UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE SEARCH OF INFORMATION ASSOCIATED WITH [REDACTED]@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, INC.	Case No. 16-mj-00757 (BAH) Chief Judge Beryl A. Howell

MEMORANDUM OPINION

In February 2017, the government sought to compel compliance with a warrant issued four months earlier, in November 2016, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) of the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, *et seq.*, requiring Google, Inc. ("Google"), a United States provider of electronic communications services, to disclose to the government the contents of a particular Google account, including emails, as part of an ongoing investigation into fraud, bribery of a public official, and money laundering. *See* Gov't's Mot. for Order Show Cause Why Google Should Not Be Compelled To Comply with Warrant ("Gov't's Mot. OTSC"), at ¶ 20, ECF No. 5; Application for Warrant ("Warrant App."), Ex. 1, Affidavit in Support of Application ("Warrant Aff."), ¶¶ 1, 5, ECF No. 1-1. Following briefing and a hearing, a U.S. Magistrate Judge granted the government's motion and directed Google to comply with the warrant in full. *In the Matter of the Search of Information Associated with [Redacted]@gmail.com that is Stored at Premises Controlled by Google*, Case No. 16-mj-757, 2017 WL 2480752, at *1 (GMH) (D.D.C. June 2, 2017) ("Mem. Op."). Now, nine months after the original warrant was issued, Google objects, pursuant to 28 U.S.C. §§ 636(b)(1)(B),(C) and Local Criminal Rule 59, to the Magistrate Judge's order, averring that the warrant constitutes an unlawful extraterritorial application of the SCA. *See* Google's Objections to Magistrate Order ("Objs."), at 1 ¶ 1, ECF No. 22. For the following reasons, the Magistrate Judge's order is

affirmed to the extent consistent with this Memorandum Opinion and Google is ordered to comply fully with the warrant.

I. BACKGROUND

Summarized briefly below is the procedural history of this matter and a description of Google's storage of electronic communications, including the records and content of communications subject to the warrant at issue.

A. The SCA Warrant

The relevant facts of this case are not in dispute. On November 8, 2016, the government submitted an application for a warrant, under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) of the SCA. *See generally* Warrant App.; Warrant Aff., ¶ 1. The application requested a warrant requiring Google to disclose records and information associated with a particular Google account, including emails. *See* Warrant Aff., ¶ 1; *see also* Gov't Mot. OTSC, Ex. 1, Search Warrant, Attachs. A ("Property to be Searched") and B ("Particular Things to Be Seized and Procedures to Facilitate Execution of the Warrant"). In an affidavit supporting the application, the government asserted 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. Warrant Aff., ¶ 5; *see* Gov't Opp'n to Objs. ("Gov't Opp'n"), at 3, ECF No. 25. The warrant ordered Google to disclose to the government, among other things, all emails and email attachments in the account. That same day, on November 8, 2016, the Magistrate Judge, "[s]atisfied with the government's showing of probable cause," Mem. Op., 2017 WL 2480752, at *3, issued the warrant and the government served it on Google's Legal Investigations Support ("LIS") team that day, Factual Stipulation by the Parties ("Stip.") ¶ 6, ECF No. 16.

B. Google's Response to Warrant

In response to the warrant, Google states it "undertook diligent efforts to identify and produce responsive information that could be determined to be located in the United States." Stip. ¶ 7.[1] For the particular target account, Google produced subscriber information, chats, "Google Plus" profile records, search and browsing history, and certain Gmail content (including attachments and headers), but did not produce attachments to emails if those "documents were determined to be stored on servers located outside the United States." *Id.* In declining to comply fully with the warrant, Google relied on the Second Circuit's opinion in *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.* (*"Microsoft I"*), 829 F.3d 197 (2d Cir. 2016), *reh'g denied*, 855 F.3d 53 (2d Cir. 2017), which held that a warrant issued under the SCA cannot compel a service provider subject to the SCA, such as Google, to disclose information the provider stores abroad because such disclosure would constitute an unlawful extraterritorial application of the SCA.

On February 27, 2017, the government filed a Motion for an Order to Show Cause why Google Should Not be Compelled to Comply with Warrant. *See* Gov't's Mot. OTSC. The Magistrate Judge issued the Order to Show Cause on February 28, 2017, and Google filed a response in opposition on March 14, 2017. *See* Order to Show Cause, ECF No. 6; Google's Resp. to Order to Show Cause ("Google's Resp."), ECF No. 7. Following briefing and oral argument, the Magistrate Judge issued, on June 2, 2017, an Order granting the government's motion to compel compliance with the Warrant. In doing so, the Magistrate Judge expressly declined to follow *Microsoft*, reasoning that the warrant was a domestic application of the SCA. Mem. Op., 2017 WL 2480752, at *8–9.

[1] Initially, Google produced information with respect to the wrong account and, at Google's Request, the government destroyed this production. Google's Resp. at 2.

On June 19, 2017, Google timely filed objections to the Magistrate Judge's Order, primarily asserting that the Magistrate Judge improperly applied the Supreme Court's framework for determining whether the conduct in question constitutes an extraterritorial application of a statute, as set forth in *Morrison v. Nat'l Australia Bank, Ltd.*, 561 U.S. 247 (2010), and *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016). *See generally* Objs. at 1–3, 11–15. Following voluminous briefing that exceeded the page limits otherwise applicable under the Local Rules of this Court, these objections became ripe for review on July 10, 2017.

C. Google's Network

Google is a U.S.-headquartered company with its principal place of business in California that, among other things, offers "a variety of different online and communications services." Stip. ¶ 1. Google stores electronic communications on a dynamic network, using servers located both in the United States and abroad, *id.* ¶ 2, and "operates a state-of-the-art intelligent network that . . . automatically moves data from one location on Google's network to another as frequently as needed to optimize for performance, reliability, and other efficiencies," *id.* ¶ 4. In other words, specific customer communications, including emails, are frequently moved among Google's servers such that the network may "change the location of data between the time when the legal process is sought and when it is served." *Id.* Further complicating the location of stored records and electronic communications on Google's network, "[s]ome user files may also be broken into component parts, and different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time." *Id.* ¶ 3.

II. STANDARD OF REVIEW

As a threshold matter, the proper legal standard must be determined for review by a district court of a magistrate judge's decision to grant a motion to compel compliance with an

SCA warrant. This standard is not obviously clear from the Federal Magistrates Act, the Federal Rules of Criminal Procedure, or the Local Criminal Rules of this Court.

The Federal Magistrates Act distinguishes between two primary categories of matters that a district judge may *refer* to a magistrate judge. Under 28 U.S.C. § 636(b)(1)(A), a district judge may refer to a magistrate judge for determination any pretrial matter, except for eight specified types of dispositive motions.[2] Subsection (b)(1)(A) is mirrored in the Federal Rules of Criminal Procedure by Rule 59(a), captioned "Nondispositive Matters," and in the Local Rules for the District of the District of Columbia by Local Criminal Rule 59.1. In addition, under § 636(b)(1)(B), a district judge may refer a matter to a magistrate judge to conduct hearings, including evidentiary hearings, and to submit to the court proposed findings of fact and recommendations for the disposition of the "excepted" motions in § 636(b)(1)(A), as well as prisoner applications for post-trial relief or challenging conditions of confinement. Subsection (b)(1)(B) is mirrored in Federal Rule of Criminal Procedure 59(b), captioned "Dispositive Matters," and in Local Criminal Rule 59.2.

These two sections of the Federal Magistrates Act expressly provide for two different standards of review. Under § 636(b)(1)(A), Federal Rule 59(a), and Local Rule 59.1, a district judge may review a magistrate judge's nondispositive pretrial order for whether it is "clearly erroneous or contrary to law."[3] In contrast, under § 636(b)(1)(B), Federal Rule 59(b)(2), and

---

[2] The eight excepted pretrial motions not authorized for referral to a magistrate judge for final determination are motions for: (1) injunctive relief, (2) judgment on the pleadings (3) for summary judgment; (4) to dismiss or quash an indictment or information by a defendant; (5) to suppress evidence in a criminal case; (6) to dismiss or permit maintenance of a class action; (7) to dismiss a claim for failure to state a claim; and (8) to involuntarily dismiss an action. *See* 28 U.S.C. § 636(b)(1)(A).

[3] Magistrate judge orders issued under the SCA in unassigned matters have occasionally been reviewed in this Court as pretrial matters governed by § 636(b)(1)(A) of the Federal Magistrates Act and therefore subject to the standard of "clearly erroneous or contrary to the law." *See, e.g., United States v. All Wire Transactions Involving Dandong Zhicheng Metallic Material Co*., 2017 U.S. Dist. LEXIS 105287, 6-7 (D.D.C. May 22, 2017) (Howell, Chief Judge); *In re Search of Info. Associated with @mac.com that is Stored at Premises Controlled by Apple, Inc*., 13 F. Supp. 3d 157, 162 (D.D.C. 2014) (Roberts, Chief Judge); *In re Search of Info. Associated with @mac.com that*

Local Rule 59.2, a district judge reviews *de novo* only those portions of the magistrate judge's report or recommendation to which objection is made. In other words, whereas a magistrate judge's resolution of nondispositive matters is subject to a deferential standard of review, a magistrate judge may only make recommendations, subject to *de novo* review of portions to which objection is lodged, with respect to dispositive motions. The concomitant level of review for these two sections is rooted in "[c]onstitutional concerns," specifically the "possible . . . objection that only an article III judge may ultimately determine the litigation." *Baylor v. Mitchell Rubenstein & Assocs., P.C.*, 857 F.3d 939, 945 (D.C. Cir. 2017) (citing 12 CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 3068.2 (3d ed. 2014)), and reflects Congress's desire that the *district court* makes the "ultimate determination" of dispositive matters, H.R. Rep. No. 94-1609, at 12 (1976), *reprinted in* 1976 U.S.C.C.A.N. 6162, 6162–63.

