeks, with more intrusive disclosures requiring a higher showing by the government. To require a provider to disclose the contents of wire or electronic communications, the government must obtain a warrant, unless prior notice is provided to the affected subscriber.[8] *Id.* § 2703(a), (b)(1)(A). If notice is provided, the government may require a provider to disclose the contents of communications (other than those in storage with a provider of electronic communication service for 180 days or less) by obtaining a § 2703(d) order or a subpoena. *Id.* § 2703(b)(1)(B). Lesser forms of process are required for non-content information. The government may require a provider to disclose non-content records and other information pertaining to a subscriber by obtaining a § 2703(d)

[8] A warrant is always required to obtain disclosure of the contents of a wire or electronic communication in electronic storage for 180 days or less from a provider of electronic communication service, regardless of whether prior notice is provided. 18 U.S.C. § 2703(a).

order,[9] *id.* § 2703(c)(1)(B), and may require disclosure of certain basic subscriber information and transactional records by way of a subpoena, *id.* § 2703(c)(2), though for either type of information, the government may also elect to proceed by warrant.

The issue in this case is whether enforcing the SCA warrants in question to require Google to produce communications and other subscriber data stored on servers located outside the United States constitutes an extraterritorial application of the statute. In analyzing this issue, the Court starts with the presumption against extraterritoriality, "a longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United Sates.'" *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991) (quoting *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949)). Under this presumption, unless a statute reflects "clearly expressed congressional intent" that it is to apply extraterritorially, it will be "construed to have only domestic application." *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100 (2016). Although the presumption serves in part "to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries," it also "reflects the more prosaic 'commonsense notion that Congress generally legislates with domestic concerns in mind.'" *Id.* (quoting *Smith v. United States*, 507 U.S. 197, 204 n.5 (1993)). The presumption thus applies "regardless of whether there is a risk of conflict between the American statute and a foreign law." *Id.* (quoting *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010)).

[9] The government may also obtain disclosure of such non-content records and information with the subscriber's consent or, where the subscriber is engaged in telemarketing and the government seeks the information in connection with a telemarketing fraud investigation, by formal written request. 18 U.S.C. § 2703(c)(1)(C), (D).

The Supreme Court has developed a "two-step framework for analyzing extraterritoriality issues." *Id.* at 2101. First, the court must determine "whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially." *Id.* If so, then the statute applies extraterritorially, subject only to "the limits Congress has (or has not) imposed on [its] foreign application." *Id.* If the presumption has not been rebutted, then the statute is not extraterritorial, and the court must determine, at the second step of the analysis, "whether the case involves a domestic application of the statute," *id.*, or, put differently, "whether the domestic contacts [of the case] are sufficient to avoid triggering the presumption [against extraterritoriality] at all," *Microsoft*, 829 F.3d at 216 (quoting *Mastafa v. Chevron Corp.*, 770 F.3d 170, 182 (2d Cir. 2014)). In making this determination, the court must discern the statute's "focus" and identify where the conduct relevant to that focus occurred. "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." *RJR Nabisco*, 136 S. Ct. at 2101. If, however, "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.*

Applying this extraterritoriality analysis, the Second Circuit held in *Microsoft* that enforcing an SCA warrant to require a domestic service provider to disclose subscriber data stored outside the United States would constitute an extraterritorial application of the statute. 829 F.3d at 221-22. At the first step of the analysis, the court concluded Congress did not intend the SCA's warrant provision to apply extraterritorially, a point the government had conceded. *Id.* at 210 & n.19, 216. Proceeding to the second step, the court held the focus of the SCA's warrant provision is on "protecting the privacy of the content of a user's stored

communications." *Id.* at 217. The court then concluded the conduct relevant to this statutory focus is the provider's invasion of its customer's privacy, which, in the court's view "takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft [the provider], acting as an agent of the government." *Id.* at 220. Because the content subject to the warrant in the *Microsoft* case "[wa]s located in, and would be seized from, [Microsoft's] Dublin datacenter," the court concluded the conduct relevant to the statute's focus—the invasion of privacy—also would occur outside the United States, and enforcing the warrant as to such content would therefore "constitute[] an unlawful extraterritorial application of the Act." *Id.* at 220-21.

