UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH
OF INFORMATION ASSOCIATED
WITH [REDACTED]@GMAIL.COM
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE, INC.

Case No. 16-mj-757 (GMH)

MEMORANDUM OPINION

On July 14, 2016, the United States Court of Appeals for the Second Circuit determined that the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* ("SCA"), "does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based [electronic communications or remote computing] service provider for the contents of a customer's electronic communications stored on servers located outside the United States." *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197, 222 (2d Cir. 2016) ("*Microsoft*"), *reh'g denied en banc*, 855 F.3d 53 (2d Cir. 2017). Following the court's decision, the government petitioned for a rehearing *en banc*, which the Second Circuit denied in an evenly split four-four vote. *See In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 855 F.3d 53, 55 (2d Cir. 2017) ("*Microsoft II*"). Against this backdrop and as a matter of first impression in this circuit, the undersigned must now resolve whether this Court will follow the Second Circuit's decision in *Microsoft*.

Last November, the Court issued a search warrant pursuant to section 2703 of the SCA requiring Google, Inc. ("Google") to disclose to the government the electronic records and information associated with a Google email account that the government believes was used by the subject of a criminal investigation.[1] Google refused to produce all of the information called for by the warrant based on its reading of the Second Circuit's decision in *Microsoft*. Specifically, Google refused to disclose any electronic data stored on servers located outside the United States. Google's refusal prompted the government to move for an order instructing Google to show cause for why it should not be compelled to comply fully with the warrant—i.e., to produce all responsive data within Google's possession, custody, or control wherever that data may be electronically stored. The Court granted the government's request and instructed the parties to submit written responses in support of their positions. After the matter became ripe for adjudication, the Court held a hearing to address the parties' arguments. Upon consideration of the parties' filings and the entire record herein,[2] the Court finds persuasive the reasoning of the four dissenters in the denial of the rehearing *en banc* in *Microsoft II*. Accordingly, the undersigned respectfully declines to follow *Microsoft* and concludes that Google's disclosure of the records and information from its headquarters in the United States is a domestic application of the SCA. Thus, Google will be compelled to comply fully with the warrant and to disclose all requested electronic records and information identified in Attachment B to the warrant within its possession, custody, or control, wherever those records and information may be electronically stored.

[1] The facts presented in the government's search warrant application and the parties' briefs involve an ongoing criminal investigation. Accordingly, the Court will describe the government's application and affidavit in only the broadest terms to prevent the disclosure of sensitive information about the government's investigation.

[2] The relevant docket entries for the purposes of this Memorandum Opinion are: (1) the Government's Motion for Order to Show Cause ("Mot.") [Dkt. 5]; (2) Google's Response in Opposition ("Resp.") [Dkt. 7]; (3) the Government's Reply to Google's Opposition ("Reply") [Dkt. 8]; (4) Google's Surreply in Opposition ("Surreply") [Dkt. 12]; and (5) Notice of Factual Stipulation by the Parties ("Stip.") [Dkt. 16]. All citations to page numbers within a particular document are to the ECF docket page numbers for the document.

BACKGROUND

A. Statutory Framework and the SCA Warrant at Issue

The SCA was enacted as part of the Electronic Communications Privacy Act in 1986 to extend privacy protections to users of electronic services. *Microsoft*, 829 F.3d at 205–06. It "'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 emails.'" *In re Search Warrant No. 16-960-M-01 to Google*, --- F. Supp. 3d ---, Misc. No. 16-960-M-01, 2017 WL 471564, at *3 (E.D. Pa. Feb. 3, 2017) (quoting *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015)). Broadly, the SCA "imposes general obligations of non-disclosure on [electronic communication and remote computing] service providers" with several exceptions. *Microsoft*, 829 F.3d at 207. Section 2702 of the SCA sets out those exceptions, which include emergencies involving the risk of death or serious physical injury and when authorized under section 2703 of the SCA. *See* 18 U.S.C. § 2702(b).

Section 2703, in turn, "sets up a pyramidal structure governing conditions under which service providers must disclose stored communications to the government." *Microsoft*, 829 F.3d at 207. In short, the government can compel disclosure from a service provider using one of three ascending tiers of legal process that are demarcated by the showing the government must make in order to utilize them: a subpoena, which requires no judicial review; a court order, which requires a judicial finding that the government has established "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"; or a judicially-approved SCA warrant, which is issued only on a showing of probable cause. *See* 18 U.S.C. § 2703; *see also* Fed. R. Crim. P. 41(d). Relatedly, the scope of the disclosure required is correlated to the showing the government is required to make; generally, the more invasive the disclosure the government seeks, the higher the evidentiary burden that is required. For example, without prior notification to the account subscriber, a subpoena only permits service providers to disclose basic subscriber and transactional information related to an email account, *see* 18 U.S.C. § 2703(c)(2), while the disclosure of the content of electronic communications requires an SCA warrant. *See* 18 U.S.C. § 2703(a)–(b); *see also Microsoft*, 829 F.3d at 207–08.