These two sections are not exhaustive, however. Under § 636(b)(3), "[a] magistrate judge may be assigned such additional duties as are not inconsistent with the Constitution and laws of the United States." Congress adopted this provision to "enable . . . the district courts to continue innovative experimentations in the use of" magistrate judges. H.R. Rep. No. 94-1609, at 12 (1976), *reprinted in* 1976 U.S.C.C.A.N. 6162, 6172. As the matter before this Magistrate Judge was not "referred" by a district court judge within the meaning of § 636(b)(1)(A) or § 636(b)(1)(B), the order granting the government's motion to compel compliance with the SCA warrant is best understood as an exercise of the magistrate judge's "additional duties"

is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 162 (D.D.C. 2014) (Roberts, Chief Judge). This Court now clarifies that these types of pretrial orders in unassigned matters actually fall under a different provision of the Federal Magistrates Act and are subject to *de novo* review. *See In re Order of Nondisclosure*, 45 F. Supp. 3d 1, 5 (D.D.C. 2014) (finding that challenge to magistrate order regarding government's application for an order under SCA's § 2705(b) is subject to § 636(b)(3) of the Federal Magistrates Act and *de novo* review) (Roberts, Chief Judge); *In re United States*, 41 F. Supp. 3d 1, 4-5 (D.D.C. 2014) (same).

jurisdiction pursuant to § 636(b)(3), in conjunction with this Court's Local Criminal Rule 57.17(a), under which magistrate judges are granted the "duty" and the "power" to "issue search warrants" as well as "[i]ssue subpoenas . . . or other orders necessary to obtain the presence of parties or witnesses or evidence needed for court proceedings." LCrR 57.17(a)(3),(a)(10).[4]

Unlike § 636(b)(1)(A) or (b)(1)(B), however, § 636(b)(3) does not specify procedures for objecting to a magistrate judge's action pursuant to this authority nor does it provide a standard of review. The Federal and Local Rules are also silent on the matter, with the Local Rules providing only that the Chief Judge "shall . . . hear and determine requests for review of rulings by magistrate judges in criminal cases not already assigned to a judge of the Court." LCrR 57.14(7). Although the Magistrate Judge cited Federal Rule of Criminal Procedure 59(a) as authority for Google to file objections, *see* Mem. Op., 2017 WL 2480752, at *11, which Rule would trigger application of a "contrary to law or clearly erroneous" review standard for nondispositive motions under § 636(b)(1)(A), the instant matter has not been "already assigned to a judge of the Court." Consequently, this matter falls within the scope of Local Criminal Rule 57.14(17) and § 636(b)(3), and Google's objections are construed as a "request for review" of the Magistrate Judge's decision.

This still leaves the "standard of review" question unanswered.[5] Some courts have determined that the appropriate standard of review for a matter under § 636(b)(3) should be the

[4] These duties and powers are among the "general duties" of magistrate judges and are contrasted from "powers exercised upon *referral* from a district judge," the latter of which are governed by Local Criminal Rule 57.17(b). *Compare* LCrR 57.17(a) *with* LCrR 57.17(b) (emphasis added).

[5] Although the parties agree that the standard of review should be *de novo*, they disagree on the basis for this determination. Google objects to the Magistrate Judge's apparent intimation that the ruling was on a nondispositive motion under Rule 59(a), *see* Objections at 3, 8, and instead asserts that the "magistrate judge's ruling on the government's motion to compel resolved all of the issues in dispute in this matter, and as such is a dispositive ruling on its merits," under § 636(b)(1)(B). In the alternative, however, Google agrees with the government that even if the magistrate judge's decision were a nondispositive ruling, the Court should still review the decision *de novo* because "Google's objections turn on a question of law." Objections at 8. Indeed, under the "contrary to law" standard, the court must "review the magistrate judge's legal conclusions—including any asserted misapplication of the relevant

same as the two standards under § 636(b)(1)(A) or § 636(b)(1)(B) depending on the *kind* of matter adjudicated. *See N.L.R.B. v. Frazier*, 966 F.2d 812, 816 (3d Cir. 1992); *see also Oliver v. Weeks Marine, Inc.*, Civil No. 10-796, 2013 WL 4433432, at *1 (E.D. La. Aug. 15, 2013) (adopting the *Frazier* standard); *Fuddruckers, Inc. v. KCOB I, LLC*, 31 F. Supp. 2d 1274, 1276 & n.1 (D. Kan. 1998). With this approach, "[i]f the matter referred were more akin to a pretrial motion, the district court should review using the clearly erroneous or contrary to law standard," whereas, "if the matter referred more closely resembles one of the eight excepted motions [of § 636(b)(1)(A)], the district court should employ *de novo* review." *Frazier*, 966 F.2d at 816. The majority of courts to consider the issue, however, have held that the exercise of a magistrate judge's powers under § 636(b)(3) are accorded *de novo* review. *See, e.g., In re U.S. for an Order Pursuant to 18 U.S.C. Section 2703(D)*, 707 F.3d 283, 289 (4th Cir. 2013); *Colorado Bldg. & Const. Trades Council v. B.B. Andersen Const. Co.*, 879 F.2d 809, 811 (10th Cir. 1989) ("[W]e have consistently recognized that '[a] magistrate exercising 'additional duties' jurisdiction remains constantly subject to the inherent supervisory power of the district judge and the judge retains the 'ultimate responsibility for decision making in every instance.'" (quoting *Harding v. Kurco, Inc.*, 603 F.2d 813, 814 (10th Cir. 1979) (quoting *Mathews v. Weber*, 423 U.S. 261, 270 (1976))); *United States v. Peacock*, 761 F.2d 1313, 1318 (9th Cir. 1985) ("Although section 636(b)(3) contains no explicit statement regarding the availability of review by an Article III

statutes, case law, and rules of procedure—*de novo*." *United States v. All Assets Held at Bank Julius, Baer & Co., Ltd.*, Civil No. 04-0798 (PLF), 2017 WL 456376, at *4 (D.D.C. Feb. 2, 2017) (citing *Intex Recreation Corp. v. Team Worldwide Corp.*, 42 F. Supp. 3d 80, 86 (D.D.C. 2013)); *accord Nunnally v. D.C.*, Civil No. 08-1464 (PLF), 2017 WL 1080900, at *2 (D.D.C. Mar. 22, 2017); *Payne v. District of Columbia*, 859 F. Supp. 2d 125, 131 (D.D.C. 2012) (a "magistrate judge's legal conclusions are reviewed *de novo*"); *Am. Center for Civ. Justice v. Ambush*, 794 F.Supp.2d 123, 129 (D.D.C. 2011); *First Am. Corp. v. Al–Nahyan*, 2 F. Supp. 2d 58, 60 (D.D.C. 1998); *see also Haines v. Liggett Group Inc.*, 975 F.2d 81, 91 (3d Cir. 1992) ("[T]he phrase 'contrary to law' indicates plenary review as to matters of law."). For the reasons stated above, however, the magistrate judge's decision in this case does not fall under § 636(b)(1)(A) or § 636(b)(1)(B), but instead falls under § 636(b)(3). In any event, the end result is the same, because the decision must be reviewed *de novo*.

judge, we have determined that the referral of matters to a magistrate pursuant to this section does not offend the Constitution so long as de novo review is available in the district court."). The reasoning underlying the latter view is the most persuasive.

In *Mathews v. Weber*, 423 U.S. 261 (1976), the Supreme Court made clear that under a prior version of § 636, which like § 636(b)(3) authorized magistrate judges to have any "additional duties as are not inconsistent with the constitution and laws of the United States," the district judge "remains free to give the magistrate's recommendation whatever weight the judge decides it merits." 423 U.S. at 273. As the Fourth Circuit has held, this low level of deference is most akin to *de novo* review. *See Matter of Application & Affidavit for a Search Warrant*, 923 F.2d 324, 326 n.2 (4th Cir. 1991) (citing *Mathews*, 423 U.S. at 273). This accords with the view of the Supreme Court that a "magistrate acts subsidiary to and only in aid of the district court" and "the entire process takes place under the district court's total control and jurisdiction." *United States v. Raddatz*, 447 U.S. 667, 681 (1980). In other words, when exercising their "additional duties" jurisdiction pursuant to § 636(b)(3), magistrate judges are "continuously subject to the inherent supervisory control of the district judge who retains ultimate decisional responsibility in every case." *United States v. Southern Tanks, Inc.*, 619 F.2d 54, 55 (10th Cir. 1980); *Bruno v. Hamilton*, 521 F.2d 114, 116 (8th Cir. 1975) (district court retains "inherent power to review final decision of its magistrates except in situations by statute or valid court rule the magistrate is empowered to make final disposition."). Accordingly, because this case arises out of the Magistrate Judge's "additional duties" jurisdiction pursuant to § 636(b)(3), the Magistrate Judge's order is subject to *de novo* review by the district court.

III. DISCUSSION

The primary question posed by this case is whether the conduct at issue—the execution

of an SCA warrant for customer records and electronic communications stored on Google servers located abroad—constitutes an unlawful extraterritorial application of the SCA. As noted and discussed in more detail below, in *Microsoft*, the Second Circuit held in analogous circumstances that such a warrant is an unlawful extraterritorial application of the SCA. *See generally Microsoft I*, 829 F.3d 197 (2d. Cir. 2016). In contrast, every other court to consider the issue, including this Court's Magistrate Judge, has resolved this question differently and rejected the holding of *Microsoft*. *See, e.g.*, *In re Search of Content that is Stored at Premises Controlled by Google*, Case No. 16-mc-80263, 2017 WL 1487625 (N.D. Cal. April 25, 2017);[6] *In re Search of Premises Located at [redacted]@yahoo.com, stored at premises owned, maintained, controlled or operated by Yahoo, Inc.*, Case No. 17-mj-1238 (M.D. Fla. April 7, 2017); *In re Information associated with one Yahoo email address that is stored at premises controlled by Yahoo*, Case Nos. 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*, Case Nos 16-mj-960-M-01, 16-mj-1061-M, 2017 WL 471564, at *12 (E.D. Pa. Feb. 3, 2017).[8] For the reasons that follow, the *Microsoft* court erred: an SCA warrant that seeks records or the content of electronic communications from a U.S.-based service provider does not amount to an extraterritorial application of the SCA, even

---

[6] Objections have been filed and are pending before the 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.

[7] The Eastern District of Wisconsin Court's Memorandum and Order dealt with two government requests for SCA warrants under § 2703, one of which requests involved a Google account. Google filed objections, but the court ordered Google to first file a motion to quash the warrant so that the magistrate judge could "assess the propriety of the warrant with the benefit of adversarial argument." 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 subsequently filed a motion to amend the warrant to require only electronic communications stored on servers located in the United States. *See* Google's Mot. Amend Warrant, Case No. 17-mj.1235 (E.D. Wis. March 17, 2017), ECF No. 8. On June 30, 2017, the Magistrate Judge denied Google's motion by written order, *see* Order, Case No. 17-mj-1235 (E.D. Wis. June 30, 2017). Google's objections to the magistrate judge's order, *see* Google's Objections, Case No. 17-mj-1235 (E.D. Wis. July 14, 2017), are pending.