A significant factor in the court's extraterritoriality analysis was the SCA's use of the term "warrant," a form of legal process traditionally understood to authorize searches and seizures only within the United States. *See United States v. Verdugo-Urquidez,* 494 U.S. 259, 274 (1990) (remarking that a U.S. warrant authorizing a search of a defendant's residence in Mexico "would be a dead letter outside the United States"). Given the territorial limitations traditionally associated with warrants—which typically "identify discrete objects and places, and restrict the government's ability to act . . . outside of the place identified, which must be described in the document," *Microsoft,* 829 F.3d at 212—the court found the statute's use of the term warrant supported the conclusion that "an SCA warrant may reach only data stored within United States boundaries," *id.* at 221.[10]

[10] A concurring panel member disagreed with the majority's characterization of the SCA's warrant requirement, observing an SCA warrant is not a traditional search warrant, and concluding that Congress's use of the term warrant was intended to invoke not the territorial limitations but the privacy protections traditionally associated with warrants—namely, "the requirement that an independent judicial officer determine that probable cause exists to believe that a crime has been committed and that evidence of that crime may be found in the communications demanded." *Microsoft,* 829 F.3d at 226-28 n.6 (Lynch, J., concurring). While

Although the panel decision in the *Microsoft* case was unanimous, the decision drew vigorous opposition from other judges of the Second Circuit when the case came before the full court on the government's petition for rehearing en banc. The petition was denied by an equally divided court, but the denial generated four separate dissents by judges who agreed that enforcing an SCA warrant to require a domestic service provider to disclose information in the provider's possession, which the provider can access within the United States, constitutes a domestic application of the statute's warrant provision, regardless of where the provider has elected to store the information. *See Microsoft Reh'g*, 855 F.3d at 61-62 (Jacobs, J., dissenting); *id.* at 66-68 (Cabranes, J., dissenting); *id.* at 70-73 (Raggi, J., dissenting); *id.* at 75-76 (Droney, J., dissenting). The *Microsoft* court's analysis has also been rejected by every magistrate judge and district court that has considered the issue to date, including the Magistrate Judge in this case.[11]

---

the concurring judge did not view the term warrant as dispositive of the instrument's reach, the judge nevertheless agreed with the panel majority that the warrant at issue could not be enforced as to communications stored on servers located abroad given the lack of any indication that Congress had considered the implications of such an application of the statute, particularly as to communications belonging to foreign nationals.

[11] *See In re Search of Content that Is Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A*, No. 16-mc-80263 (N.D. Cal. Aug. 14, 2017), *aff'g* 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *In re Search of Info. Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757, 2017 WL 3445634 (D.D.C. July 31, 2017), *aff'g* 2017 WL 2480752 (D.D.C. June 2, 2017); *In re Search of Info. Associated with Accounts Identified as [Redacted]@gmail.com and Others Identified in Attachment A that Are Stored at Premises Controlled by Google Inc.*, No. 16-mj-2197, 2017 WL 3263351 (C.D. Cal. July 13, 2017); *In re Search Warrant to Google, Inc.*, Mag. No. 16-4116, 2017 WL 2985391 (D.N.J. July 10, 2017) (objections filed); *In re Two Email Accounts Stored at Google, Inc.*, No. 17-M-1235, 2017 WL 2838156 (E.D. Wisc. June 30, 2017) (objections filed); *In re Search of Premises Located at [Redacted]@yahoo.com*, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017); *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017).

Having withheld the foreign-stored communications and information the government seeks based on the *Microsoft* decision, Google urges this Court to follow a variation of the panel majority's extraterritoriality analysis in this case. As in the *Microsoft* case, there is no dispute as to the first step of the extraterritoriality analysis. The parties here agree that § 2703 gives no indication Congress intended for that provision to apply extraterritorially. *See* Google's Br. 3; Government's Opp'n Br. 18. The dispute instead centers on the second step of the analysis, at which the Court must determine whether this case involves a domestic application of the SCA by identifying the focus of the statute and where "the conduct relevant to the statute's focus" occurred. *RJR Nabisco*, 136 S. Ct. at 2101.