The SCA does not specify whether its warrant provisions apply extraterritorially. Rather, the SCA directs that warrants must be "issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction." 18 U.S.C. § 2703(a). For federal SCA warrants, the SCA defines a "court of competent jurisdiction" as a United States district court (including a magistrate judge of such court) or court of appeals that: (1) has jurisdiction over an offense being investigated; (2) is in the service provider's district or is in the district where the electronic records or information at issue is stored; or (3) is acting on a request for foreign assistance under 18 U.S.C. § 3512. *Id.* § 2711(3).

B. The SCA Warrant at Issue

On November 8, 2016, the government submitted an application for a warrant pursuant to section 2703 of the SCA. *See* Application and Affidavit for Search Warrant [Dkt. 1]. The application requested a warrant requiring Google to disclose all electronic records and information associated with a specific Google account, including emails to and from the account. The affidavit in support of the application asserts that there is probable cause to believe that the Google account belongs to the subject of a federal criminal investigation and was used by that subject to facilitate the criminal activity under investigation. The warrant makes no mention of the location of the

Google server or servers on which the records and information the government seeks are stored, calling instead for Google to produce to law enforcement all records and documents associated with the account within the possession, custody, or control of Google's California headquarters. Upon Google's disclosure of that electronic information to law enforcement, the warrant provides that government agents will search it and seize information falling within defined categories relevant to the criminal activity under investigation.

Satisfied with the government's showing of probable cause, the Court issued the warrant on November 8, 2016 and the government served it on Google's Legal Investigations Support ("LIS") team in California that same day. *See* Stip. at ¶ 6.

C. Google's Data Network and Production of Data Pursuant to the Warrant

Google is a California-based company that provides users with online and electronic communication services. Stip. at ¶ 1. Google operates a dynamic "intelligent network" that stores its data on servers located around the world. *Id.* at ¶ 2. The network automatically moves certain data, including the data at issue here, from one server to another "as frequently as needed to optimize for performance, reliability, and other efficiencies." *Id.* at ¶ 4. As counsel for Google explained at oral argument, a Google user has no capacity to control the storage location of their data on the network. Rather, by signing up with Google, users agree to allow Google to access and transfer their data at-will to maintain the efficiency of its services.

Through a process known as "sharding," Google's network automatically breaks down certain types of data, including the type of data at issue here, into component parts (or "shards") and stores these parts on servers in different locations. *Id.* at ¶ 3. Google's network automatically moves these shards of data from one server to another to optimize the network's "performance, reliability and other efficiencies," meaning that a single file—an email, for example—at any given moment may be broken down into several parts and each part may be stored on different servers located around the world. *Id.* at ¶¶ 3–4. Indeed, according to Google's counsel, an email's content, header information, and attachments may be stored on three servers in three different physical locations one day, whether within or outside the United States, and on three different servers the next day. It is possible, therefore, that the location of data responsive to a search warrant may change between the time the warrant is sought from the Court and when it is served on Google. *Id.* at ¶¶ 3–4.

Further, the shards of data are effectively meaningless on their own—for purposes of an SCA warrant, a recognizable file useful to law enforcement may exist only when its component parts are compiled remotely from within Google's California headquarters and then produced to the government pursuant to a warrant. *See In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *13 ("[W]ithout *all* of the shards being collected and put together at once to form the actual digital file, each shard alone is a useless piece of coded gibberish." (emphasis in original)). The only Google personnel who have authority to access the content of communications in order to compile and produce them in response to legal process are located at Google's headquarters in California. *Id.* at ¶ 5.

As a large provider of electronic communication services, Google receives tens of thousands of such legal process requests each year. To accommodate these requests, Google employees have developed a database management tool that can query Google's network for specific data. *Id.* at ¶ 4. Before the *Microsoft* decision, counsel for Google explained, the tool was designed to search Google's global network for information sought in a search warrant. Pre-*Microsoft*, Google would regularly disclose any electronic information and records sought by a properly-issued SCA warrant regardless of where that information was electronically stored. Post-*Microsoft*, however, Google has reconfigured the tool such that it only searches for information stored on servers in its domestic data centers, and "does not report the country in which [any] foreign-stored data is located." *Id.* Accordingly, after the government serves an SCA warrant, a member of Google's LIS team—all of whom work at Google's headquarters in California—must review the warrant and use this tool to run a targeted search of Google's domestic network for responsive information. *See id.* at ¶ 5. After conducting the search, Google's LIS team in California compiles whatever responsive data is stored domestically and produces a copy of it to the government.