[8] Objections have been filed and are pending before the district court for 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. Mar. 10, 2017), ECF No. 53.

when the targeted information, in whole or in part, may be stored on servers abroad. Basic notions of enforcement jurisdiction combined with the plain language of the statute, confirm that a court with jurisdiction over the offense being investigated, or in the same district where the service provider or the information being sought is located, *see* 18 U.S.C. § 2711(3)(A) (SCA definition of "court of competent jurisdiction"), may issue an SCA warrant to compel a U.S.-based service provider to retrieve user information stored on the provider's servers located abroad, provided the government has sufficiently supported its application with probable cause.

Google's specific objections raised here are assessed following review of the relevant statutory language, the *Microsoft* decision and the Magistrate Judge's decision in this matter.

A. Statutory Framework

In 1986, Congress enacted the SCA as part of the Electronic Communications Privacy Act ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986).[9] The SCA regulates how stored wire and electronic communications may be lawfully accessed or disclosed. Among other things, the SCA's § 2703, permits the government, in specified circumstances, to compel service providers to disclose records or information pertaining to their customers as well as the contents of their customers' stored electronic communications.[10] This provision's framework provides a sliding

[9] ECPA is comprised of three titles: Title I "addresses the interception of wire, oral and electronic communications," amending the existing chapter 119 of title 18 "to bring it in line with technological developments and changes in the structure of the telecommunications industry"; Title II is the SCA, at issue in this matter; Title III "addresses pen register and trap and trace devices," requiring government entities to obtain a court order authorizing their installation. S. Rep. 99-541, at 3, *reprinted at* 1986 U.S.C.C.A.N. 3555, 3557; *see generally* ECPA, Pub. L. No. 99-508, 100 Stat. 1848 (1986). Title I is codified in chapter 119 of Title 18, at 18 U.S.C. §§ 2510-22; Title II is codified in chapter 121 of Title 18, at 18 U.S.C. §§ 2701–12; and Title III is codified in chapter 206 of Title 18, at 18 U.S.C. §§ 3121-3127.

[10] The SCA provides protections for electronic communications stored by two kinds of service providers: "electronic communication services" ("ECS") and "remote computing services" ("RCS"). The statute defines ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications," 18 U.S.C. § 2510(15), a category of provider generally understood to refer to "telephone companies and electronic mail companies," Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It ("User's Guide")*, 72 GEO. WASH. L. REV. 1208, 1243 n.38 (2004) (citing S. Rep. No. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. at 3568). RCS, by contrast, is defined as "the provision in the public of computer storage or processing services by means of an electronic communications system," *id.* § 2711(2), with the term

scale of protections, such that the legal mechanism law enforcement utilizes and showing required depends on the kind of information sought. In other words, "[t]he rules for compelled disclosure operate like an upside-down pyramid. . . . The higher up the pyramid you go, the more information the government can obtain." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It ("User's Guide")*, 72 GEO. WASH. L. REV. 1208, 1222 (2004).

First, the SCA authorizes the government, when using an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena," to require a service provider "to disclose" the following information: basic subscriber account information, *id.* § 2703(c)(2);[11] unopened emails in electronic storage with a provider for more than 180 days, *id.* § 2703(a), (b)(1)(B)(i); and any opened emails in electronic storage with a provider, regardless of age, *id.* § 2703(b)(1)(B)(i).[12] The SCA imposes no requirement that the

---

"electronic communications system" further defined to mean "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the *electronic storage* of such communications," *id.* § 2510(14)(emphasis supplied). The term "electronic storage" means "any temporary, intermediate storage of a wire or electronic communication incident to the electronic transmission thereof," *id.* § 2510(17)(A), including any storage "for purposes of backup protection of such communication," *id.* § 2510(17)(B). With technological advances since enactment of ECPA and the SCA, the difference between ECS and RCS has eroded because "most network service providers are multifunctional" and "[t]hey can act as providers of ECS in some contexts, providers of RCS in some contexts, and as neither in some contexts as well." Kerr, *User's Guide*, 72 GEO. WASH. L. REV. at 1215; *see also In re Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to not Disclose the Existence of the Search Warrant* ("*In re United States*"), 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) ("Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself.").

[11] Basic "subscriber" or "customer" account information includes the "name," "address," "local and long distance telephone connection records, or records of session times and durations," "length of service (including start date) and types of service utilized," "telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address," and "means and source of payment for such service (including any credit card or bank account number)." 18 U.S.C. § 2703(c)(2)(A)–(F). When seeking this kind of information, the government is "not required to provide notice to a subscriber or customer." *Id.* § 2703(c)(3). The government's access to this kind of information is not at issue in this matter since Google has already complied with this part of the warrant.

[12] The distinction between "opened" and "unopened" emails is due to the interpretation of the term "electronic storage," which determines whether the content is subject to rules for a provider of ECS, 18 U.S.C. § 2703(a), or those for a provider of RCS, 18 U.S.C. § 2703(b). Section 2703(a) states that "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic

issuance of such a subpoena be supported by any articulation of probable cause or even reasonable suspicion, but "prior notice from the governmental entity to the subscriber or customer" is required when the subpoena compels the production of content. *Id.* § 2703(b)(1)(B).[13] That said, the government may apply for a court order authorizing the government to delay notice to the customer for definite periods up to ninety days, under § 2705(a), as well as, precluding the service provider from disclosing to the subscriber the existence of government demand for the records or electronic communication, under § 2705(b). *See* 18 U.S.C. §§ 2705(a)(1),(b). In order to obtain such a § 2705 order, the government must show that disclosure to the subscriber could result in "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(a)(1),(2)(A)–(E).[14]

Second, the SCA authorizes the government, when using a court order, pursuant to § 2703(d) ("§ 2703(d) order"), to require "disclosure" of the same records and stored electronic communications covered by a subpoena, plus "other information pertaining to a subscriber," *id.*

---

communication . . . that is in *electronic storage* in an electronic communications system . . . ." 18 U.S.C. § 2703(a) (emphasis added); *see supr*a, n.10 (discussing definition of term "electronic storage" provided in 18 U.S.C. § 2510(17)). An email has been deemed no longer in "electronic storage" after opening by the recipient. *See, e.g.*, *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); *United States v. Weaver*, 636 F. Supp. 2d 769, 771–73 (C.D. Ill. 2009); *see also* Kerr, *User's Guide*, 72 GEO. WASH. L. REV. at 1216 ("The traditional understanding has been that a copy of an opened e-mail sitting on a server is protected by the RCS rules, not the ECS rules"); *but see Theofel v. Farley-Jones*, 359 F.3d 1066, 1076–77 (9th Cir. 2004) (stating that an email is no longer in electronic storage if "the underlying message has expired in the normal course" and that "prior access is irrelevant to whether the messages at issue were in electronic storage.").

[13] Although unresolved in this Circuit, the Sixth Circuit has held that the Fourth Amendment applies to the contents of emails and thus that a warrant, issued upon probable cause, is required to search or seize those communications. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (concluding the Fourth Amendment protects the contents of emails based on a user's reasonable expectation of privacy). The Sixth Circuit appears to be the only Circuit that has so held. The Supreme Court came close to addressing the matter in *Riley v. California*, 134 S. Ct. 2473 (2014), which held that, in the context of a search incident to arrest, "officers must generally secure a warrant before conducting" a search "of data on cell phones." 134 S. Ct. at 2485. In any event, the policy of the Department of Justice since 2013 has been to use SCA warrants exclusively when compelling the disclosure of the contents of electronic communications. *See* H.R. Rep. No. 114-528, at 9 (2016).

[14] Extensions of the delayed notice may also be granted. *See* 18 U.S.C. § 2705(a)(4).

§ 2703(c)(1), "such as logs maintained by a network server," Kerr, *User's Guide*, 72 GEO. WASH. L. REV. at 1219. A § 2703(d) order may be issued only where the government provides a court with "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d). Again, the government is not required to provide notice if the government is seeking access to non-content records, *see* 18 U.S.C. § 2703(c)(3), but as with use of a subpoena, when a § 2703(d) order is used to access the content of electronic communications the SCA requires the government to provide prior notice to the subscriber or customer, *id.* § 2703(b)(B), subject to the same delayed notification provisions of § 2705.

Finally, the SCA authorizes the government, when using a "warrant" (an "SCA warrant"), pursuant to § 2703(a), (b)(1)(A) and (c)(1)(A), to "require the disclosure" by a service provider of any records subject to production under a § 2703(d) order as well as contents of communications in electronic storage with a provider for fewer than 181 days. *Id.* § 2703(a). Thus, an SCA warrant enables the government to obtain all email communications in a particular account and all related records. *Id.* § 2703(b)(1)(A). An SCA warrant, however, may only be "issued using the procedures described in Federal Rules of Criminal Procedure." *Id.* § 2703(a), (b)(A), (c)(A). The applicable *procedures* are those found in Federal Rule of Criminal Procedure 41, which, for example, in subsection (d), titled "Obtaining a Warrant," requires a judicial finding of probable cause based on sworn testimony or an affidavit, FED. R. CRIM. P. 41(d), and in subsection (e), titled "Issuing the Warrant," authorizes the "the seizure or copying of electronically stored information" with "later review of the media or information consistent with the warrant," FED. R. CRIM. P. 41(e)(2)(B).[15]

[15] The SCA warrant is subject to differing "notice" requirements depending on how long the electronic communication is in storage, based on the distinction made between recent and older emails in § 2703(a).

B. The *Microsoft* Decision

The *Microsoft* case addressed the use of an SCA warrant, issued in the Southern District of New York, for the content of emails and other materials in a Microsoft user's account. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 467–68 (S.D.N.Y. 2014), *aff'd*, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014), *rev'd*, 829 F.3d 197 (2d. Cir. 2016), *reh'g denied*, 855 F.3d 53 (2d Cir. 2017). Although Microsoft produced some of its customer's non-content information stored in the United States, the company moved to quash the SCA warrant with respect to the content of the user's emails, which Microsoft stored in a data center in Ireland. *Microsoft*, 15 F. Supp. 3d at 468. According to Microsoft, an SCA warrant was akin to a traditional search warrant and could not be applied extraterritorially to data located abroad. *Id.* at 470.

