United States District Court, N.D. Alabama, Northeastern Division. IN RE SEARCH WARRANT ISSUED TO GOOGLE, INC.

CASE NO. 5:17–mj–532–HNJ

Signed September 1, 2017

MEMORANDUM OPINION AND ORDER

HERMAN N. JOHNSON, JR., UNITED STATES MAGISTRATE JUDGE

*1 The United States served on Google, Inc., a search warrant issued by the Court pursuant to the Stored Communications Act, 18 U.S.C. § 2703 *et seq.*Google complied with the search warrant as to data stored in the United States, yet it refused to disclose responsive data and information stored on a server located on foreign territory. According to Google, the SCA's provisions do not apply extraterritorially, and disclosing the data stored on foreign territory would constitute an impermissible, extraterritorial application of the statute. The Government filed a motion to compel Google to disclose the data stored on foreign territory. For the reasons set forth below, the Court GRANTS the Government's Motion because Google's disclosure of the data would constitute a domestic application of the SCA.[1]

I. BACKGROUND

Congress enacted the Stored Communications Act as Title II of the Electronic Communications Privacy Act of 1986. The other provisions of the ECPA updated prior statutes governing wiretaps, pen registers, and other aspects of electronic communication interception, *see* 18 U.S.C. §§ 2510 *et al.*, while the SCA aims to protect privacy by regulating access to stored communications. 18 U.S.C. § 2601 *et seq.*[2] Section 2701 of the SCA proscribes unauthorized access to data stored by electronics communications providers, and § 2702 prohibits electronics communications providers from disclosing stored communications data except in certain circumstances. 18 U.S.C. §§ 2701, 2702.

The dispute at bar concerns § 2703, which regulates government access to stored communications. As other courts have described, the SCA controls government access to stored communications in an ascending, or pyramidal, structure of protection. *See Matter of Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 207 (2d Cir. 2016) (*Microsoft I*), *rehearing en banc denied*, 855 F.3d 53 (2d Cir. 2017) (*Microsoft II*); *In re Search Warrant to Google, Inc.*, No. 16-4116, 2017 WL 2985391, at *3 (D.N.J. July 10, 2017). Administrative and investigatory subpoenas permit government access to basic subscriber and transactional data. 18 U.S.C. § 2703(c)(2). A court may order government access to other non-content information upon demonstration of "specific and articulable facts showing ... reasonable grounds to believe that the contents or records ... are relevant and material to an ongoing criminal investigation." *Id.* at §§ 2703(c), (d). Subpoenas give governmental access to the content of private communications, so long as the government gives notice to the customer or subscriber. *Id.* at § 2703(b)(1)(B). Upon establishing probable cause, a court may issue a warrant compelling government access to the previously-described stored communications, including the content of such communications such as emails, social media, etc. *Id.* at § 2703(a). The SCA does not require the Government to provide notice to a warrant's target. *Id.* at § 2703(b).

*2 In the case at bar, the Court issued a warrant pursuant to § 2703 commanding Google to disclose the information and content associated with several email accounts. In response, Google provided the government with data stored on servers located in the United States, but Google declined to produce responsive information stored on servers located in Dublin, Ireland. Google argues that the SCA does not apply extraterritorially, and thus the issued warrant does not apply to communications stored in areas outside of U.S. control.

Google's position rests upon the Second Circuit's decision in *Microsoft I.* In *Microsoft I*, the Second Circuit held that the government's warrant at issue therein could not compel Microsoft to produce communications and information stored overseas because the SCA does not apply extraterritorially. 829 F.3d at 222. On rehearing *en banc*, the Second Circuit split four-to-four on reversing the panel decision. *Microsoft II*, 855 F.3d

at 53. After the Second Circuit's dispositions, several courts disagreed with *Microsoft* and ruled that various providers, including Google, must produce information stored in foreign territories in response to warrants properly-issued under the SCA. *See In re Search Warrant to Google, Inc.*, No. 16-4116, 2017 WL 2985391 (D.N.J. July 10, 2017); *In re Two Email Accounts at Google, Inc.*, Case No. 17-MJ-1235, 2017 WL 706307 (E.D.Wis. Feb. 21, 2017), *mot. amend warrant denied*, No. 17-MJ-1235, 2017 WL 2838156 (E.D.Wis. June 30, 2017); *In the Matter of the Search of Info. Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc.*, Case No. 16–mj–757, ––– F.Supp.3d ––––, 2017 WL 2480752 (D.D.C. June 2, 2017); *In the Matter of Search of Content that Is Stored at Premises Controlled by Google*, Case No. 16-mc-80263-LB, 2017 WL 1487625 (N.D.Cal. Apr. 25, 2017); *In the Matter of the Search of Premises Located at [redacted]@yahoo.com, Stored at Premises Owned, Maintained, Controlled, and Operated by Yahoo, Inc.*, No. 6:17–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. 2017).