Google maintains that it followed this procedure in this case and retrieved and produced to law enforcement the following records in response to the warrant, none of which were stored on servers outside the United States: (1) subscriber information; (2) Google chats; (3) Google Plus profile records; (4) searching and browsing history; and (5) Gmail content (including some attachments) and email header information. *Id.* at ¶ 7. An undetermined number of email attachments that were stored on servers located outside the United States—at least at the moment in time that Google's LIS team conducted its network search in response to the warrant—were not included in the production. *Id.* According to the government, many of these attachments only include a title and a statement explaining that the content of the attachment was not produced because it is stored outside the United States. Mot. at ¶ 16. The government has been unable to determine the location of the servers on which these email attachments are stored, as Google's representatives in California either have refused, or are unable, to provide the government with that information.[3]

[3] In one of the parties' exchanges that occurred prior to the government seeking relief from this Court, a Google representative confirmed that Google withheld responsive records and information based on its reading of the *Microsoft* decision but refused to reveal to the government the location of the server or servers on which the missing information was stored. Mot. at ¶¶ 12–14. Counsel for Google explained at oral argument that Google has no set policy with respect to the latter issue because, at least in part, the tool Google uses to locate customer content responsive to an SCA warrant does not provide Google employees with the information needed to determine foreign data storage locations.

Following Google's final production of responsive material, the government filed its Motion for an Order to Show Cause.

D. The Second Circuit's Decision in *Microsoft*

At the heart of the parties' dispute lies the Second Circuit's decision in *Microsoft*. Some background on that decision would be instructive prior to addressing the merits of the parties' arguments regarding whether it should be followed in this jurisdiction.

In *Microsoft*, the Second Circuit heard an appeal from Microsoft Corporation, a web-based electronic communication service provider, of an order issued in the Southern District of New York denying Microsoft's motion to quash an SCA warrant. *Microsoft*, 829 F.3d at 200. Microsoft sought to quash the warrant because full compliance would have required it to access data that was stored on a server physically located in Ireland. Although the data could be electronically retrieved from the server in Ireland by Microsoft personnel located in the United States, Microsoft declined to produce the data on the Irish server to law enforcement in the United States. *Id.* The district court held the company in contempt of court for refusing to comply with the warrant, and Microsoft appealed. The Second Circuit reversed, reasoning that the SCA did not "envision the application of its warrant provisions overseas." *Id.*

To reach this conclusion, the Second Circuit analyzed the SCA in light of the "strong and binding" presumption against the extraterritorial application of federal statutes articulated by the Supreme Court in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010) and, more recently, in *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090 (2016). *See Microsoft*, 829 F.3d at 209–22. Under the *Morrison* framework, courts must "presume that legislation of Congress 'is meant to apply only within the territorial jurisdiction of the United States,' unless a contrary intent clearly appears." *Id.* at 210 (quoting *Morrison*, 561 U.S. at 255). This presumption is designed, in part, "to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries." *RJR Nabisco, Inc.*, 136 S. Ct. at 2100. Accordingly, the Supreme Court developed a two-step framework for analyzing extraterritoriality issues related to federal statutes. *Id.* at 2101. At the first step, courts "ask whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially." *Id.* If no such indication exists, "then at the second step [courts] determine whether the case involves a domestic application of the statute . . . by looking to the statute's 'focus.'" *Id.* In particular, courts must look to the *conduct* relevant to the statute's focus. If that conduct "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.*; *see also Microsoft*, 829 F.3d at 210.

Following this two-step inquiry, the *Microsoft* court first determined that the relevant statutory provisions of the SCA did not expressly contemplate the statute's extraterritorial application. *Id.* at 210. Proceeding to the second step, the Second Circuit examined the SCA and determined that its "relevant provisions . . . focus on protecting the privacy of the content of a user's stored electronic communications," thereby rejecting the government's argument that its focus was on the "disclosure" of stored electronic information to the government. *Id.* at 216-17. The Second Circuit reasoned that the conduct relevant to that focus—the invasion of the Microsoft customer's privacy—occurred in Ireland, where the information sought by the warrant was located and where Microsoft, "acting as an agent of the government," seized it. *Id.* at 220. For that reason, the Second Circuit concluded that "the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the

United States." *Id.* Accordingly, the Second Circuit found that, "to enforce the [w]arrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the [SCA]." *Id.* at 221.

Notably, Circuit Judge Gerard Lynch issued a concurring opinion in *Microsoft* which was somewhat more ambivalent in its support for the majority opinion. While he expressed his "general agreement with the [panel's] conclusion" he simultaneously emphasized the oddity that its interpretation of the SCA meant that a Microsoft customer's privacy hinges "not on the traditional constitutional safeguard of private communications—judicial oversight of the government's conduct of criminal investigations—but rather on the business decisions of a private corporation" regarding electronic data storage. *Id.* at 222–24 (Lynch, J., concurring). Judge Lynch further described the government's argument that the focus of the SCA is "on the place where the service provider discloses the information to the government" as "quite reasonabl[e]," and explained that the nature of storing electronic information, whereby files are fragmented and dispersed across servers in different locations only to be compiled and viewed again from inside the United States, rendered the panel's decision a "very close case to the extent that the presumption against extraterritoriality shapes [the court's] interpretation of the statute." *Id.* at 229. While acknowledging that the Second Circuit's decision in *Microsoft* should not be "regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy," Judge Lynch nevertheless concurred with the Second Circuit's result, albeit with a recommendation that the government seek congressional revisions of the SCA to "clarify[] the international reach of those provisions after carefully balancing the needs of law enforcement . . . against the interests of other sovereign nations." *Id.* at 233.