Specifically, § 2703(a) authorizes use of an SCA warrant for recent electronic communications stored for 180 days or less but directs that disclosure of emails older than 180 days is governed by § 2703(b)(1)(A). *See* 18 U.S.C. §§ 2703(a),(b)(1)(A). The SCA further expressly provides that the latter, older emails may be obtained "without required notice to the subscriber," *id*. at § 2703(b)(1)(A); *see also* FED. R. CRIM. P. 41(f)(3) (authorizing on government request, "delay [of] any notice required by this rule if the delay is authorized by statute"), but is otherwise silent regarding whether notice to the customer is required when recent emails are disclosed to the government, pursuant to an SCA warrant issued under § 2703(a), leaving this issue to be resolved by reference to "the procedures described in" Federal Rule of Criminal Procedure 41, *id*. at § 2703(a). Notably, the delayed notice authorities of § 2705 do not apply to SCA warrants issued pursuant to § 2703(a). *See id.* § 2705(a)(1) (providing that authority to seek delayed notice applies only to "governmental entity acting under section 2703(b) . . ."). In considering application of Rule 41's notice requirements to SCA warrants for recent emails, one court determined that, assuming the Fourth Amendment applied to electronic communications, any constitutional notice requirement was met by providing notice to the third party in possession of the communications, and that the service of the warrant on the service provider satisfied the notice requirement of Rule 41(f)(1)(C), without imposing any requirement on the government to notify the customer, similar to the express relief from notice provided in § 2703(b)(1)(A). *In re United States*, 685 F. Supp. 2d 1210, 1221-24 (D. Or. 2009). This reasoning does not answer the question, however, of whether a § 2705(b) order precluding the *service provider* from notifying the customer is available to the government when using an SCA warrant under § 2703(a), since use of a § 2705(b) order is expressly limited to when either the government "is not required to notify the subscriber or customer under section 2703(b)(1)" or where "it may delay such notice pursuant to" § 2705(a), neither of which circumstance applies to SCA warrants for recent emails under § 2703(a). The Court need not reach this question—or the question of whether other authorities are available to the government to preclude a service provider from disclosing an SCA warrant for recent electronic communications under § 2703(a) to a subscriber or customer—as this issue is not raised by the parties here.

After unsuccessfully seeking to quash the SCA warrant before the magistrate judge and district court, Microsoft appealed to the Second Circuit, which reversed the order denying Microsoft's motion to quash. The Second Circuit's panel applied the two-step framework for assessing whether the conduct in question is an extraterritorial application of the statute, as set forth in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 261–65 (2010), and *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2100–01 (2016). *See Microsoft I*, 829 F.3d at 209. The panel first assessed whether Congress expressly intended § 2703's disclosure provision to apply extraterritorially. *Id.* at 210. Although both Microsoft and the government conceded the SCA did not apply extraterritorially, the Second Circuit engaged in a discussion of the use of the word "warrant" in § 2703, reasoning that this term carried with it all the "traditional, domestic connotations" of ordinary warrants authorizing searches and seizures of physical items. *Id.* at 212–13. Based on this discussion, the panel concluded that Congress did not intend the SCA to apply extraterritorially. *Id.*

Turning to the second "step" under *Morrison* and *RJR Nabisco*, the panel evaluated whether "domestic contacts" were the "focus" of the SCA or "the objects of the statute's solicitude," or whether they were "merely secondary." *Id.* at 216–17. In determining the "focus" of the relevant statutory provision, the panel relied on "the familiar tools of statutory interpretation," including the "text and plain meaning of the statute, . . . as well as its framework procedural aspects, and legislative history." *Id.* at 217 (internal citation omitted). Based on its analysis of the SCA's "warrant" provisions, the panel found the "most natural reading . . . suggests a legislative focus on the privacy of stored communications," citing the requirement that an SCA warrant comply with the Federal Rules of Criminal Procedure, "whose Rule 41 is undergirded by the Constitution's protections of citizens' privacy," *id.*; the fact that

"§ 2703's warrant language appears in a statute entitled the Electronic Communications Privacy Act." *id.*; and that the first two provisions of the SCA, §§ 2701 and 2702, address protection of communications content, *id.* at 218. The panel also cited the statute's legislative history as supporting the finding that "privacy" is the "focus" of the SCA because, when enacting the SCA, Congress "expressed a concern that developments in technology could erode the privacy interest that Americans traditionally enjoyed in their records and communications." *Id.* Further, Congress was aware at the time that the actions of private parties in electronic communications were "largely unregulated" and that "recent Supreme Court precedent called into question the breadth of the protection to which electronic records and communications might be entitled under the Fourth Amendment." *Id.* (citing S. Rep. No. 99–541, at 3 (citing *United States v. Miller*, 425 U.S. 435 (1976))).

The panel rejected the government's argument that the SCA's warrant provision focuses on "disclosure" rather than "privacy." *Id.* As support for that argument, the government pointed to the SCA's authorization for the government to obtain, by subpoena, the content of emails that have been held by an ECS for more than 180 days, *id.*; *see* § 2703(a), explaining that "reading the SCA's warrant provisions to focus on the privacy of stored communications instead of disclosure would anomalously place newer e-mail content stored on foreign servers beyond the reach of the statute entirely, while older e-mail content stored on foreign servers could be obtained simply by subpoena, if notice is given to the user." *Microsoft I*, 829 F.3d at 218. The panel effectively punted on this argument, reasoning that it assumes that a "subpoena issued to Microsoft under the SCA's subpoena provisions would reach a user's e-mail content stored on foreign servers." *Id.* Although the panel recognized that the Second Circuit's own precedent suggested this would be the case, *see In re Marc Rich & Co., A.G.* ("*Marc Rich*"), 707 F.2d 663

(2d Cir. 1983), the panel concluded that it did not have to "determine the reach of the SCA's subpoena provisions, because [it was] faced here only with the lawful reach of an SCA warrant." *Microsoft I*, 829 F.3d at 219.

After finding that "privacy" was the SCA's "focus," the panel then turned to whether the execution of the warrant in this case was an "unlawful extraterritorial application of the Act," for which the panel had "little trouble" concluding was the case. *Id.* at 220. As the content to be "seized" was stored in Ireland, the panel held that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed." *Id.* The panel also concluded that by complying with the warrant, Microsoft would "act[] as an agent of the government." *Id.* "Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter," the panel found 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.*

Concurring in the panel decision, Judge Lynch wrote "to explain why [he] believe[s] that the government's arguments are stronger than the Court's opinion acknowledges; and to emphasize the need for congressional action to revise a badly outdated statute." *Id.* at 222 (Lynch, J., concurring). Judge Lynch first observed that upholding the warrant in this case would not "undermine basic values of privacy" as the "government complied with the most restrictive privacy-protecting requirements of the Act" by seeking an SCA warrant. *Id.* at 222–23. As Judge Lynch emphasized, in this case, "the government proved to the satisfaction of a judge that a reasonable person would believe that the records sought contained evidence of a crime," and such a showing complies with the privacy protections of the Fourth Amendment. *Id.* at 223. Thus, according to Judge Lynch, Microsoft's argument was not that the Court should

create, as a matter of Constitutional law, "stricter safeguards on the protection" of e-mails, but rather that Microsoft "can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing—in its own discretion—to store them on a server in another country." *Id.* at 224. In other words, Judge Lynch explained that under Microsoft's and the panel majority's interpretation of the SCA, "the privacy of Microsoft's customers' emails is dependent not on the traditional safeguard of private communications" in the form of a warrant requirement, "but rather on the business decisions of a private corporation." *Id.* Accordingly, Judge Lynch reasoned that the dispute in the case was not about "privacy, but rather about the international reach of American law." *Id.* at 225. Although the courts "have a significant role in the protection of privacy," Judge Lynch stated, "[w]hether American law applies to conduct occurring abroad . . . is a question that is left entirely to Congress." *Id.* (citing *Bens v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957) (explaining that Congress "alone has the facilities necessary to make fairly [the] important policy decision" about whether a particular statute applies extraterritorially)).

Judge Lynch also noted the peculiar nature of an SCA warrant. "Significantly," Judge Lynch wrote, "the SCA does not describe the warrant as a *search* warrant." *Id.* at 226 (emphasis in original). Unlike a search warrant, which is "focused on the *place* to be searched," the "SCA warrant provision does not purport to authorize any such thing," rather "it simply authorizes the government to *require the service provider to disclose* certain communications to which it has access." *Id.* at 227–28 (emphasis in original). This language parallels the other provisions of the SCA, all of which require the service provider "to disclose" the communications in question. *Id.* at 227. Based on this statutory language, the government "reasonably argues that the focus of such a provision is not on the place where the service provider stores the communications, but on

the place where the service provider discloses the information to the government, as requested." *Id.* at 228. Thus, Judge Lynch viewed the matter as "a very close case to the extent that the presumption against extraterritoriality shapes our interpretation of the statute." *Id.* at 229.

Judge Lynch expressed "considerable doubts" that the SCA provisions at issue in the case focus on "protecting the privacy of the content of a user's stored electronic communications." *Id.* at 229 n.7 (citing *id.* at 217). Rather, "[p]rivacy . . . is an abstract concept with no obvious territorial locus" and thus, the "conclusion that the SCA's focus is privacy . . . does not really help us to distinguish domestic applications of the statute from extraterritorial ones." *Id.* The crux of the majority opinion, Judge Lynch reasoned, was not the "conclusion that the statute focuses on privacy" but the "majority's determination that the locus of the invasion of privacy is where the private content is stored—a determination that seems . . . suspect when the content consists of emails stored in the 'cloud.'" *Id.* Contrary to this determination, Judge Lynch indicated that it was "at least equally persuasive that the invasion of privacy occurs where the person whose privacy is invaded customarily resides." *Id.*

Despite these concerns, Judge Lynch concluded that the panel majority had reached the correct result, because: "If we frame the question as whether Congress has demonstrated a clear intention to reach situations of this kind in enacting the Act, I think the better answer is that it has not, especially in the case (which could well be this one) of records stored at the behest of a foreign national on servers in his own country." *Id.* at 230. Since the "now-familiar idea of 'cloud' storage of personal electronic data by multinational companies was hardly foreseeable to Congress in 1986, and the related prospects for diplomatic strife and implications for American businesses operating on an international scale were surely not on the congressional radar screen when the Act was adopted," *id.* at 231, Judge Lynch explained "that there is no evidence that

Congress has *ever* weighed the costs and benefits of authorizing court orders of the sort at issue in this case," *id.* (emphasis in original).