After the parties at bar failed to resolve their dispute, the resulting impasse led to the government filing the motion to compel.

II. ANALYSIS

As the following analysis portrays, the SCA does not apply extraterritorially because the statute does not contain any indication that Congress intended foreign application of the statute's provisions. However, the SCA's "focus" centers on access to private communications, and in particular government access to such data via provider disclosure on United States territory. Because Google's disclosure will occur on United States territory, the government's warrant entails a domestic application of the SCA, not an extraterritorial application.

The Supreme Court established a two-part framework in considering a statute's extraterritorial application. As an initial matter, there exists a presumption against extraterritoriality: "[a]bsent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." *Morrison v. National Australia Bank Ltd*, 561 U.S. 247, 255, 130 S.Ct. 2869, 177 L.Ed.2d 535 (2010). The inquiry ensues "whether Congress has affirmatively and unmistakably instructed that [a] statute will do so." *Id.* at 261, 130 S.Ct. 2869. "When a statute gives no clear indication of an extraterritorial application, it has none." *Id.* at 255, 130 S.Ct. 2869.

Therefore, the first part of the framework determines "whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially." *RJR Nabisco, Inc. v. European Cmty.*, ––– U.S. ––––, 136 S.Ct. 2090, 2101, 195 L.Ed.2d 476 (2016). If the first step does not dislodge the presumption against extraterritoriality, then the framework's second step discerns "whether the case involves a domestic application of the statute" 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.*

A. The SCA Does Not Apply Extraterritorially

*3 As for the first step in the framework, the court will not depart from the largely unanimous finding by the other courts considering this issue that the SCA does not apply extraterritorially.[3] The government argues that § 2703 contemplates provision of a hybrid warrant-subpoena vehicle that grants courts *in personam* authority over recipients, and this *in personam* power elides any territorial limitations upon the SCA. Google responds that § 2703 adopts the restrictions pertinent to a traditional warrant; as traditional warrants purportedly afford only *in rem* authority over places and things, Congress limited SCA warrants territorially by definition. Regardless of the parties' dispute over nomenclature, the SCA fosters no provisions rebutting the presumption against territoriality.

Section 2703 expressly requires warrants for the production envisioned here, not subpoenas. The government seeks the content of emails and other communications stored by Google, and as described previously, the SCA accords the warrant power for access to such content. Therefore, the government falters by referring to cases examining the scope of subpoena power—rather than the scope of authority pursuant to warrants—issued in other statutory contexts that require production of documents stored in foreign locations.

Indeed, that subpoenas may apply extraterritorially in other statutory contexts does not indicate such devices —or warrant-subpoena hybrids—apply extraterritorially under the SCA. That is, to the extent some forms of

subpoenas subject their recipients to a court's *in personam* authority, Congress may still limit courts' exercise of such personal jurisdiction in other contexts. *C.f., Republic of Panama v. BCCI Holdings (Luxembourg) S.A.*, 119 F.3d 935, 942, 946–47 (11th Cir. 1997) (pursuant to the Fifth Amendment's Due Process Clause, federal courts exercise personal jurisdiction over any defendant with sufficient contacts with the United States, but Congress may limit such jurisdiction by statutory authorization).[4] That Congress compels foreign access in one statutory context granting *in personam* jurisdiction does not demonstrate the same authority applies in other contexts, including the SCA.

However, Google's arguments regarding a warrant's purported *in rem* nature of jurisdiction suffer similar infirmities. As Google confirms, warrants issued pursuant to Rule 41, Federal Rules of Civil Procedure, do not apply extraterritorially. *See*Fed. R. Crim. P. 41(b) (limiting out-of-district warrants to particular locations no broader than United States territory or places under United States' control); *Amendments to the Federal Rules of Criminal Procedure*, 129 F.R.D. 557, 558 (1990) (rejecting an amendment to Rule 41 that would have permitted extraterritorial warrants, stating "The Court is of the view that the [proposed amendment to Rule 41 allowing for the issuance of search warrants with extraterritorial effect] requires further consideration."). However, Rule 41(a)(1)clearly provides that it "does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances."Therefore, Rule 41's proscription against extraterritorial application does not encircle all warrants into its ambit. For example, the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 permits warrants for the surveillance of U.S. persons in foreign countries. FISA Amendments Act of 2008, Pub. L. No. 110–261 §§ 703, 704, 122 Stat. 2436, 2448–57 (2008) (codified at 50 U.S.C. §§ 1881b, 1881c (2017)).