Google argues the focus of the SCA is on protecting the privacy of electronic communications. As to § 2703 in particular, Google argues this provision protects the privacy of communications and other subscriber data by requiring the government to obtain one of the enumerated forms of legal process in order to compel a provider to disclose such information. Google maintains that where the required form of process is a warrant, the conduct relevant to the SCA's privacy focus includes the search and seizure process Google must undertake in order to disclose the requested communications to the government—i.e., the searching, accessing, and retrieval of the compelled communications—a process that, in Google's view, occurs primarily where the communications are stored. In making this argument, Google emphasizes the SCA's use of the term warrant, asserting that in using this term of art, Congress would have intended to convey the term's widely accepted meaning as "a form of legal process authorizing the execution of a search of private places and a seizure of private things," and that such places and things must be located in the United States to be within a warrant's territorial reach. *See* Google's Reply Br. 3-4.

The government disputes Google's characterization of the warrant authorized by § 2703, arguing an SCA warrant is not a traditional search warrant but its own form of process. The government contends that unlike a traditional warrant, which is executed with respect to a place, an SCA warrant is directed to a person—the service provider from which the government seeks to compel disclosure of subscriber information. In the government's view, because an SCA warrant operates with respect to a person, rather than a place, so long as the enforcing court has personal jurisdiction over the provider, the warrant may be enforced to reach information in the provider's custody or control, regardless of the location of the information, consistent with the law governing other forms of compelled disclosure. As to the Supreme Court's extraterritoriality framework, the government argues the focus of § 2703 is compelled disclosure, as disclosure is the end result of each of the forms of process outlined therein and is thus the basic conduct the statute regulates. The government maintains the conduct relevant to the compelled disclosure focus is the compulsion, which "occurs in the United States, on United States providers, and in United States courts." Gov't's Opp'n 21-22. Alternatively, the government argues that even if § 2703's focus is privacy, the conduct relevant to the statute's privacy focus is the disclosure of subscriber information to the government and the government's search of the disclosed records, both of which occur in the United States.

As an initial matter, this Court agrees with the government that the warrant contemplated by the SCA is not a traditional search warrant. Notwithstanding its use of the term warrant, the SCA gives no indication that the warrant to which § 2703 refers authorizes a search and seizure in the traditional sense—i.e., entry by government agents into a provider's premises to search for and seize the device containing the communications sought. *See Microsoft*, 829 F.3d at 226 (Lynch, J., concurring). Instead, the SCA requires a warrant as the procedural mechanism by

which the government may require a service provider to disclose the contents of electronic communications in its possession, suggesting an SCA warrant is executed with respect to a person (the service provider) rather than a place (the data center).[12] For most categories of communications, a warrant is simply one of several alternative means, along with a subpoena and a § 2703(d) order, by which the government may require a provider to disclose the contents of communications, depending upon whether notice is given to the affected subscriber. *See Microsoft*, 829 F.3d at 227 (Lynch, J., concurring) (noting the various methods § 2703 provides for obtaining subscriber communications, with or without notice, "are not merely parallel," but "depend on the same verbal phrase"). In manner of operation, then, an SCA warrant is "more

[12] That an SCA warrant is not a traditional search warrant is underscored by the ways in which the SCA departs from the requirements of Federal Rule of Criminal Procedure 41. Although an SCA warrant must be issued "using the *procedures* described in the Federal Rules of Criminal Procedure," 18 U.S.C. § 2703(a), (b)(1), (c)(1)(A) (emphasis added)—including the requirement that a warrant may be issued only upon a showing of probable cause, *see* Fed. R. Crim. P. 41(d)(1)—an SCA warrant is not, strictly speaking, a Rule 41 warrant, *cf.* 18 U.S.C. § 3512(a)(2) (listing a Rule 41 search warrant and an SCA warrant as different types of orders a federal judge may issue to execute a request from a foreign authority for assistance in the investigation or prosecution of criminal offenses). Whereas a traditional Rule 41 warrant generally requires notice to the affected party upon execution, *see* Fed. R. Crim. P. 41(f)(1)(C), an SCA warrant may be executed without notice to the subscriber in most instances, *see* 18 U.S.C. § 2703(b)(1)(A). The SCA also dispenses with the requirement that an officer be present for service or execution of an SCA warrant. *Id.* § 2703(g). Most significantly, SCA warrants are not subject to Rule 41's venue provisions, which emphasize the location of the place to be searched in defining a magistrate judge's authority to issue a search warrant. Rather, since the SCA was enacted, Congress has twice amended the statute to expand the federal courts' authority to issue SCA warrants. As a result of the amendments, an SCA warrant may be issued not only by a court in the district where the service provider is located or the communications sought are stored, but also by a court with "jurisdiction over the offense being investigated." *Id.* § 2711(3)(A) (defining a "court of competent jurisdiction" capable of issuing an SCA warrant). As one court has recently noted, extending authority to issue SCA warrants to a court with jurisdiction over the offense reinforces the similarity between an SCA warrant and a federal criminal subpoena, which also may be "issued out of an investigating district and served anywhere the recipient is subject to service." *See In re Search of Info. Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.*, 2017 WL 3445634, at *20 (citation omitted).