The government sought rehearing *en banc* of the *Microsoft* decision, which the Second Circuit denied in a four-four split decision. *See Microsoft II*, 855 F.3d 53, 55 (2d Cir. 2017); *see also* Fed. R. App. P. 35(a) (requiring majority approval of active circuit judges to order rehearing *en banc*).[4] In *Microsoft II*, the prevailing members of the circuit's *en banc* panel reiterated that "the SCA's focus lies on protecting user privacy" and "read the statute to treat the locus of the SCA's privacy protections as the place of data storage," meaning, in that case, Ireland. *Id.* at 55–56. Conversely, the four dissenting judges characterized the statute's focus—or, in some instances, the conduct relevant to the SCA's focus—as the "disclosure" of the information subject to the warrant, which occurs in the United States where the service provider accesses the user's content electronically and provides it to law enforcement. *Id.* at 64–68, 73. As Circuit Judge Jose Cabranes explained in dissent, "[b]ecause the location of a provider's *disclosure* determines whether the SCA is applied domestically or extraterritorially, the enforcement of the warrant . . . involved a domestic application of the SCA." *Id.* at 68 (Cabranes, J., dissenting).

While the government has not yet sought review of the *Microsoft* decision in the Supreme Court, a number of federal courts across the country have confronted the same question following the *en banc* decision. Every court outside the Second Circuit that has considered the issue has rejected the holding of *Microsoft* and has concluded that the disclosure of electronic information accessed within the United States but stored on servers abroad does not implicate extraterritoriality concerns. *See 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. April 25, 2017);[5] *In the Matter of the Search*

[4] Three active Second Circuit judges were recused from participating in the rehearing.

[5] Objections have been filed and are still pending before the respective district court in the Northern District of California. *See* Google's Motion, *Matter of Search of Content that is Stored at Premises Controlled by Google*, Case No. 16-mc-80263-LB (N.D. Cal. May 3, 2017), ECF No. 47.

of Premises Located at [redacted]@yahoo.com, stored at premises owned, maintained, controlled, or operated by Yahoo, Inc., Case No. 6:17-mj-1238 (M.D. Fla. April 7, 2017);[6] *In re Information associated with one Yahoo email address that is stored at premises controlled by Yahoo*, Case No. 17-mj-1234, 17-mj-1235, 2017 WL 706307, at *4 (E.D. Wis. Feb. 21, 2017);[7] *In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *12.[8] This Court is now faced with the same quandary—namely, whether it will compel Google to disclose to United States law enforcement electronic records and information accessible from Google's headquarters in California but potentially stored on Google's servers around the world despite the Second Circuit's decision. A review of the SCA, relevant case law, and the record below establishes that it must.

ANALYSIS

The technological realities of modern electronic data storage have, in many ways, outstripped the traditional legal framework that applies to search warrants. As Circuit Judge Dennis Jacobs observed in *Microsoft II*, "'[t]he very idea of online data being located in a particular physical place is becoming rapidly outdated' because electronic 'files can be fragmented and the underlying data located in many places around the world' such that files 'only exist in recognizable

[6] The undersigned was unable to access the docket in this matter through PACER to determine whether Yahoo has objected to the court's decision.

[7] The court's memorandum and order addressed two cases in which the government submitted an application for a warrant pursuant to 18 U.S.C. § 2703—one involving a Yahoo account and another involving a Google account. In the Google case, Google filed an objection to the magistrate judge's memorandum and order, but the court instructed Google to file a motion to quash the warrant so that the magistrate judge can "assess the propriety of the warrant with the benefit of adversarial argument" before the parties sought review from a district judge. *See* Order at 3, *In re: Two email accounts stored at Google, Inc.*, Case No. 17-mj-1235 (E.D. Wis. March 9, 2017), ECF No. 4. Google then filed a motion to amend the warrant so that it would require Google to produce only data confirmed to be stored in data centers in the United States. *See* Google's Motion, Case No. 17-mj-1235 (E.D. Wis. March 17, 2017), ECF No. 8. That motion is still pending before the court. The undersigned was unable to access the docket through PACER to determine whether Yahoo has objected to the court's memorandum and order in the related case.

[8] Objections have been filed and are still pending before the respective district court in the Eastern District of Pennsylvania. *See* Google's Brief, *In re Search Warrant No. 16-960-M-01 to Google*, Case No. 16-960-M-01 (E.D. Pa. March 10, 2017), ECF 53.

form when they are assembled remotely.'" *Microsoft II*, 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)). This is particularly true when faced with a dynamic data storage network like Google's, which, in addition to fragmenting and dispersing its users' data for storage, automatically relocates those fragments again and again to different servers within the United States and around the world as frequently as needed to optimize the network's performance. In that context, the Second Circuit's suggestion that electronic information is stored and accessible in the same way that paper documents are—that is, in tangible files capable of being located in a single place, taken from that place, and delivered to the United States for seizure by law enforcement—is outdated and not particularly helpful to the analysis.[9]

Fortunately, the issue presented in the instant case does not call for a deep exploration of the interface between modern electronic data storage and traditional Fourth Amendment norms. Rather, it requires the Court to determine, based on the two-part statutory analysis set forth in *Morrison*, whether compelling Google to access and disclose the electronic information sought in the warrant at issue constitutes an unlawful extraterritorial application of the SCA. Echoing many of the arguments raised by the four dissenting judges in *Microsoft II*, the government contends that an order from this Court compelling Google's compliance with the warrant does not result in such an application. *See* Reply at 23–37. Google maintains that it does. *See* Response at 6; Surreply at 10–14. For the reasons that follow, the Court finds that Google's compliance with the warrant is a domestic application of the SCA.