*4 Indeed, several courts persuasively hold that Rule 41(b)'s territorial limits do not apply to SCA warrants executed outside of the issuing federal courts' districts. As those cases cogently discuss, the SCA invokes the "procedures used in the Federal Rules of Criminal Procedure" to govern the issuance of warrants, 18 U.S.C. § 2703(a), yet this invocation does not incorporate Rule 41's substantive aspects, including any notions regarding extraterritorial application. *See, e.g., United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) ("The common definition of 'procedure' supports the conclusion that § 2703(a) incorporates only those provisions of Rule 41 that address the 'specific method' or 'particular way' to issue a warrant.... Rule 41(b) deals with substantive judicial authority—not procedure—and thus does not apply to § 2703(a)."); *United States v. Bansal*, 663 F.3d 634, 662 (3d Cir. 2011) (rejecting contention that Rule 41(b) trumps § 2703(a)); *United States v. Kernell*, No. 3:08-CR-142 (CCS), 2010 WL 1408437 (E.D.Tenn. Apr. 2, 2010), *rept. and recomm. adopted*, No. 3:08-CR-142 (TWP), 2010 WL 1491861 (E.D.Tenn. Apr. 13, 2010) ("[T]he plain language of 18 U.S.C. § 2703(a) expresses the intent that only the 'procedures,' (i.e., the procedural portions) as 'described' in Rule 41 are to be 'used.' This Court further finds that Rule 41(b) is not a 'procedural' provision, but is a 'substantive' provision, and thus, it is not incorporated under 18 U.S.C. § 2703(a)."); *United States v. McGuire*, No. 2:16–cr–00046–GMN–PAL, 2017 WL 1855737, at *8 (D.Nev. Apr. 9, 2017) ("The plain language of § 2703 allows magistrate judges with jurisdiction over an offense under investigation to issue warrants seeking the production of stored electronic communications from service providers located outside of their own district.").

In any event, the delineation between *in personam* and *in rem* jurisdiction falters upon recognition that the Supreme Court eradicated any substantive difference between the concepts. *Shaffer v. Heitner*, 433 U.S. 186, 206, 97 S.Ct. 2569, 53 L.Ed.2d 683 (1977) ("rights cannot depend on the classification of an action as *in rem* or *in personam*, since that is a classification for which the standards are so elusive and confused generally") (citations and quotation marks omitted). "The phrase, 'judicial jurisdiction over a thing', is a customary elliptical way of referring to jurisdiction over the interests of persons in a thing." *Id.* at 207, 97 S.Ct. 2569(citations omitted). *In personam* jurisdiction proffers authority over persons, yet conceptually *in rem* jurisdiction posits control over a person's rights in a thing or place, not merely authority over the place or thing. *Id.* at 211, 97 S.Ct. 2569 ("The fiction that an assertion of jurisdiction over property is anything but an assertion of jurisdiction over the owner of the property supports an ancient form without substantial modem justification.").

Therefore, as a conceptual matter, the purported exercise of *in rem* jurisdiction fashions a court's authority over the rights regarding stored data; such *in rem*jurisdiction differs insubstantially from the authority permitted by *in personam*jurisdiction over the holder of such rights. In this conception, the vehicle for the compelling authority—whether termed *in personam* or *in rem*, or via a warrant or a subpoena—matters little, as there exists no territorial baseline for any of the concepts. Indeed, as the comparison between Rule 41 and the SCA's warrants provisions demonstrates, Congress may alter the reach of purported *in rem*jurisdiction just as readily as it configures the reach of *in personam* jurisdiction.