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). Four dissenting judges, each of whom wrote individual dissents and joined the others' dissents, expressed the view that the statute's focus, or, relatedly, the conduct at issue, was the "disclosure" of the information sought by the government, which they asserted occurs wholly inside the United States where the service provider accesses the user's data. *See id.* at 64–68, 73.

C. Magistrate Judge's Decision

In this case, the Magistrate Judge issued a thorough and well-reasoned opinion declining to follow *Microsoft.* Accepting the parties' agreement that the SCA does not apply extraterritorially under step one of the two-step framework of *Morrison* and *RJR Nabisco,* the Magistrate Judge turned to step two, for which *RJR Nabisco* instructs that "[i]f the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad." *RJR Nabisco*, 136 S. Ct. at 2101. Alternatively, "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.* Applying this analysis, the Magistrate Judge first found that *Microsoft* had erred by improperly identifying the focus of the SCA as "privacy" when instead the "focus" of § 2703 is the "disclosure" of the information to law enforcement, as the government contended. The Magistrate Judge further disagreed with Google's position that the relevant conduct by the provider was the provider's "accessing" of the user's data, noting that the relevant provisions of the SCA refer to "disclosure," while only § 2701 "specifically limit[s]

access to customer communications." Mem. Op., 2017 WL 2480752, at *9 (quoting *Microsoft II*, 855 F.3d at 67 (emphasis in original) (Cabranes, J., dissenting)).

Having found that the focus of § 2703 is "disclosure," the Magistrate Judge identified the territorial locus of that disclosure to be in the United States, since this is the country "where Google discloses the responsive information in its control to the government pursuant to the warrant." *Id.* at *9 (citing *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.")). Accordingly, the Magistrate Judge discounted as making no difference whether the "focus" of the SCA is "privacy" or "disclosure" because "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." *Id.*

Dismissing Google's argument that the relevant conduct occurs abroad where the service provider "search[es] for and seiz[es]" the user's data, the Magistrate Judge described this position as "fundamentally misunderstand[ing] the particular legal process at issue" because the service provider is not actually "seizing" the data. *Id.* at *10. In support, the Magistrate Judge relied on case law stating that a seizure does not occur unless there has been "some meaningful interference with an individual's possessory interests in that property." *Id.* (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). The Magistrate Judge further found that Google's position was undermined by its denial that the company acted as an agent of the government when accessing user information in execution of an SCA warrant, noting that in *Microsoft*, "the finding that the service provider was 'acting as an agent of the government' . . . was critical to

the court's conclusion that a service provider is 'seizing' a customer's data and invading that customer's privacy at a data's storage site." Mem. Op., 2017 WL 2480752, at *10 (quoting *Microsoft*, 829 F.3d at 220).

Cautioning that the *Microsoft* decision would lead to "bizarre results," the Magistrate Judge explained that if that decision were applied to dynamic storage networks, such as Google's, "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." *Id.* at *10. In this respect, Google's dynamic data storage network, which "fragment[s] and dispers[es] its users data for storage" and "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," *id.* at *6, differs from Microsoft's network, which locates entire files in a single data center depending on the user's self-reported location, *see Microsoft I*, 829 F.3d at 202 ("Microsoft generally stores a customer's e-mail information and content at datacenters located near the physical location identified by the user as its own when subscribing to the service."). Further, even if the service provider with a dynamic storage network "could and would identify for law enforcement the location of the foreign-based servers on which the missing data was stored," that information would be rendered useless because "[b]y the time the government could initiate the international legal process necessary . . . it is entirely possible that the network would have relocated the data yet again to a server in a different country." Mem. Op., 2017 WL 2480752, at *11.

D. Google's Objections

Google objects to the Magistrate Judge's order granting the government's motion to compel compliance with the SCA warrant. Relying heavily on the *Microsoft* decision, Google

argues the Magistrate Judge erred in concluding "that disclosing content stored outside of the United States in response to an SCA warrant 'is a domestic application of the SCA.'" Objs. at 1. In particular, Google contends that the Magistrate Judge "'ignor[ed]' Supreme Court case law establishing the presumption against extraterritorial application of statutes," and incorrectly applied "step two of the *Morrison* and *RJR Nabisco* tests by concluding that the 'conduct relevant to the statute's focus occurs in the United States.'" *Id.* at 1–2. According to Google, the "conduct relevant to the focus of the SCA" includes the "access," "search," and "retrieval" of user records and electronic communications from data centers outside the United States, and thus the execution of an SCA warrant as to user communications located abroad "amount[s] to an impermissible extraterritorial application of the SCA." Google's Reply Supp. Objs. ("Google's Reply"), at 1, ECF No. 28. Further, Google disputes the Magistrate Judge's opinion that "'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,'" Objs. at 2–3 (quoting Mem. Op., 2017 WL 2480752, at *10), because, even if not an agent, the "SCA does not provide authority for the government to conscript a private party to do what the government cannot itself do," *id.* at 3. Finally, Google asserts that "Congress chose the term 'warrant' in Section 2703 of the SCA to convey the traditional, widely-recognized—and territorially limited—meaning of the term 'warrant.'" Google's Reply, at 1.

E. Analysis

"The basic legal question confronting us is not a total stranger to this Court." *United States v. First Nat. City Bank*, 396 F.2d 897, 900 (2d Cir. 1968). "With the growing interdependence of world trade and the increased mobility of persons and companies, the need arises not infrequently, whether related to civil or criminal proceedings, for the production of

evidence located in foreign jurisdictions." *Id.* Likewise, the last two decades has seen an exponential growth of mobility of data, as we "have witnessed a dramatic globalization of the Internet." Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 287 (2015). As the Supreme Court has recognized, "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior." *City of Ontario v. Quon*, 560 U.S. 746, 759 (2010).

As a result, the judiciary and legislature have been challenged to keep up with precipitous advancements in technology and global interconnectedness. Traditional notions of "territoriality" and "jurisdiction" have been muddied, especially when it comes to determining the scope of statutes governing access and disclosure of electronic records and communications. The picture is murkier still with the advent of so-called "cloud" computing, which is "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).[16] For this reason, legislators have recently viewed statutes, such as ECPA and the SCA, as increasingly "outdated," *see* Charlie Savage, *Panel Approves a Bill to Safeguard Email*, N.Y. TIMES, Nov. 30, 2012 (stating that ECPA "is widely seen as outdated"), and some lawmakers have for several years called for reforming the law, *see* Press Release, Sen. Mike Lee, *Sens. Lee and Leahy Introduce ECPA Modernization Act* (July 27, 2017) (announcing a new bill to amend the ECPA "to better reflect Americans' modern expectations of privacy"); *see also* Press Release Sen. Patrick Leahy, *Leahy*

[16] According to the National Institute of Standards and Technology, "cloud computing" is defined as follows: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Peter Mell & Timothy Grance, U.S. Dep't of Commerce, Special Pub. 800-145, THE NIST DEFINITION OF CLOUD COMPUTING: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2 (2011) *available at* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Joined By Bipartisan, Bicameral Group to Introduce Bill Protecting Online Privacy (Feb. 4, 2015) (announcing an effort to reform ECPA to "bring Americans' privacy rights and protections into the digital age); *id.* (statement by Sen. Mike Lee that "In the nearly three decades since ECPA became law, technology has advanced rapidly and beyond the imagination of anyone living in 1986."). At bottom, however, even if aspects of the ECPA and SCA are outdated and in need of reform, these statutes need not be regarded, as the *Microsoft* panel effectively did, as so antiquated as to be both ineffectual and inapplicable in the current environment.

The *Microsoft* panel's decision rests on several fundamental errors. First, the panel erred in determining that the case turned on where the targeted information is "located," as opposed to the salient considerations under the statute, such as the location of the service provider or the offense conduct at issue. Second, the panel compounded this error by then holding that the territorial limitations on the execution of a "search warrant" also limited an SCA warrant's reach to data "located" in the United States. *See Microsoft I*, 829 F.3d at 209. Third, the panel erroneously applied the Supreme Court's extraterritoriality analysis, as set forth in *Morrison* and *RJR Nabisco*, by determining that the "focus" of the SCA is "privacy" and that the conduct "relevant" to that focus was the "access" of user data stored in foreign servers. Google, relying on *Microsoft* for support for its arguments, makes the same missteps.

The explication of these errors proceeds by explaining, first, why the SCA warrant was simply a domestic execution of the court's statutorily authorized enforcement jurisdiction over a service provider, which may be compelled to retrieve electronic information targeted by the warrant, regardless of where the information is "located;" second, why an SCA warrant is unlike a traditional "search warrant" and thus does not carry with it the "traditional, domestic connotations" of an ordinary search warrant, *see Microsoft I*, 829 F.3d at 213; third, why, if

applicable, the extraterritoriality analysis of *Morrison* and *RJR Nabisco* puts the correct "focus" of the SCA warrant provision on "disclosure"; and fourth, why, regardless of whether the "focus" of the SCA provision is "privacy," "disclosure," or both, the "conduct relevant to that focus" is Google's "disclosure" of the user communications, which takes place wholly inside the United States and is a domestic application of the statute. Finally, this section concludes with discussion of the serious policy implications of the *Microsoft* panel's decision, which, while not dispositive, highlight its legal defects

1. Enforcement Jurisdiction

A well-established principle is that courts have the power to exercise authority on people and entities over whom they have personal jurisdiction, including compelling those individuals or entities to retrieve documents from abroad. *See, e.g., Blackmer v. United States*, 284 U.S. 421, 438 (1932) ("The jurisdiction of the United States over its absent citizen, so far as the binding effect of its legislation is concerned, is a jurisdiction *in personam*, as he is personally bound to take notice of the laws that are applicable to him and to obey them."). The SCA warrant was merely an exercise of this Court's enforcement jurisdiction, which is "a state's authority to compel compliance or impose sanctions for noncompliance with its administrative or judicial orders." *F.T.C. v. Compagnie De Saint-Gobain-Pont-a-Mousson*, 636 F.2d 1300, 1315 (D.C. Cir. 1980) (citing RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 6 cmt. *s* (1965)). "When an American court orders enforcement of a subpoena requiring the production of documents . . ., it invokes the enforcement jurisdiction, rather than the prescriptive jurisdiction, of the United States." *Id.* at 1316.[17]

[17] Generally speaking, there are two types of jurisdiction: jurisdiction to prescribe and jurisdiction to enforce. "Jurisdiction to prescribe signifies a state's authority to enact laws governing the conduct, relations, status or interests of persons or things, whether by legislation, executive act or order, or administrative rule or regulation."