[9] To be clear, "electronic data are not stored on disks in the way that books are stored on shelves or files in cabinets. Electronic 'documents' are literally intangible: when we say they are stored on a disk, we mean they are encoded on it as a pattern." *Microsoft II*, 855 F.3d at 61 (Jacobs, J., dissenting). Accordingly, an SCA warrant is not asking Google "to import and deliver a disk (or anything else)" to law enforcement, but rather "to deliver information that is encoded on a disk in a server" that Google can access and read from the United States. *Id.*

As noted above, assessing whether Google's full compliance with the instant SCA warrant is an extraterritorial application of the statute involves a two-step process prescribed in *Morrison* and *RJR Nabisco*. *Morrison*, 561 U.S. at 265–67; *RJR Nabisco*, 136 S. Ct. at 2101. The Court finds no dispute between the parties at step one of the analysis. Reply at 23–24; Surreply at 10. Having reviewed the statute, the undersigned also finds no basis to challenge the Second Circuit's conclusion in *Microsoft* that the SCA does not expressly apply extraterritorially. *See RJR Nabisco*, 136 S. Ct. at 2100 ("Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application."). [10] Accordingly, the crux of this Court's

[10] Because both parties concede that the SCA lacks extraterritorial application, there is no need to further pursue step one of the *Morrison* analysis. To the extent that the Second Circuit did so in *Microsoft* by engaging in a discussion of the use of the word "warrant" in section 2703, *Microsoft*, 829 F.3d at 210–16, that analysis was superfluous, *see Microsoft II*, 855 F.3d at 79 (Raggi, J., dissenting) ("[T]here was no need for the panel to locate *domestic* intent in the SCA; it is presumed in the absence of a showing of express *extraterritorial* intent, which the government concedes is absent here."). It was also faulty. The panel concludes that Congress' use of the term "warrant" in section 2703 invoked all of the "traditional, domestic connotations" that pertain to a warrant seeking to search and seize physical things, including its "traditional domestic limits." *Microsoft*, 829 F.3d at 213. But that fundamentally misperceives the nature of the legal process involved. As Judge Lynch observed, an SCA warrant is not "a traditional search warrant." *Id.* at 226 (Lynch, J., concurring). By statute, it involves no notice to the account customer or user who is the target of the warrant, and no entry on, or seizure of, private property by government agents. *See* 18 U.S.C. §§ 2703(c)(3), 2703(g). Indeed, "the presence of [a law enforcement] officer [is] not . . . required for service or execution of a search warrant issued in accordance with [the SCA] . . . ." *Id.* at 2703(g). Rather, an SCA warrant is a "procedural mechanism to allow the government to 'require a [service provider] to disclose the contents of [certain] electronic communication[s].'" *Microsoft*, 829 F.3d at 227 (Lynch, J., concurring) (quoting 18 U.S.C. § 2703(b)(1)(A)). Circuit Judge Cabranes expressed well this distinction between traditional warrants and SCA warrants in his dissent from the order denying rehearing *en banc*:

> The panel majority conflates SCA disclosure warrants with traditional search warrants. While the latter authorize government action as to *places*, the former authorize government action on *persons*. The fact that warrants generally do not authorize government searches of places outside the United States—a limitation grounded in respect for sovereignty, not privacy, *see, e.g.*, *The Apollon*, 22 U.S. (9 Wheat.) 362, 371, 6 L.Ed. 111 (1824) (Story, J.); Restatement (Third) of Foreign Relations Law § 432(2); *see also In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 167–72 (2d Cir. 2008)—does not support a conclusion that warrants are impermissibly applied extraterritorially when they compel persons within the United States to disclose property lawfully in their possession anywhere in the world. *Cf. Linde v. Arab Bank, PLC*, 706 F.3d 92, 109 (2d Cir. 2013) (Carney, *J.*) (observing that the Supreme Court has held that "the operation of foreign law 'do[es] not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [law].'" (quoting *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court*, 482 U.S. 522, 544 n. 29, 107 S. Ct. 2542, 96 L.Ed.2d 461 (1987))). In that sense, a disclosure warrant is more akin to a subpoena, *see, e.g.*, *Marc Rich & Co. A.G. v. United States*, 707 F.2d 663, 668–70 (2d Cir. 1983) (holding that persons in the United States can be required to retrieve subpoenaed material from abroad), *but* with the important added protection of a probable cause showing to a neutral magistrate.

analysis will center on the second step of the analysis—that is, whether the conduct relevant to the statute's focus is domestic or extraterritorial in nature. With respect to this step, the Supreme Court instructed in *RJR Nabisco*:

> 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.