When unmoored from the afore-mentioned distinctions, the inquiry devolves to an examination whether Congress affirmatively and unmistakably intended extraterritorial application of the SCA, contrary to the prevailing presumption against such treatment. Clearly, review of the SCA reveals no rebuttal against the presumption. In fact, courts have forbidden extraterritorial application of the wiretapping provisions of Title I of the ECPA, the companion law to the SCA. *See* *Huff v. Spaw*, 794 F.3d 543, 547 (6th Cir. 2015) ("Courts have repeatedly applied the general 'legal presumption' against extraterritorial application" to wiretaps); *United States v. Peterson*, 812 F.2d 486, 492 (9th Cir. 1987) (same); *Stowe v. Devoy*, 588 F.2d 336, 341 (2d Cir. 1978) (same); *United States v. Toscanino*, 500 F.2d 267, 279–80 (2d Cir. 1974) ("[T]he statute significantly makes no provision for obtaining authorizations for a wiretap in a foreign country."), *abrogation on other grounds recognised by In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 167 n.5 (2d Cir. 2008); *United States v. Angulo–Hurtado*, 165 F.Supp.2d 1363, 1369 (N.D.Ga. 2001) (same); *United States v. Bennett*, 538 F.Supp. 1045, 1048 (D.P.R. 1982) (citing *Toscanino*, 500 F.2d at 279); *Berlin Democratic Club v. Rumsfeld*, 410 F.Supp. 144 (D.D.C. 1976); *see also* S. Rep. No. 99–541, at 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566 (the Electronic Communications Privacy Act, which amended the Wiretap Act, "regulates only those interceptions conducted within the territorial United States").

*5 Indeed, Congress could not have envisioned the SCA applying in foreign territory when it enacted the law because firms overwhelmingly stored private communications in the United States. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PENN. L. REV. 404–05 (2014) (explaining that Congress enacted the SCA when most computer users were United States customers using services in the United States). Legislative history, in particular the 1986 House Judiciary Committee Report on the SCA, confirms that the provisions "regarding access to stored wire and electronic communications are intended to apply only to access in the territorial United States." H.R. Rep. No. 99–647, at 32–33 (1986). Furthermore, Congress tided the 2001 amendment authorizing the issuance of multidistrict warrants as the "*Nationwide* Service of Search Warrants for Electronic Evidence." Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107–56, § 220, 2001 U.S.C.C.A.N. (115 Stat.) 272, 291–92 (codified at 18 U.S.C. §§ 2703, 2711) (emphasis added); H.R. Rep. No. 107–236, at 57 (2001). Therefore, based on this review Congress did not intend extraterritorial application of the SCA.

As a final consideration on this issue, the government's invocation of the Senate's 2006 ratification of the Council of Europe Convention on Cybercrime does not alter this finding. The Cybercrime Convention requires signatories to compel persons to produce data in their possession or control. Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185, Art. 18.1.a, *available at* https://rm.coe.int/1680081561. The Explanatory Report transmitted with the Convention interpreted the custody-or-possession provision to include signatory authority to compel persons to produce data that may be stored outside of the signatory's territory. Explanatory Report to the Convention on Cybercrime, Nov. 23, 2001, 173, *available at*, https://rm.coe.int/16800cce5b. The government argues that Senate ratification of the Cybercrime Convention indicates that the SCA already provided the afore-mentioned authority required by the Convention.

The government's arguments fail to convince on this score. The Senate's ratification of the Convention does not even mention the SCA. Furthermore, the Senate did not ratify the Cybercrime Convention until 2006, more than 20 years after enactment of the SCA. The Supreme Court disfavors such *post hoc* interpretation of legislation. *Waterman S.S. Corp. v. United States*, 381 U.S. 252, 269, 85 S.Ct. 1389, 14 L.Ed.2d 370 (1965) (" 'the views of a subsequent Congress form a hazardous basis for inferring the intent of an earlier one.' ") (citing *United States v. Price*, 361 U.S. 304, 313, 80 S.Ct. 326, 4 L.Ed.2d 334 (1960); *United States v. Philadelphia Nat'l Bank*, 374 U.S. 321, 348, 83 S.Ct. 1715, 10 L.Ed.2d 915 (1963)). Indeed, the Cybercrime Convention does not even constitute legislation. The Convention incites the Senate's advice and consent function under Article II of the Constitution, not its legislative function pursuant to Article I. *In re Search Warrant to Google*, 2017 WL 2985391, at *9. Therefore, the President and the Senate's considerations cannot represent the interpretation by the entire Congress that the SCA fulfills certain of the Convention's conditions.

Therefore, based on the foregoing analysis, § 2703 of the SCA does not apply extraterritorially.