To be sure, enforcement jurisdiction has territorial limitations: "a nation can exercise enforcement jurisdiction only against persons or entities with a presence or assets within its territory." Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EUR. J. INT'L L. 135, 139 (2000). At the same time, if a court has personal jurisdiction over a defendant, it has jurisdiction to enforce and, as the Second Circuit itself has made clear, "[i]t is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has in personam jurisdiction of the person in possession or control of the material." *United States v. First Nat'l City Bank*, 396 F.2d at 900–01; *see also* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432 cmt. b ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States."). Indeed, a company availing itself of the opportunity of doing business in the United States is subject to U.S. criminal laws and can be compelled to bring assets and evidence from abroad into the United States. *See, e.g.*, *In re Sealed Case*, 832 F.2d 1268, 1283 (D.C. Cir. 1987) (stating that a subpoena for documents in Switzerland was enforceable if the district court had jurisdiction over the companies whose records were sought and that "[a] United States Court has the power to order any party within its jurisdiction to testify or produce documents regardless of a foreign sovereign's views to the contrary." (quoting *In re Anschuetz & Co.*, 754 F.2d 602, 613 n. 28 (5th Cir. 1985)) *abrogated on other grounds by Braswell v. United States*, 487 U.S. 99 (1988); *see also id.* at 1284 ("Most courts, including this one, are reluctant to embrace doctrines that would allow those who break American laws to

Compagnie De Saint-Gobain-Pont-a-Mousson, 636 F.2d at 1315 (citing RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 6–7).

escape sanctions by setting up base abroad."); *Commodity Futures Trading Comm'n v. Nahas*, 738 F.2d 487, 492 n.11 (D.C. Cir. 1984) (noting that the Commodity Futures Trading Commission would "have authority to require production of documents held abroad" if it served a subpoena on U.S. citizen within the United States (citing *CAB v. Deutsche Lufthansa Aktiengesellschaft*, 591 F.2d 951, 953 (D.C. Cir. 1979)); *see also Linde v. Arab Bank PLC*, 706 F.3d 92 (2d Cir. 2013) (recognizing that the Supreme Court has held that "the operation of foreign law 'do[es] not deprive an American court 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 (1987))); *United States v. Bank of Nova Scotia*, 730 F.2d 817, 828 (11th Cir. 1984); *Marc Rich*, 707 F.2d at 668–70 (holding that a US person can be compelled to retrieve material from abroad); *SEC* v. *Minas de Artemisa, S. A.*, 150 F.2d 215, 216-218 (9th Cir. 1945) ("The obligation to respond applies even though the person served [with a subpoena] may find it necessary to go to some other place within or without the United States in order to obtain the documents required to be produced."); 9A CHARLES ALAN WRIGHT AND ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2456 at 31 ("[E]ven records kept beyond the territorial jurisdiction of the district court . . . may be covered if they are controlled by someone subject to the court's jurisdiction."); *cf. Hale v. Henkel*, 201 U.S. 43, 75 (1906) ("It would be a strange anomaly to hold that a state, having chartered a corporation to make use of certain franchises, could not, in the exercise of its sovereignty, inquire how these franchises had been employed, and whether they had been abused, and demand the production of the corporate books and papers for that purpose.").

Most of this case law was firmly established at the time ECPA was enacted in 1986 and courts generally presume that Congress understood the current state of the law when passing legislation. *See Cannon v. Univ. of Chicago*, 441 U.S. 677, 696-97 (1979). This presumption applies here. Although courts may not issue warrants for extraterritorial searches, *see, e.g.*, *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 171 (2d Cir. 2008), a statute may authorize courts to issue orders compelling an individual or entity within its enforcement jurisdiction to produce records located abroad that are relevant to an offense committed in the United States, *see Bank of Nova Scotia*, 740 F.2d at 828, 832.[18] In the SCA, Congress authorized the government to use an SCA warrant, a subpoena, or a § 2703(d) order to compel defined types of service providers subject to the jurisdiction of U.S. courts to disclose electronic records under its control, including such records stored abroad, just as any other subpoena, order or warrant so directed could compel disclosure of other forms of information located abroad.

Google resists the similarity in authority to demand production of both electronic and other forms of records, arguing instead that "[t]he government seeks here not the equivalent of requiring a bank or a hotel to retrieve business records from outside the United States, as it might with a subpoena, but rather the equivalent of requiring a bank to search, seize, and retrieve to the United States documents its customer has stored in a safe deposit box in a foreign branch or requiring a hotel chain to search, seize, and retrieve to the United States luggage or correspondence a customer has stored in a room in a foreign hotel." Objs. at 14. Google concedes that it does not act as an "agent" of the government when it accesses user's electronic

[18] Courts have recognized that corporations operating in more than one country might be subject to the "jurisdiction of two sovereigns and confronted with conflicting commands." *First Nat. City Bank*, 396 F.2d at 901. Accordingly, courts are permitted to "weigh[] the conflicting legal obligations of U.S. discovery orders and foreign laws." *Linde*, 706 F.3d at 108. Google, however, has not raised this as a potential concern and, in any event, "the operation of foreign law 'does 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.'" *Linde*, 706 F.3d at 109 (quoting *Societe Nationale Industrielle Aerospatiale*, 482 U.S. at 544 n.29.

records and communications pursuant to an SCA warrant. Mem. Op., 2017 WL 2480752, at *10. Nonetheless, Google contends it is "constript[ed] . . . to do electronically what the government cannot." Google's Reply at 10.

At least three problems are apparent with Google's argument. First, Google chooses the wrong analogy. Electronic records and communications are not like "paper files intermingled in a file cabinet." *United States v. Ganias*, 824 F.3d 199, 211 (2d Cir.) (*en banc*), *cert. denied*, 137 S. Ct. 569 (2016). "Even the most conventional 'files'—word documents and spreadsheets [ ]—are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files. They are in fact 'fragmented' on a storage device, potentially across physical locations." *Id.* (citing Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y, art. 5, at 1, 13 (2007)). This is an apt description of Google users' electronic records and communications, which are stored "in various locations," and "[s]ome user files may also be broken into component parts, and different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time." Stip. ¶¶ 2, 3. Thus, rather than being like discrete physical items placed in a safe deposit box, as Google suggests, electronic files uploaded to the "cloud" are more akin, in terms of being mobile and divisible, to money deposited in a bank account. If an American bank account holder deposits a twenty-dollar bill in her U.S. bank account, she expects to be able to receive the same *amount* of money when she makes a withdrawal but without regard or care whether, after the funds are deposited, those funds may be wired across the globe to various branches or stored elsewhere. That her "twenty dollars" may be wired to or stored in a bank branch in Geneva does not strip a U.S. court of jurisdiction. The same is true of electronic records and communications. When a user uploads a photograph to Google's "cloud" storage

network, the user does not much care that Google might split the file into several fragments, and shuttle them from server to server across the globe—indeed, the user has no choice. *See* Stip. ¶¶ 2, 3. What matters is that the service provider is able to provide the intact file to the user from the "cloud" when the user wants to access it. To effectuate this user experience, Google itself must access its users' records and communications, and by so doing, the company does not search or seize that data any more than a bank "searches" or "seizes" a depositor's twenty dollars when it wires those funds to other branches across the globe.

Second, in the context of electronic information, when Google queries its database, finds the communications in question, and retrieves it for storage on its local servers in the United States, Google does not "search" or "seize" the communications in a Fourth Amendment sense. The Fourth Amendment "protects two types of expectations, one involving 'searches' the other 'seizures.'" *United States v. Jacobsen*, 466 U.S. 109, 113 (1986). "A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." *Id.* "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property.'" *Id.; see also California v. Hodari D*, 499 U.S. 621, 624 (1991) ("From the time of the founding to the present, the word 'seizure' has meant a 'taking possession.'"). The mere transfer by Google of customer information from a server in a foreign country to Google's data center in California does not amount to a "search" or a "seizure." This is because Google regularly transfers such information from server to server "as frequently as needed to optimize for performance, reliability, and other efficiencies." Stip. ¶ 4. These transfers do not infringe on any expectation of privacy nor do they meaningfully interfere with the customer's possessory interests in the information. *See Arizona v. Hicks*, 480 U.S. 321, 323–24 (1987) (holding that an officer copying the serial number off a stereo did not constitute a

"seizure" because it did not "meaningfully interfere" with the owner's possessory interest in "either the serial numbers or the equipment."). Rather, § 2701 expressly permits Google to access a customer's electronic communications, exempting it from rules prohibiting unauthorized access. *See* 18 U.S.C. § 2701(c)(1),(a)(1) (exempting "the person or entity providing a wire or electronic communications service" from the statute's prohibitions on intentional access "without authorization a facility through which an electronic communication is provided"). Consequently, by accessing its customers' records and communications to respond to a government demand for disclosure, Google is essentially performing the same internal operations as if the customer had requested the information.