RJR Nabisco, 136 S. Ct. 2101.

Turning to that step, the proper focus of the SCA must first be determined. The government contends that the Second Circuit erred when it decided that the focus of the section 2703 warrant provision in the SCA is "privacy," and then erred again when, based on that determination, it concluded that the conduct relevant to that focus would occur in Ireland, where Microsoft was storing the data subject to the warrant. *See* Reply at 23–24. As it did in *Microsoft*, the government argues instead that the relevant focus of section 2703 is the "disclosure" of the information in question to law enforcement and that the conduct relevant to that "disclosure" occurs in the United States, where the service provider produces electronic data to government agents. *Id.* at 23–28. Even assuming that the Second Circuit properly determined that the focus of section 2703 is user privacy, the government continues, it nevertheless erred in failing to find that the disclosure of a user's information to law enforcement is the conduct relevant to that focus, which, again, happens domestically. *Id.* at 26–27.

Microsoft II, 855 F.3d at 65, n.19 (Cabranes, J., dissenting) (emphasis in original); *see also Reinsurance Co. of America, Inc. v. Administratia Asigurarilor de Stat,* 902 F.2d 1275, 1281 (7th Cir. 1990) ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to the its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information . . . is outside the United States.").

Google maintains that the *Microsoft* court correctly found the focus of the SCA—and specifically section 2703 of the SCA—to be user privacy, and the conduct relevant to that focus to occur where the service provider searches its data centers for a user's electronic information. *See* Surreply at 11–14. The service provider's searching of its data centers, Google argues, is critical to the effectiveness of any warrant issued under section 2703 and, thus, cannot be ignored in the *Morrison* analysis. At oral argument, however, Google refused to embrace the Second Circuit's conclusion that a service provider is acting as an agent of the government when it seizes a user's data by accessing and retrieving that data from a foreign data center. *See Microsoft*, 829 F.3d at 220 ("[I]t is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government."). The relationship between the service provider and the government is a secondary concern under the *Morrison* framework, Google contends, because the relevant conduct—the invasion of a user's privacy occasioned by a service provider searching its data centers, wherever they are located, for that user's information—is the same regardless of the nature of that relationship. In other words, Google argues that section 2703 of the SCA "focuses on protecting privacy by regulating the procedures by which the government may infringe upon it," and one such procedure is "the requirement that a warrant be obtained and executed[.]" Surreply at 12. According to Google, "[t]he provider's conduct is literally . . . the conduct the SCA 'seeks to regulate'" in that the provider's searching foreign data bases and accessing data abroad "is a necessary part of executing the warrant and a necessary precondition to the disclosure of customer communications." *Id.*

The Court believes that the best reading of the relevant provision of the SCA is that offered by the government: that the focus of the SCA's warrant provisions—section 2703—is on the disclosure of customer records and information to law enforcement. Indeed, section 2703 is entitled "Required *disclosure* of customer communications or records." 18 U.S.C. § 2703 (emphasis added). Similarly, its text specifically governs the circumstances under which "[a] governmental entity may require the *disclosure* by a provider of electronic communication service of the contents of wire or electronic communications . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure[.]" *Id.* § 2703(a) (emphasis added); *see also* § 2703(b) ("A governmental entity may require a provider of remote computing service to *disclose* the contents of any wire or electronic communication . . . ." (emphasis added)); § 2703(c) ("A governmental entity may require a provider of electronic communication service or remote computing service to *disclose* a record or other information pertaining to a subscriber to or customer of such service . . . ." (emphasis added)).

Though Google is correct that the warrant provisions of the SCA also seek to regulate a service provider's conduct, the most relevant conduct of those sections is not the provider's *accessing* customer data, but rather its *disclosure* of that data to law enforcement. A plain reading of the relevant provisions of the statute confirms as much. Of the three major provisions of the SCA—sections 2701, 2702, and 2703—section 2701 is the only one "to specifically limit *access* to customer communications." *Microsoft II*, 855 F.3d at 67 (Cabranes, J., dissenting) (emphasis in original); *see also* 18 U.S.C. § 2701. And while section 2701 deals with "[u]nlawful access to stored communications" and the concomitant punishments for such conduct, it also "expressly exempts from its restrictions on *access* 'conduct authorized . . . by the person or entity providing a wire or electronic communications service,' i.e., the provider." *Microsoft II*, 855 F.3d at 67 (emphasis in original) (quoting 18 U.S.C. § 2701). Conversely, section 2702, which is entitled "Voluntary disclosure of customer communications or records," and section 2703, which, again, is entitled "Required disclosure of customer communications or records," specifically regulate the circumstances under which a provider may disclose customer content. *See* 18 U.S.C. § 2702(a) (providing prohibitions with which an electronic communication service provider must comply regarding the divulgence of customer communications); *see also* 18 U.S.C. § 2703 (authorizing the government to require the disclosure of the contents of an electronic communication by a service provider under specified circumstances).