B. The Government's Warrant Falls Within the SCA's Focus

Because the SCA does not apply extraterritorially, the second step of the inquiry requires the undersigned to determine "whether the case involves a domestic application of the statute"—rather than an extraterritorial application—by "looking to the statute's 'focus.' " *RJR Nabisco*, 136 S.Ct. at 2101. "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." *Id.*Before conducting this inquiry, the meaning of "focus" in this context requires further elaboration. In particular, the Supreme Court's construal of a statute's "*focus*" delineates the inquiry from discerning a statute's *purpose*, and Google's arguments on this second prong of the analysis rests upon the SCA's purpose, not its focus.

*6 As established by the Supreme Court, a statute that does not have extraterritorial reach may still apply in a particular case because the "conduct" subject to the statute's focus occurs domestically. *Id.* In *Morrison*, the Court portrayed a statute's "focus" as encompassing particular "territorial event[s]" or "relationship[s]," or the "objects of [a] statute's solicitude." *Morrison*, 561 U.S. at 266–67, 130 S.Ct. 2869. Therefore, this second step requires a determination whether a dispute's conduct, event, relationship, or "object of solicitude"—which is purportedly regulated by a statute's focus—occurs in the United States.

Critically, the Supreme Court hones in on a statute's text to ascertain the conduct, event, relationship, or object of solicitude constituting its regulatory "focus," and the Court distinguishes this textual focus from other aspects of a statute's interpretation. Thus, in *Morrison* itself, the Court construed the "focus" of the Security and Exchange Act's § 10(b) (codified at 15 U.S.C. § 78j(b)) after rejecting extraterritorial application of that provision. 561 U.S. at 266–70, 130 S.Ct. 2869. Section 10(b) regulates the purchase and sale of securities so as to address fraudulent activities, yet the respondents in *Morrison* argued that the statute applied to European securities transactions because some of the deceptive conduct at issue occurred in the state of Florida. *Id.* at 266, 130 S.Ct. 2869. Although the Court acknowledged that § 10(b) serves to punish and dispel deceptive conduct, the statutory provision accomplishes this purpose by regulating the object of its solicitude—securities purchase-and-sale transactions—and in particular, domestic transactions of that nature. *Id.* at 267–69, 130 S.Ct. 2869; *see also RJR Nabisco*, 136 S.Ct. at 2100 (Section 10(b)'s "focus is on domestic securities transactions, and we therefore held that the statute does not apply to frauds in connection with foreign securities transactions, even if those frauds involve domestic misrepresentations."). Therefore, the Court ruled that the respondents could not rely upon § 10(b) to address European securities transactions that allegedly resulted from domestic, fraudulent activity. *Id.*

The same analysis coheres in *RJR Nabisco.* In that decision, the Court reviewed whether certain provisions of the Racketeer Influenced and Corrupt Organizations Act (RICO) (18 U.S.C. §§ 1962(a)–(d), and 1964(d)) applied extraterritorially. RICO proscribes patterns of racketeering activity committed through perpetrating conduct that violates predicate, criminal statutes. *RJR Nabisco*, 136 S.Ct. at 2096–97. Despite the allegation some of the racketeering activity occurred in the United States—and in fact some of RICO's § 1962 provisions applied extraterritorially—the Court ruled that § 1964(d)'s private cause-of-action remedy only applied to domestic injuries. 136 S.Ct. at 2106–09. Therefore, although RICO's purpose involves countermanding racketeering activity in the United States and abroad, and some of the alleged, racketeering activity occurred in Europe, § 1964(d)'s private cause-of-action provision focuses upon domestic injuries as its proscribed "event" or "object of solicitude," not all injuries resulting from alleged racketeering activity. 136 S.Ct. at 2111.

Likewise, the *Morrison* decision relied upon *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 255, 111 S.Ct. 1227, 113 L.Ed.2d 274 (1991) (*ARAMCO*), to depict this crucial distinction. *Morrison*, 561 U.S. at 266, 130 S.Ct. 2869. In *ARAMCO*, the plaintiff sued the respondent U.S. company for discriminatory employment practices in Saudi Arabia. The Court ruled that Title VII of the Civil Rights Act of 1964 (42 U.S.C. § 2000e, *et seq.*) did not apply extraterritorially. *ARAMCO*, 499 U.S. at 250–59, 111 S.Ct. 1227. More importantly for the present dispute, although Title VII's purpose encompasses the eradication of employment discrimination, the Court found that the statute's "focus" centered upon domestic employment, not foreign employment where the discriminatory practices occurred. *Id.* at 247, 255, 111 S.Ct. 1227; *see also Morrison*, 561 U.S. at 266, 130 S.Ct. 2869 (in *ARAMCO*, "neither [the foreign] event nor [the foreign] relationship was the 'focus' of congressional concern, ... but rather domestic employment").[5]