Third, Google readily admits that it would fully comply with the SCA warrant if the customer's electronic communications were stored on servers inside the United States. Even if an SCA warrant is akin to requiring a bank to "search, seize, and retrieve . . . documents its customer has stored in a safe deposit box," Objs. at 14, Google concedes such a request is appropriate as long as the "safe deposit box" is located in the United States. Mem. Op., 2017 WL 2480752, at *3 (explaining that after the *Microsoft* decision, Google redesigned its database management tool so that, in response to legal process, it would only "search[] for information stored on servers in its domestic data centers" and that after the search, Google's legal team "compiles whatever responsive data is stored *domestically* and produces a copy of it to the government" (emphasis added)). Google advances a distinction between a server located abroad versus a server located in the United States. Yet, this distinction has no legal basis since "[t]he test for the production of documents is *control*, not *location*." *Marc Rich*, 707 F.2d at 667 (emphasis added). A provider with the "power to cause . . . records to be sent from a branch to the home office for any corporate purpose[] surely has sufficient control to cause them to be sent

on when desired for a governmental purpose properly implemented by a subpoena." *First Nat. City Bank v. I.R.S.*, 271 F.2d 616, 618 (2d Cir. 1959); *see also Microsoft II*, 855 F.3d at 72 ("The question whether the caretaker's actions respecting materials in his possession constitute a 'search' or 'seizure' undertaken as an agent of the government does not turn on whether the item is located here or overseas. Indeed, as Judge Lynch states, we have upheld the use of a subpoena to compel a caretaker to produce client materials in its domestic possession." (citing *Microsoft*, 829 F.3d at 228 n.5 (Lynch, J., concurring and citing *In re Horowitz*, 428 F.2d 72 (2d Cir. 1973)) (Raggi, J., dissenting).[19]

Thus, where the evidence is stored or "located" is irrelevant. Instead, the critical inquiry is whether the service provider has sufficient "control" to retrieve and disclose the targeted records and communications in the United States. *See In re Sealed Case*, 832 F.2d at 1283; *see also Marc Rich*, 707 F.2d at 667.[20]

---

[19] To be clear, the Fourth Amendment broadly permits the government to obtain an individual's records held by a third-party business through a subpoena, without a warrant based on probable cause, and such a demand does not constitute a Fourth Amendment "search." *See Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 194–95 (1946); *United States v. Miller*, 425 U.S. 435, 445–46 (1976). For example, in *Miller*, the government obtained by subpoena records of a defendant's accounts from one of his banks, including copies of checks, deposit slips, financial statements, and other records. *See Miller*, 425 U.S. at 436–48. The Supreme Court held the acquisition was not an "intrusion into any area in which [the defendant] had a protected Fourth Amendment interest." *Id.* at 440. The defendant could "assert neither ownership nor possession" of the records because they were "business records of the banks," and the defendant had no "reasonable expectation of privacy" in the records because "they [were] merely copies of personal records that were made available to the banks for a limited purpose." *Id.* at 440, 442. The Supreme Court explained that it had "held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose." *Id.* at 443. Accordingly, because the defendant had voluntarily conveyed the information to the banks, the defendant had "take[n] the risk, in revealing his affairs to another, that the information w[ould] be conveyed by that person to the Government." *Id.* at 442, 443; *see also Smith v. Maryland*, 442 U.S. 735, 742–46 (1979) (applying the *Miller* principle to records created by a telephone company).

[20] The "control" test is not without consequences. To skirt the reach of SCA warrants, providers may be incentivized to store data on foreign servers owned by so-called "data trustees." For example, Microsoft has already engaged in a "trustee" relationship with a German company, allowing certain subscribers to store electronic communications on servers operated by a subsidiary of Deutsche Telekom. *See* Press Release, *Microsoft Announces Plans to Offer Cloud Services from German Datacenters* (Nov. 11, 2015), *available at* https://news.microsoft.com/europe/2015/11/11/45283/. Under the agreement, "Microsoft will not be able to access th[e] data without the permission of customers or the data trustee, and if permission is granted by the data trustee, will only do so under its supervision." *Id.* The Court need not reach the question of whether this "data trustee"

2. The SCA's Warrant Provision is Not Territorially Limited

Google nonetheless argues that "Congress used the term of art 'warrant' in Section 2703 of the SCA to convey the traditional, widely-recognized—and territorially limited—meaning of the term 'warrant[.]'" Google's Reply, at 1, 3–11; Objs. at 9–10. According to Google, the provision's distinction between a "warrant" on the one hand, and a "subpoena" or an "order" on the other hand, "was designed to do more than require the government to make a probable cause showing to obtain user content[.]" Objs. at 9. In support, Google relies on *F.A.A. v. Cooper*, 566 U.S. 284 (2012), in which the Supreme Court stated that "when Congress employs a term of art, 'it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken.'" 566 U.S. at 292 (quoting *Molzof v. United States*, 502 U.S. 301, 307 (1992)). According to Google, the "cluster of ideas" includes the fact "that the private content of stored communications was protected by the Fourth Amendment, and that accessing them would entail a search and seizure," Objs. at 10 (citing H.R. Rep. No. 99-647, at 68 (1986)), and that "[s]earch warrants are not directed at persons; they authorize the search of 'place[s]' and the seizure of things," *id.* (quoting *Zurcher v. Stanford Daily*, 436 U.S. 547, 555 (1978) (second alteration in original)). In Google's view, "[i]t is beyond question, for example, that an SCA warrant could not authorize the FBI to travel to a Google data center in Singapore, demand access to the servers located there, and download from them communications otherwise within the scope of the warrant." *Id.* (footnote omitted).

The government, for its part, argues that Congress's use of the term "warrant" "was intended to import the probable cause standard and not to protect privacy in any territorial way." Gov't Opp'n, at 20. The government also avers that the authority upon which Google relies is

---

arrangement sufficiently undercuts Microsoft's "control" over the electronic communications to put that evidence outside the reach of an SCA warrant, subpoena, or § 2703(d) order.

"misleading and unavailing." *Id.* at 21. Although acknowledging that the House Report of the Judiciary Committee "did indeed assume that the contents of email messages in storage are protected in some measure by the Fourth Amendment," the government points to the Report of the Senate Judiciary Committee, which stated that because emails are "subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection." *Id.* at 22 (quoting S. Rep. No. 99-541, at 2). Further, the government notes that neither the House nor the Senate Report "remotely suggests that Congress understood that a provider's '*accessing* [email] would entail a *search* and *seizure*.'" *Id.* (alteration and emphasis in original). Instead, the government notes that Congress "expressly exempted providers from the account access limitations Congress imposed in section 2701." *Id.* The government also challenges Google's reliance on *Zurcher v. Stanford Daily*, arguing that *Zurcher* involved a "premises search warrant" and does not hold that "warrants cannot act *in personam* to compel persons to disclose information, as Google contends, but merely that a premises warrant may be executed upon locations which have no association to persons under investigation." *Id.* (citing *Zurcher*, 436 U.S. at 555). The government's arguments are persuasive that the territorial limits associated with Rule 41 search warrants do not apply to SCA warrants, as review of the pertinent statutory language, structure, history demonstrates.

a) Statutory Language

"As in any statutory construction case, '[w]e start, of course, with the statutory text,' and proceed from the understanding that '[u]nless otherwise defined, statutory terms are generally interpreted in accordance with their ordinary meaning.'" *Sebelius v. Cloer*, 133 S. Ct. 1886, 1893 (2013) (quoting *BP Am. Prod. Co. v. Burton*, 549 U.S. 84, 91 (2006)). The relevant statutory provision at issue, § 2703, authorizes a "governmental entity" to "require" the

"disclosure" by a service provider of "the contents of a wire or electronic communication" if the government "obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." 18 U.S.C. §§ 2703(a),(b)(1)(A). Although the language is not precise, the "procedures described in the Federal Rules of Criminal Procedure" assuredly refers to Rule 41, which describes the procedures for the issuance of a search and seizure warrant.

As other courts have found, however, the phrase "issued using the procedures described in the Federal Rules of Criminal Procedure" is ambiguous, possibly incorporating all or only some of the provisions of Rule 41 into § 2703. *See, e.g.*, *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 470–71 (S.D.N.Y. 2014) (finding the words "using the procedures described in the Federal Rules of Criminal Procedure" ambiguous); *Hubbard v. MySpace, Inc.*, 788 F. Supp. 2d 319, 325 (S.D.N.Y. 2011) (finding the phrase "'issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation'" ambiguous "as to whether a state or federal warrant authorizing a search beyond the ordinary territorial authority of the issuing magistrate or judge is acceptable"); *In re United States*, 665 F. Supp. 2d 1210, 1219 (D. Or. 2009) (finding ambiguity in that "'[i]ssued' may be read to limit the procedures that are applicable under § 2703(a), or it might merely have been used as a shorthand for the process of obtaining, issuing, executing, and returning a warrant, as described in Rule 41"); *In re Search of Yahoo, Inc.*, No. 07–3194, 2007 WL 1539971, at *5 (D. Ariz. May 21, 2007) (finding that "the phrase 'using the procedures described in' the Federal Rules remains ambiguous"). Accordingly, because the language is ambiguous, it is appropriate to look to

"statutory structure, relevant legislative history, [and] congressional purposes." *Florida Power & Light Co. v. Lorion*, 470 U.S. 729, 737 (1985).

b) Statutory Structure

Google primarily relies on the term "warrant" to assert that Congress meant "to convey the traditional, widely-recognized—and territorially limited—meaning of the term 'warrant[.]'" Google's Reply at 1. The *Microsoft* panel relied, in part, on Rule 41(b)'s venue provisions for the notion that "[w]arrants traditionally carry territorial limitations." *Microsoft I*, 829 F.3d at 201; *see id.* at 214–15 ("We see no reason to believe that Congress intended to jettison the centuries of law requiring the issuance and performance of warrants in specified, domestic locations, or to replace the traditional warrant with a novel instrument of international application."). The structure of § 2703, however, evinces an intent to create a distinct procedural mechanism from a traditional Rule 41 "search warrant." As one commentator has explained, SCA warrants "are not like the search warrants used in the physical world: they are 'executed' when a law enforcement agent delivers (sometimes by fax) the warrant to the [service provider]." Paul K. Ohm, *Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1610–11 (2004). "The [service provider], not the agent, performs the 'search'; the [service provider] 'produces' the relevant material to the agent; the user associated with the inbox often never learns that his inbox has been 'searched.'" *Id.* at 1611. "In sum, these are not search warrants at all and to call them such confuses legal terminology." *Id.*

Indeed, the nomenclature used to refer to an SCA warrant has limited probative value. *Cf. Bay Ridge, Inc. v. Fed'l Mine Safety & Health Review Comm'n*, 715 F.3d 631, 646 (7th Cir. 2013) ("For purposes of our Fourth Amendment analysis, we look to the substance of [the

government's] power rather than how the Act nominally refers to those powers."). An SCA warrant operates much like a subpoena, as it "authorizes the government to *require the service provider to disclose* certain communications to which it has access." *Microsoft I*, 829 F.3d at 227–28 (Lynch, J., concurring); *Microsoft II*, 855 F.3d at 60 (Jacobs, J., dissenting) ("The instrument functions as a subpoena though the Act calls it a warrant."); *id.* at 66 (Cabranes, J., dissenting) ("[A] disclosure warrant is more akin to a subpoena."); *see* 18 U.S.C. § 2703(a). As Judge Lynch observed in his concurring opinion in *Microsoft I*, the SCA does not "contain language implying (let alone saying outright) that the warrant to which it refers authorizes government agents to go to the premises of a service provider without prior notice to the provider, search those premises until they find the computer, server or other device on which the sought communications reside, and seize that device (or duplicate and 'seize' the relevant data it contains)." *Microsoft I*, 829 F.3d at 226 (Lynch, J., concurring). In this respect, an SCA warrant does not authorize a "search and seizure;" rather, it is a "procedural mechanism to allow the government to 'require a [service provider] to disclose the contents of [certain] electronic communication[s]' *without notice to the subscriber or customer*." *Microsoft I*, 829 F.3d at 226 (Lynch, J., concurring) (quoting 18 U.S.C. § 2703(b)(1)(A)) (emphasis in original). Search warrants are executed "with respect to a *place*—the place to be searched," whereas a § "2703 warrant is executed with respect to a *person*—the person ordered to divulge materials in his possession." *Microsoft II*, 855 F.3d at 70 (Raggi, J., dissenting).