closely analogous to the workings of subpoenas and court-ordered discovery," forms of legal process generally understood to be capable of reaching records in the possession or control of a party of which the enforcing court has personal jurisdiction, regardless of where the records are located, without raising extraterritoriality concerns.[13] *Microsoft*, 829 F.3d at 228 nn.5 & 6 (Lynch, J., concurring); *see also Microsoft Reh'g*, 855 F.3d at 65 n.19 (Cabranes, J., dissenting) (characterizing an SCA warrant "more akin to a subpoena, *but* with the important added protection of a probable cause showing to a neutral magistrate" (internal citation omitted)); *id.* at 71 (Raggi, J., dissenting) (concluding that "when a § 2703(a) warrant supported by probable cause is executed on a person within the jurisdiction of the United Sates, the SCA is being applied domestically without regard to the location of the materials that the person must divulge"); *In re Search of Info. Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc.*, 2017 WL 3445634, at *14-17 (holding an SCA warrant is "a domestic execution of the [issuing] court's statutorily authorized enforcement jurisdiction over a service provider, which may be compelled to retrieve electronic information targeted by the warrant, regardless of where the targeted information is 'located'").

[13] *See, e.g.*, *Gerling Int'l Ins. Co. v. Comm'r of Internal Revenue*, 839 F.2d 131, 136, 140 (3d Cir. 1988) (holding a litigating corporation with control over documents in the physical possession of another corporation may be compelled to produce the documents, even if located abroad); *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983) (holding a court with personal jurisdiction over a foreign corporation under investigation for violating United States law could enforce a grand jury subpoena requiring production of documents located abroad as "[t]he test for the production of documents is control, not location"); *United States v. Bank of Nova Scotia*, 691 F.2d 1384, 1390 (11th Cir. 1982) (enforcing a grand jury subpoena served on the Florida agency of a Canadian chartered bank which called for the production of records maintained in the bank's Bahamian branch); *United States v. First Nat'l City Bank*, 396 F.2d 897, 900-01 (2d Cir. 1968) ("It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has in personam jurisdiction of the person in possession or control of the material.").

Turning to the Supreme Court's extraterritoriality framework, although the SCA as a whole is undeniably concerned with the privacy of electronic communications held by third-party service providers, to determine the focus of the SCA's warrant provision,[14] this Court must consider what the provision "seeks to regulate" and what interests it "seeks to protect." *Morrison*, 561 U.S. at 267 (alteration, citation, and internal quotation marks omitted). Applying this analysis, the Court is persuaded the focus of § 2703 is on a provider's disclosure of electronic communications and other subscriber data to the government.

Section 2703's disclosure focus is apparent from the text of the provision, which is aptly titled, "Required disclosure of customer communications or records." The first three subsections of § 2703 define the conditions under which the government may obtain disclosure of different categories of subscriber information, establishing the particular form of legal process the government must obtain in order to "require a provider . . . to disclose" each type of information. *See* 18 U.S.C. § 2703(a)(1) (describing conditions under which the government "may require the disclosure by a provider of electronic communication service" of the contents of wire or electronic communications); *id.* § 2703(b)(1) (describing conditions under which the government