*7 In addition, *Morrison* cites to *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 69 S.Ct. 575, 93 L.Ed. 680 (1949), in support of its rulings on this point. 561 U.S. at 266, 130 S.Ct. 2869. In *Foley Bros.*, the Court considered whether the federal Eight Hours Law applied extraterritorially to workplaces in Iran and Iraq. The Court determined that the statute did not apply to restrict work hours in foreign locations. *Foley Bros.*, 336 U.S. at 285, 69 S.Ct. 575. Critically, the Court declared that via the Eight Hours Law Congress addressed a "concern with domestic labor conditions" (that is, the statute's purpose) by focusing upon "hours of work." *Id.* at 286, 69 S.Ct. 575.

Based upon the foregoing analyses, *Morrison* and related cases portray that Courts should discern a statute's focus textually, whereas a statute's purpose establishes a broader lens of perspective. A statute's purpose represents the aim, end, or goal a legislative body endeavors to address. *See* BLACK'S LAW

DICTIONARY (10th ed. 2014) (defining "purpose" as an "objective, goal, or end"); William C. Burton, LEGAL THESAURUS 424 (2d ed. 1992) (defining "purpose" as "aim, ambition, ... aspiration, ... goal, ... principle, ... objective, ..."). A statute's focus represents the conduct, events, relationships, or "objects of solicitude" Congress centers upon to effect the purpose of the statute. *See* Burton, LEGAL THESAURUS at 230 (defining "focus" as "arena, center, center of activity, center of attention, ... center of interest ...."); WEBSTER'S II NEW RIVERSIDE UNIVERSITY DICTIONARY 492 (1994) (defining "focus," *inter alia*, as a "center of interest or activity").

With this explanation, the errors in Google's arguments manifest. Google's argument that the SCA's "focus" is the privacy protection falters because that concern is not the statute's *focus.* Rather, the SCA laudably serves to protect private communications and prevent invasions of privacy, and this concern constitutes the statute's *purpose*,[6] The SCA effects this purpose, however, by focusing upon various forms of conduct, events, relationships, and "objects of solicitude," which coalesces under the broad category of regulating access. So long as the access occurs domestically, then the SCA properly applies to the conduct or event at issue.

Interpreting the plain language of the SCA's text, the SCA's purpose revolves around protecting private communications, but the SCA's focus rests upon effecting the purpose by controlling access to private communications. The statute itself, and even the larger ECPA of 1986 of which it is a part, barely mention "privacy." *See* Pub. L. 99–508, 100 Stat. 1848, 1848–73 (1986) (*codified as amended at* 18 U.S.C. § 2510, *et seq.*, 18 U.S.C. § 2701, *et seq.*, and 18 U.S.C. § 3121, *et seq.*) (only the title of the ECPA, and one definitional provision regarding radio communications (§ 101(a)(16)(B)), contains the word "privacy"). Furthermore, the ECPA's wiretapping and pen register provisions clearly focus upon the rights and procedures regarding access to private communications through interception.

*8 As for the SCA itself, the SCA's official title includes "access" as an operative term: "Stored Wired and Electronic Communications and Transactional Records *Access.*" Pub. L. 99–508 at Chap. 121 (1986) (codified as amended at 18 U.S.C. § 2703) (emphasis added); *see generally, INS v. National Ctr. for Immigrants' Rights, Inc.*, 502 U.S. 183, 189, 112 S.Ct. 551, 116 L.Ed.2d 546 (1991) ("[T]he title of a statute or section can aid in resolving an ambiguity in the legislation's text."); *Brotherhood of R.R. Trainmen v. Baltimore & Ohio R.R.*, 331 U.S. 519, 528–29, 67 S.Ct. 1387, 91 L.Ed. 1646 (1947) (The "heading is but a short-hand reference to the general subject matter involved.... For interpretive purposes, they are of use only when they shed light on some ambiguous word or phrase."). Furthermore, the SCA's text includes several references to its focus upon access. Section 2701, which proscribes, as titled, "[u]nlawful access to stored communications," prohibits unauthorized "access" to electronic communications facilities. Section 2702 limits access to customer communications by regulating providers' disclosure of such information.