Taken together, these provisions of the SCA are thus designed to "protect[] user privacy by prohibiting unlawful access of customer communications (such as hacking), and by regulating a provider's *disclosure* of customer communications to third parties." *Microsoft II*, 855 F.3d at 68 (Cabranes, J., dissenting) (emphasis in original). It is not a coincidence, however, "that the SCA recognizes a provider's standing authority to *access* a user's communications [under section 2701] and, at the same time, prohibits a provider from *disclosing* those communications to third-parties except as authorized by sections 2702 and 2703." *Id.* (emphasis in original). Put differently, Google has always had the right to access its foreign data bases and transfer any data stored abroad to the United States. Where Google stores the data that comprises its customers' communications is an internal business decision made with an eye toward optimizing network efficiency, not a decision based on concern for customer privacy or one controlled by the SCA. The only conduct that would be unlawful absent an SCA warrant—that is, "the object[] of the [relevant provisions'] solicitude"—is Google's disclosure of that data to the government. *Morrison*, 561 U.S. at 267.

To be sure, a service provider's customer's privacy concerns are relevant to section 2703 of the SCA, but those concerns arise only in the context of setting forth the requirements the government must satisfy in order to compel a service provider to disclose the customer's private information. Moreover, privacy does not *occur* anywhere; it "is an abstract concept with no obvious territorial locus[.]" *Microsoft*, 829 F.3d at 230 n.7 (Lynch, J., concurring). It makes little sense, therefore, to view privacy, which is inherently territorially-amorphous, as the territorial focus of the statute as the panel did in *Microsoft*. *See Microsoft II*, 855 F.3d at 61 (Dennis, J., dissenting). Instead, the territorial focus of the statute ought to be the conduct that would otherwise give rise to the infringement of user privacy in the absence of an SCA warrant—the provider's disclosure. Stated differently, while the purpose of the SCA might be aptly described as enhancing privacy for users of electronic communication service providers, the territorial focus of the statute is regulating the instances where customer communications can be disclosed and the conduct relevant to that focus would occur wherever a service provider is disclosing information in a manner that would otherwise infringe a user's privacy rights in the absence of a warrant or other legal process. Here, that happens in the United States, where Google discloses the responsive information in its control to the government pursuant to the warrant. *In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *12 ("When Google produces the electronic data in accordance with the search warrants and the Government views it, the actual invasion of the account holder's privacy—the searches—will occur in the United States."). Thus, whether the focus of the relevant provisions of the SCA is disclosure or privacy is ultimately of little import to the outcome of the *Morrison* analysis. Under either conception, the conduct relevant to the statute's focus occurs in the United States, where the service provider either discloses the customer's data to law enforcement or infringes a customer's privacy by disclosing that data to law enforcement.

Google maintains the opposite, arguing that the relevant conduct here occurs abroad, where the service provider "search[es] for and seiz[es]" the data that constitutes a customer's communications from foreign data centers for domestic production. Surreply at 12. But such a position again fundamentally misunderstands the particular legal process at issue. *See supra* note 10. As both parties seem to recognize, 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. *See* Resp. at 5 n.5; *see also* Reply at 11–12, 32 n.20. In fact, the service provider is not "seizing" the data at all. "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Merely copying a document or taking a photograph of material—both reasonable analogs to the instant case, 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, and the same is true here, at least at the point where Google accesses and copies the user's data. *See Arizona v. Hicks*, 480 U.S. 321 (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."); *see also United States v. Thomas*, 613 F.2d 787, 793 (10th Cir. 1980) ("The agent's act of photocopying, with UPS permission, certain materials before they were repackaged, was not a 'seizure.'"); *In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *9–10 (law enforcement accessing electronic data pursuant to an SCA warrant is not a "seizure" in the traditional sense). Certainly, 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. After all, Google is entitled to access and transfer its users' data within its network at will in accordance with its user agreements and pursuant to 18 U.S.C. § 2701(c). *See In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *9 ("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."). 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. *Id.* at *11.

Google's position is further muddled by its insistence that it does not act as an agent of the government when it accesses its user's data pursuant to an SCA warrant. In *Microsoft*, the finding that the service provider was "acting as an agent of the government" when searching data centers in Ireland was critical to the court's conclusion that a service provider is "seizing" a customer's data and invading that customer's privacy at the data's storage site. *Microsoft*, 829 F. 3d at 220. Google's concession that it acts through its own agency when complying with an SCA warrant thus undermines the Second Circuit's holding in *Microsoft*. But its concession is also well taken. A service provider is not properly viewed as acting as an agent of the government when "seizing"—or, more appropriately, simply accessing—customer content pursuant to an SCA warrant. *See Microsoft II*, 855 F.3d at 72–73 (Raggi, J., dissenting). The cases relied upon by the Second Circuit to establish the contrary principle are inapposite. In those cases, the third party's property seized by the actor to turn over to the federal government was "*not* already in the actor's possession." *Id.* (emphasis in original); *see also id.* at 67 n.30 (Cabranes, J., dissenting); *compare Gambino v. United States*, 275 U.S. 310, 316–17 (1927) (state troopers acted as agents of United States when they searched individual's car and seized liquor found therein without a warrant, based on belief they were required to by federal law), *with Coolidge v. New Hampshire*, 403 U.S. 443, 487-89 (1971) (wife did not act as agent of law enforcement when she produced husband's guns and clothing after law enforcement arrived at their house to question wife). That was not the case in *Microsoft* and is not the case here. The relevant records and information called for by the warrant are already in the Google's possession, custody and control, and it did not need the authorization or agency of the government to lawfully access them.