[14] The parties agree the determination whether a statute applies extraterritorially should be made on a section-by-section basis. *See* Tr. 10; Gov't's Opp'n 20 n.11; *see also RJR Nabisco*, 136 S. Ct. at 2101-10 (assessing extraterritoriality separately as to different provisions of the federal RICO statute); *Morrison*, 561 U.S. at 263-65 (holding that § 30(a) of the Securities Exchange Act of 1934 applies extraterritorially, but § 10(b) does not). Google argues, however, that in determining a statute's focus at the second step of the extraterritoriality analysis, a court need not "narrowly confine its inquiry regarding the focus of the statute to a single, isolated subsection, but rather can take into account the whole statute and related legislation." Google's Br. 8 n.4. Insofar as Google suggests that the relevant statutory focus is something other than the focus of the particular provision at issue, this Court disagrees. Although a court may consider provisions of a statute other than the particular provision at issue as part of its focus inquiry, the point of the inquiry is to determine the focus of the provision at issue. *See Morrison*, 561 U.S. at 266-68 (determining the focus of § 10(b) of the Exchange Act by considering the language of § 10(b), as well as other provisions of the Exchange Act and a companion statute).

"may require a provider of remote computing service to disclose" the contents of certain wire or electronic communications); *id.* § 2703(c)(1) (describing conditions under which the government "may require a provider . . . to disclose" non-content information pertaining to a subscriber); *id.* § 2703(c)(2) (describing the circumstances under which "[a] provider . . . shall disclose" to the government certain subscriber information and transactional records). Subsection (d) sets forth the requirements for a "court order for disclosure," one of the forms of process by which the government may "require a provider . . . to disclose" certain subscriber information. *See id.* § 2703(b)(1)(B)(ii), (c)(1)(B), (d).

The remaining three subsections of § 2703 address other aspects of compelled disclosure. Subsection (e) addresses the consequences of such disclosure for a provider, insulating the provider from liability for "providing information" in accordance with the terms of a warrant or other form of process requiring disclosure. *Id.* § 2703(e). Subsection (f) requires a provider to "preserve records and other evidence in its possession pending the issuance of a court order or other process," so that such information will be available for disclosure when the appropriate process is obtained. *Id.* § 2703(f). And subsection (g) specifies that an officer need not be present during the service or execution of a warrant "requiring disclosure by a provider." *Id.* § 2703(g).

The repeated emphasis on disclosure throughout § 2703 make clear that a provider's disclosure to the government is the conduct the statute seeks to regulate. Indeed, the Third Circuit has previously recognized as much, characterizing § 2703 as "directed to *disclosure* of communication information by providers." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 306 (3d Cir. 2010) (emphasis added). Moreover, while § 2703 seeks to balance "the privacy expectations of

American citizens and the legitimate needs of law enforcement agencies," S. Rep. No. 99-541, at 5, by defining the circumstances in which subscriber privacy must give way to law enforcement needs, the provision makes clear that it is the government's ability to obtain disclosure that the statute seeks to protect. *See also* 18 U.S.C. § 2703(f) (protecting the government's ability to obtain disclosure of subscriber information by permitting the government to require a provider to preserve evidence pending issuance of appropriate process).

Section 2703's relationship to other provisions of the SCA underscores that the focus of the warrant provision is on disclosure. While § 2702 generally prohibits a provider from "knowingly divulg[ing]" subscriber communications and other data to third parties, § 2703 creates an exception to this default rule of nondisclosure. That § 2703 "identifies circumstances when the government . . . 'may require' service providers to disclose their subscribers' communications," notwithstanding § 2702's general prohibition on such disclosure, "gives some force to the government's argument that the focus of § 2703 is compelled *disclosure*, not enhanced *privacy*." *Microsoft Reh'g*, 855 F.3d at 73 (Raggi, J., dissenting).

Insofar as disclosure is the focus of § 2703, the conduct relevant to this statutory focus is Google's disclosure to the government of responsive subscriber data, which will occur in the United States, where Google is located, regardless of where Google has chosen to store the data. Indeed, the disclosure can only occur in the United States, which is the sole location from which Google personnel may access the contents of communications in order to produce them in response to legal process. But even if the statute's focus is privacy, the Court nevertheless agrees with the Magistrate Judge and the government that the relevant conduct for purposes of the extraterritoriality analysis remains Google's disclosure of the compelled information to the government.