As for the provision at issue in this case, § 2703 regulates specifically the government's access to private communications, and it does so by prescribing the process by which providers may disclose data to the government. Hence, Congress expressly describes the terms by which the government may access private communications by requiring providers to disclose information pursuant to a warrant, subpoena, or court order. 18 U.S.C. § 2703(a)–(d). Most critically, government access does not occur on foreign territory. Rather, the government gains access to private communications when a provider discloses information and data to the government, and such disclosure occurs domestically, not in foreign territories where the provider may store information and data.

Therefore, the conduct relevant to the SCA's focus—giving the government access to private data via provider disclosure (whether in the form of warrants, subpoenas, or by court order)—occurs in the circumstances at bar domestically. The government does not garner access to private communications until Google discloses data to the government, and such disclosure occurs in the United States, not in a foreign territory. The SCA's mechanisms exist to protect privacy, but § 2703 focuses upon government access via provider disclosure as the means to effect the privacy purpose.

That Google has to retrieve the data from servers located overseas does not implicate the SCA's focus because the statute does not regulate the location of stored private data. The statute does not evince any interest in where Google stores data, and it does not protect data privacy by controlling providers' territorial storage of data. It protects privacy by requiring probable cause and other standards for the government's access to data, and the government does not gain access until Google discloses data at a domestic location.

Google's primary rejoinder hones in upon *RJR Nabisco*'s phrase, "conduct relevant to a statute's focus," and implicitly upon the term "relevant." 136 S.Ct. at 2101. Google apparently construes the term "relevant" as a term of art, and thus, any activities that are "required by, and essential to the execution of," a statute's focus

should bear dispositive consideration in determining whether conduct occurs extraterritorially or domestically. As Google argues, its activities in accessing, retrieving, and copying data from its foreign servers factor decisively in the extraterritorial analysis due to the activities' relation to data disclosure.

Google errs in its argument because it ascribes undue significance to its access, retrieval, and copying of data. Properly considered, *RJR Nabisco*'s use of the term "relevant" distinguishes critical activities regulated by Congress from inconsequential activities that bear negligible impact under a statute's regime. Therefore, the phrase "conduct relevant to a statute's focus" refers to those activities that comprise the event, relationship, or "object of solicitude" Congress focuses upon in a statute, not inconsequential activities that nevertheless facilitate commission of those activities germane to a statute's focus. Properly discerned, the SCA focuses upon government access via provider disclosure; related provider activities—such as retrieving data from a foreign server while perched at a location in the United States—facilitate such disclosures yet do not represent the SCA's focus.

*9 In a further objection, Google argues that the event at issue in this case occurs in foreign territory because executing the warrant involves a search and seizure overseas. However, the government search here does not occur until the government accesses the data domestically, and a seizure does not occur until a person is dispossessed of property, which in these circumstances occur domestically. As another court considering this issue discerned, "complying with an SCA warrant does not require a service provider to access and seize data in the traditional sense that law enforcement might access and seize physical property." *Matter of Search of Info. Associated with [Redacted]@gmail.com*, 2017 WL 2480752, at *10. As the court discussed, a " 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *Id.* (citing *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984)). "Merely copying a document or taking a photograph of material—both reasonable analogs to [the circumstances] where Google accesses and makes an electronic copy of a user's data—is not a 'seizure' of that material because there is no meaningful interference with the owner's possessory interest in it ...." *Id.* (citing, *inter alia, Arizona v. Hicks*, 480 U.S. 321, 107 S.Ct. 1149, 94 L.Ed.2d 347 (1987) ("[T]he mere recording of the serial numbers [of a stereo system] ... did not 'meaningfully interfere' with respondent's possessory interest in either the serial numbers or the equipment, and therefore did not amount to a seizure."); *In re Search Warrant No. 16–960–M–01 to Google*, 232 F.Supp.3d at 719–21 (law enforcement accessing electronic data pursuant to an SCA warrant is not a "seizure" in the traditional sense)).