Finally, it must be said that the above *Morrison* analysis of the operative sections of the SCA has the added benefit of avoiding the bizarre results that application of the *Microsoft* decision to modern data networks like Google's would produce. If that decision's focus on the physical location of the data's storage were to be applied to service providers using such networks, the records and information the government would receive in response to an SCA warrant may differ significantly depending on the date on which the warrant is served. Indeed, the same warrant served on ten different days may well produce ten different results depending on where on the network the shards of responsive data are located at the moment each warrant is served. Such random results—generated by a computer algorithm—would serve the interests of neither privacy nor international comity.

Compounding the problem, even assuming the service provider could and would identify for law enforcement the location of the foreign-based servers on which the missing data was stored (as Google refused to do here), that knowledge would effectively be useless to the government here. By the time the government could initiate the international legal process necessary to obtain the missing data from wherever it was stored, it is entirely possible that the network would have relocated the data yet again to a server in a different country. Moreover, it is Google's position that it need not respond overseas to any such international legal requests because it is only at its headquarters in California that its data can be accessed and compiled into a recognizable electronic file. Thus, in Google's view, the only means available to obtain records and information related to a Google account is by serving an SCA warrant on its LIS team in California. *See In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *13. If Google is correct on that score—a question that would be decided in the first instance by courts outside the United States when Google refuses to produce anything in response to legal process overseas—the application of the *Microsoft* decision to Google SCA warrants would effectively leave law enforcement with no means of obtaining data stored on Google's foreign-based servers. *See Microsoft II,* 855 F.3d at 65 (Cabranes, J., dissenting). And this "Catch-22" would not only obstruct the efforts of law enforcement in the United States, but also the efforts of foreign investigative bodies seeking evidence on Google's servers outside the United States to advance their own investigations. As Google would have it, electronic evidence of crimes stored on its foreign-based servers would be effectively immune from legal process anywhere in the world. These are the kinds of bizarre, impractical outcomes that the Supreme Court has reminded lower courts time and again to avoid whenever possible when interpreting a statute. *See, e.g., American Tobacco Co. v. Patterson,* 456 U.S. 63, 71 (1982) ("Statutes should be interpreted to avoid untenable distinctions and unreasonable results whenever possible.").

CONCLUSION

To reach the conclusion advanced by Google here, the Court would need to find that a properly-issued SCA warrant requiring the disclosure to law enforcement in the United States from Google's headquarters in the United States of digital files accessible only from the United States constitutes an extraterritorial application of the SCA simply because pieces of data that make up those files were stored on a server located outside the United States at the moment in time the warrant was executed. Because such a conclusion runs contrary to the straightforward extraterritorial analysis of the SCA under *Morrison* detailed above, the Court finds that Google has not shown cause for its failure to produce all the records and information called for in the instant warrant within its possession, custody, or control. Google's LIS representatives in California can access, compile, and disclose to the government those records and information with the push of a button and "without ever leaving their desks in the United States." *Microsoft*, 829 F.3d at 229 (Lynch, J., concurring). Because that "entire process takes place domestically," *id.*, Google will be ordered to comply with the warrant in full, and to disclose to the government all responsive electronic records and information identified in Attachment B to the warrant within its possession, custody or control, wherever those records and information may be electronically stored.

An appropriate Order will accompany this Memorandum Opinion.

* * * * * *

The parties are advised that any objections to this Memorandum Opinion and accompanying Order must be filed with the Chief Judge of the United States District Court for the District of Columbia within fourteen (14) days. The failure to file timely objections to the undersigned's Memorandum Opinion and Order may waive the parties' right to review. *See* Fed. R. Crim. P. 59(a); *see also* LCrR 57.14(7).

Date: June 2, 2017

G. MICHAEL HARVEY
United States Magistrate Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [REDACTED]@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, INC.

Case No. 16-mj-757 (GMH)

ORDER

For the reasons stated in the Memorandum Opinion issued contemporaneously herewith, it is, hereby

ORDERED that, no later than fourteen (14) days from the entry of this Order, Google, Inc. shall fully comply with the requirements of the warrant, issued by this Court on November 8, 2016 and disclose to the government all requested records and information identified in Attachment B to the warrant within its possession, custody, or control, wherever those records and information may be electronically stored. It is further

ORDERED that, should Google file a timely objection seeking review of the undersigned's decision, this Order is **STAYED** pending disposition of that objection by the Chief Judge of the United States District Court for the District of Columbia. *See* LCrR 57.14(7).

SO ORDERED.

Date: June 2, 2017

G. MICHAEL HARVEY
United States Magistrate Judge