As noted, in arguing that the conduct relevant to § 2703's privacy focus includes the steps a provider must take to search for, access, and retrieve subscriber communications and other data from its network, Google emphasizes the statute's use of the term warrant, noting that unlike the other forms of process enumerated in the statute, a warrant contemplates a search and seizure process in which providers play a necessary part by "accessing and searching data centers outside the United States and seizing and retrieving to the United States customer communications." Google's Reply Br. 10. Google argues that because § 2703 protects user privacy "by regulating the procedures by which the government may infringe upon it," requiring different types of legal process for different types of information, where the applicable process is a warrant, the provider's conduct is "a necessary part of executing the warrant and a necessary precondition to the disclosure of the customer communications," and is therefore conduct relevant to the focus of the statute. *See id.* at 9-10.

As Google notes, a provider served with an SCA warrant plays a role in executing the warrant. The provider must retrieve the categories of information delineated in the warrant (for example, all emails associated with a particular account for a particular date range) and provide a copy of that information to the government so that the government can then search for and seize information constituting evidence of crime. Contrary to Google's assertion, however, the provider's accessing and retrieval of subscriber data do not implicate the subscriber's privacy within the meaning of the SCA. Rather, it is only when the provider discloses a subscriber's data to the government that the subscriber's privacy is implicated.

To the extent that the SCA addresses access to subscriber communications, the statute is concerned solely with unauthorized access by third parties. *See* 18 U.S.C. § 2701(a) (making it a crime to "intentionally access[] without authorization" or to "intentionally exceed[] an

authorization to access" a facility through which electronic communication service is provided). As a provider of electronic communication service, however, Google is exempt from § 2701's prohibitions on unauthorized access with respect to communications stored on its own system. *See id.* § 2701(c)(1) (specifying the prohibitions on access "do[] not apply with respect to conduct authorized . . . by the person or entity providing a wire or electronic communications service"); *Fraser*, 352 F.3d at 114-15 (holding § 2701 does not prohibit a service provider from searching emails stored on its own system). The SCA does not prevent Google from accessing its subscribers' data, or from moving subscriber data around its network, which the company admittedly does routinely for efficiency purposes. *See* Tr. 13-14 (acknowledging Google has authorized access to information on its network); Stip. ¶ 4. Such actions by Google thus do not implicate subscriber privacy under the SCA. *See Microsoft Reh'g*, 855 F.3d at 73 (Raggi, J., dissenting) (noting the SCA provides no privacy right against a provider's accessing and movement of subscriber communications, which actions "disclose nothing to the government about the existence or content of such communications").[15]

Rather than preventing a provider from accessing subscriber communications in its custody, § 2703 prevents the provider from disclosing the contents of those communications to the government unless the government first obtains a warrant or other required form of legal

[15] For similar reasons, Google's accessing and retrieval of a subscriber's communications do not amount to a search or seizure of the communications in the Fourth Amendment sense. *See Microsoft Reh'g*, 855 F.3d at 73 (Raggi, J., dissenting) ("[A] service provider who complies with a § 2703(a) warrant compelling disclosure of communications in his lawful possession does not thereby conduct a search or seizure as the agent of the government."); *In re Search of Info. Associated with [Redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*, 2017 WL 3445634, at *26 (holding Google's accessing and transfer of customer information to which the company has lawful access does not amount to a search or seizure); Mem. of Dec'n 19-23 (concluding Google's electronic transfer of data from a foreign data center to a data center in California does not constitute a Fourth Amendment search or seizure).

process. Indeed, it is only a provider's disclosure of communications to the government that is unlawful in the absence of a warrant. *See Microsoft Reh'g*, 855 F.3d at 68 (Cabranes, J., dissenting); *id.* at 73 (Raggi, J., dissenting). Consequently, to the extent that privacy is the focus of § 2703, "the territorial event that is the focus of that privacy interest is the service provider's disclosure of the subscriber communications to [the government]," and it is "where that disclosure occurs that determines whether [§ 2703] [is] being applied domestically or extraterritorially." *Id.* at 73 (Raggi, J., dissenting); *see also id.* at 68 (Cabranes, J., dissenting). Because the warrants the government seeks to enforce in this case were issued in the United States to a United States-based provider and require disclosure in the United States, enforcing the warrants constitutes a domestic application of the SCA.