As the court explained, "Google's actions themselves do not result in an invasion of the user's privacy or an interference with the user's possessory interest in the data [because] Google is entitled to access and transfer its users' data within its network at will in accordance with its user agreements and ... § 2701(c)." 2017 WL 2480752, at *10 (citing *In re Search Warrant No. 16–960–M–01 to Google*, 232 F.Supp.3d at 720 ("Electronically transferring data from a server in a foreign country to Google's data center in California does not amount to a seizure because there is no meaningful interference with the account holder's possessory interest in the user data.")). Thus, the "privacy invasion occurs where Google discloses the compiled data to law enforcement, and government agents search those files for information relating to suspected criminal activity, all of which occurs domestically." 2017 WL 2480752, at *10 (citing *In re Search Warrant No. 16–960–M–01 to Google*, 232 F.Supp.3d at 721).

Therefore, the Court agrees with the overwhelming majority of courts that the SCA's § 2703 focuses upon government access via provider disclosure, and such disclosure occurs in the United States when the providers produce data and information to the government. *See In re Search Warrant to Google, Inc.*, 2017 WL 2985391, at *11; *In re Two Email Accounts at Google, Inc*, 2017 WL 2838156, at *4; *In the Matter of the Search of Info. Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc.*, 2017 WL 2480752, at **8–10; *In the Matter of Search of Content that Is Stored at Premises Controlled by Google*, 2017 WL 1487625, at *4; *In re Search Warrant No. 16–960–M–01 to Google*, 232 F.Supp.3d at 722.

CONCLUSION

Based on the foregoing discussion, the Court GRANTS the Government's Motion to Compel and ORDERS Google to comply with the search warrant insofar as it stores any responsive information in foreign territories.

Footnotes

[1]

In its Reply to the Government's Motion, Google argued that the Court should set an expiration date for the

non-notice provision of its Order granting the search warrant. Pursuant to 18 U.S.C. § 2705(b), the Court ordered Google not to inform the subscriber targeted by the warrant about the existence of the Government's warrant and associated activities, until otherwise authorized by the Court. Google argues that establishing an indefinite duration for a non-disclosure order violates the First Amendment. The Court will review Google's request in a separate Order.

[2]

The "ECPA" commonly refers to the three titles of the statute as a group (Titles I, II, and III of Pub. L. 99–508). Title I "prohibits the intentional actual or attempted interception, use, disclosure, or procurement of any other person" to intercept wire, oral, or electronic transmissions; Title II is the Stored Communications Act; and, Title III "addresses pen register and trap and trace devices," requiring government entities to obtain a court order authorizing their installation. *Id.* The code codifies Title I and III at 18 U.S.C. §§ 2510–22.

[3]

See, e.g., Microsoft I, 829 F.3d at 210; *Microsoft II*, 855 F.3d at 55, 60(dissent, J. Jacobs); *In re Search Warrant to Google*, 2017 WL 2985391 at *9; *Matter of Search of Info. Associated with [Redacted]@gmail.com*, 2017 WL 2480752, at *7; *Matter of Search of Content that is Stored at Premises Controlled by Google*, 2017 WL 1487625, at *3.

[4]

Compare Fed. R. Civ. P. 4(k) (limiting federal courts to the personal jurisdiction authority of the state courts of general jurisdiction where they are located), *with* the following statutes extending federal court personal jurisidiction nationally by provision of nationwide service of process: 9 U.S.C. § 9 (2012) (confirmations of arbitration awards); 15 U.S.C. § 22 (2012) (antitrust suits); 28 U.S.C. § 1694 (patent infringement); *id.* § 1695 (derivative actions); *id.* § 1697 (multidistrict litigation); *id.* § 2361 (statutory interpleader); 29 U.S.C. § 1132(e)(2) (2012) (ERISA).

[5]

Congress amended Title VII to abrogate *ARAMCO* and provide for the extraterritorial application of the statute. *See* Civil Rights Act of 1991, § 109(a), 105 Stat. 1077, *codified at* 42 U.S.C. § 2000e(f) ("With respect to employment in a foreign country," the term "employee" "includes an individual who is a citizen of the United States."

[6]

Legislative history indicates that the ECPA's purpose, including the SCA, relates to

The purpose of the legislation is to amend tide 18 of the United States Code to prohibit the interception of certain electronic communications; to provide procedures for interception of electronic communications by federal law enforcement officers; to provide procedures for access to communications records by federal law enforcement officers; to provide procedures for federal law enforcement access to electronically stored communications; and to ease certain procedural requirements for interception of wire communications by federal law enforcement officers.

H. Rept. 99–647 at 16. To the extent Google would equate "purpose" to "focus," the House Report bolsters the argument that the SCA's focus is government access to stored electronic communications via provider disclosure.

End of Document.