Even if the steps taken by a provider to search for, access, and retrieve subscriber communications for eventual disclosure to the government were conduct relevant to § 2703's focus, this Court has considerable difficulty with Google's assertion that, where the communications in question are stored in foreign data centers, the "vast majority" of this conduct occurs outside of the United States. *See* Tr. 30. By Google's own account, the search and retrieval process consists of a series of queries initiated by Google personnel in the United States to which servers in the targeted data centers respond. *See id.* at 30-32 (describing a process whereby Google employees in California query foreign data centers to locate and isolate a subscriber's documents and to retrieve such documents to the United States). While these queries may be run on servers in Google's foreign data centers, it is difficult to see how this amounts to *conduct* by Google at the location of the data center, given that the United States-based employees direct the search and retrieval process remotely, without involvement by any personnel located abroad. *See Microsoft*, 829 F.3d at 229 (Lynch, J., concurring) (concluding

"[t]he entire process of compliance [with an SCA warrant] takes place domestically" because corporate employees in the United States can review and provide the relevant materials to the government "without ever leaving their desks in the United States"); *cf. Microsoft Reh'g*, 855 F.3d at 68 n.35 (Cabranes, J., dissenting) (suggesting the legal point of access of stored communications is better understood as "the location from which the service provider electronically gains *access* to the targeted data" rather than "the physical location of the datacenter"). That the subscriber's communications are accessed only by—and can be accessed only by—Google personnel in the United States, and are produced by such personnel in the United States, reinforces the conclusion that the only conduct involved in the search and retrieval process occurs domestically.[16]

For the reasons set forth above, this Court agrees with the Magistrate Judge's conclusion that enforcing the SCA warrants at issue in this case to require Google to produce data stored outside the United States is a domestic application of the SCA, the Magistrate Judge's Order granting the government's motions to compel Google to fully comply with those warrants will be affirmed. An appropriate Order follows.

[16] Google analogizes the warrant compliance process to "requiring a bank to search, seize, and retrieve to the United States documents its customer has stored in a safe deposit box in a foreign branch or requiring a hotel chain to search, seize, and retrieve to the United States luggage or correspondence a customer has stored in a room in a foreign hotel," Google's Br. 9, but the nature of electronic documents make this analogy inapt. Unlike paper documents, which have a tangible physical existence and location, "[e]lectronic 'documents' are literally intangible," *Microsoft Reh'g*, 855 F.3d at 61 (Jacobs, J., dissenting), and "[t]heir location on a computer server in a foreign country is, in important ways, merely virtual," *Microsoft*, 829 F.3d at 229 (Lynch, J., concurring). This is particularly true of subscriber communications that have been subjected to Google's sharding process, as such documents can "only exist in recognizable form when they are assembled remotely." *Microsoft Reh'g*, 855 F.3d at 61 (Jacobs, J., dissenting) (quoting Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 408 (2014)).

BY THE COURT:

/s/ Juan R. Sánchez
Juan R. Sánchez, J.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE SEARCH WARRANT NO. 16-960-M-1 TO GOOGLE	:	MJ NO. 16-960
IN RE SEARCH WARRANT NO. 16-1061-M TO GOOGLE	:	MJ NO. 16-1061

ORDER

AND NOW, this 17th day of August, 2017, upon consideration of Respondent Google Inc.'s Brief in Support of Objections to Magistrate Judge's Order Granting the Government's Motion to Compel, the Government's Brief in Opposition thereto, Google's Reply, the amicus briefs submitted by Yahoo Inc. and by Microsoft Corporation, Amazon.com, Cisco Systems, Inc., and Apple Inc., and the arguments presented at the April 18, 2017, oral argument, and for the reasons set forth in the accompanying Memorandum, it is ORDERED the Magistrate Judge's Order granting the Government's motions to compel is AFFIRMED. Google shall fully comply with the requirements of the search warrant issued in each of the above-captioned cases no later than 14 days from the date of this Order.

BY THE COURT:

/s/ Juan R. Sánchez
Juan R. Sánchez, J.