As the Magistrate Judge in the *Microsoft* case explained, the SCA warrant "is not a conventional warrant"; instead, it "is a hybrid: part search warrant and part subpoena." *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 471 (S.D.N.Y. 2014). "It is obtained like a search warrant when an application

is made to a neutral magistrate who issues the order only upon a showing of probable cause." *Id.* "On the other hand, it is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question." *Id.* Further, unlike a search warrant, which requires that the warrant and receipt for property taken be left with "the person from whom, or from whose premises, the property was taken," FED. R. CRIM. P. 41(f)(1)(C), no notice to the customer is required to be given by the government when using an SCA warrant.[21] To be sure, the service provider may give notice to its customer, but it can be precluded from doing so if the government obtains a court order pursuant to § 2705(b), at least for emails older than 180 days. *See supra* n.15

Accordingly, the structure of § 2703 strongly suggests that Congress intended an SCA warrant to be a distinct procedural mechanism from a traditional Rule 41 search warrant.

c) Legislative History

That SCA warrants are distinct from traditional search warrants is further underscored by amendments made to the SCA. Until 2001, the SCA warrant was called "a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant," 18 U.S.C. § 2703(a) (1994), and, thus, in accordance with Federal Rule of Criminal Procedure 41(b)(1), had to be issued in the district of where the service provider was located and, by extension, where the "account" was located, *see* H.R. Rep. No. 107-236(I), at 57 (2001). In the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), Pub. L. 107-56, 115 Stat. 272, 291-292**,**

[21] *But see supra* n.15. If the information is obtained via subpoena or § 2703(d) order, under § 2705(a), the government may apply for a court order permitting the government to delay notification for ninety days. This delayed notification order must be renewed every ninety days, however, whereas an SCA warrant triggers no user notification requirement.

however, Congress amended the SCA's § 2703 in significant ways to de-link the issuance of warrants for electronic communications and related records from many of the requirements—particularly the territorial limitations—of Rule 41.

The 2001 amendments struck references in § 2703 to "under the Federal Rules of Criminal Procedure" and substituted the different language "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation," *id*. at § 220(a)(1); and, second, defined the term "court of competent jurisdiction" with reference to the amended definition of this term in the Pen Register statute, at 18 U.S.C. § 3127 (amending term to add "(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or," *id*. § 216(c)(1)), which definition had the critical addition of the following language: "and includes any Federal court within that definition, *without geographic limitation*," *id*. § 220(a)(2)(C) (emphasis supplied).[22]

The 2001 change has two implications. First, the amended version of the SCA provided courts "with jurisdiction over the offense under investigation" to issue SCA warrants, regardless of the location of the ISP, the "account," or the targeted records or communication. Indeed,

[22] Eight years later, in 2009, Congress modified the language in § 2703 by replacing the words "by a court with jurisdiction over the offense under investigation or an equivalent State warrant" with "(or, in the case of a State Court, issued using State warrant procedures) by a court of competent jurisdiction," Foreign Evidence Request Efficiency Act of 2009, § 2, Pub. L. 111-79, 123 Stat 2086 (Oct. 19, 2009), and shifted the phrase "with jurisdiction over the offense under investigation" to the definition of "court of competent jurisdiction," *id*. Thus, the current definition of "court of competent jurisdiction" provides, in relevant part, that this term includes (A) "any district court of the United States . . . that (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to" 18 U.S.C. § 3512. 18 U.S.C. § 2711(3) (2009). The 2009 amendments struck the phrase "without geographic limitation" in part to "clarify [an] ambiguity in section 2703 by re-articulating the bases for courts to act" without "chang[ing] the existing standards that the government must meet in order to obtain evidence, nor . . . alter[ing] any existing safeguards on the proper exercise of such authority." Letter from M. Faith Burton, Acting Assistant Attorney General, to Senator Sheldon Whitehouse (Mar. 27, 2009), *reprinted in* 155 Cong. Rec. S. 6807, 6810 (2009).

"[c]ommentators have suggested that one reason for the amendments effected by § 220 of the Patriot Act was to alleviate the burden placed on federal district courts in the Eastern District of Virginia and the Northern District of California where major internet service providers [ ] AOL and Yahoo, respectively, are located." *In re Search of Yahoo, Inc.*, No. 07–3194 (LAO), 2007 WL 1539971, at *4 (D. Ariz. May 21, 2007); *see, e.g.*, Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens,* 72 GEO. WASH. L. REV. 1375, 1454 (2004) (stating that the "effect of the change was to shift the responsibility for issuance of the order from the court where the service provider is located to the court with jurisdiction over the offense being investigated; prior to passage of the USA Patriot Act, a disproportionate number of such orders were issued in the Eastern District of Virginia, where AOL is located."). Further, the House Judiciary Committee's Report accompanying the USA PATRIOT Act explains that the amendments to § 2703(a) were driven by "attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet" and to allow "the court with jurisdiction over the investigation to issue the warrant directly, without requiring the intervention of its counterpart in the district where the ISP is located." H.R. Rep. No. 107–236, at 57 (2001). Consequently, an SCA warrant may be obtained from any court that "has jurisdiction over the offense," 18 U.S.C. § 2711(3), just as a federal criminal subpoena may be issued out of an investigating district and served anywhere the recipient is subject to service, FED. R. CRIM. P. 17(e). In this way, the current version of the SCA plainly grants this Court jurisdiction to issue the SCA warrant in question and to compel Google to provide the information, "without geographical limitation" on where the electronic communications and related records may be "located," because Google has "control" over the information. *See In re Sealed Case,* 832 F.2d at 1284; *see also Tiffany (NJ) LLC v. Qi Andrew*, 276 F.R.D. 143, 147–48 (S.D.N.Y. 2011) ("If the party subpoenaed has the practical ability to

obtain the documents, the actual physical location of the documents—even if overseas—is immaterial.").

Second, by amending the language "under the Federal Rules of Criminal Procedure" to read "a warrant issued using the *procedures* described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant," 18 U.S.C. § 2703(a) (2002) (emphasis added), Congress indicated that it meant that an SCA warrant is not a traditional search warrant, but instead a distinct procedural mechanism that imports some—but not all—of the requirements of Rule 41, including, most importantly, the probable cause requirement, *see* FED. R. CRIM. P. 41(d)(1).

Congress also amended the statute in 2002 to make clear that not all of the ordinary requirements for a Rule 41 search warrant are necessary for an SCA warrant. In particular, the 2002 amendment added subsection (g) to § 2703 which provides that the "presence" requirement of 18 U.S.C. § 3105 is not required for "service or execution of a search warrant issued in accordance with this chapter." 18 U.S.C. § 2703(g). This change was passed in response to the Eighth Circuit's decision in *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002), which held that the presence of a law enforcement officer requirement of § 3105 was applicable to SCA warrants. *See* Paul K Ohm, *Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1617 (2004) (explaining that § 2703(g) was added in response to the Eighth Circuit's decision in *Bach*).

This distinction between an SCA warrant and a traditional search warrant is further illustrated by how an SCA warrant is referred to in related statutes. The Foreign Evidence Request Efficiency Act of 2009, codified at 18 U.S.C. § 3512, for example, authorizes applications by the government for an order to "execute a request from a foreign authority for

assistance in the investigation or prosecution of criminal offenses." 18 U.S.C. § 3512(a)(1); *see* Foreign Evidence Request Efficiency Act of 2009, § 2, Pl. 111-79, 123 Stat. 2086 (2009). In particular, this statute states that such an order authorizing assistance may include the issuance of the following:

> (A) a search warrant, as provided under Rule 41 of the Federal Rules of Criminal Procedure; [or]
>
> (B) a warrant or order for contents of stored wire or electronic communications or for records related thereto, as provided under section 2703 of this title;

18 U.S.C.A. § 3512(a)(2)(A)–(B).[23] The separate entries for subsections 3512(a)(2)(A) and (a)(2)(B) reflects a recognition that an SCA warrant is a distinct procedural mechanism and not the "traditional, widely-recognized" search warrant of Rule 41, as Google posits. Put differently, if Congress understood an SCA warrant to be just like any other Rule 41 "search warrant," then 18 U.S.C. § 3512(a)(2)(B) would be superfluous, and "[i]t is 'a cardinal principle of statutory construction' that 'a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.'" *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) (quoting *Duncan v. Walker*, 533 U.S. 167, 174 (2001)).[24]

---

[23] There are other types of orders permitted under 18 U.S.C. § 3512, including an order for a "pen register or trap and trace device," *id.* § 3512(a)(2)(C), and an order requiring the appearance of a person for the purpose of providing testimony or a statement, or requiring the production of documents or other things, or both," *id.* § 3512(a)(2)(D).

[24] Google argues that the Wiretap Act's reference to an order supported by "probable cause," without using the word "warrant," shows that the SCA's reference to a "warrant" was not intended to solely import the probable cause requirement. *See* Objections at 9 (citing 18 U.S.C. § 2518(3)). In Google's view, had Congress meant the term "warrant" to only import the "probable cause" standard, they could have just said so as they did in the Wiretap Act. This argument is unavailing for at least three reasons. First, while § 2703 incorporates more than just the probable cause requirement of Rule 41, the territorial limitations of Rule 41 are not among the Rule 41 "procedures" applied to SCA warrants. Consequently, the fact that § 2703(a) did not just use the term "probable cause" does not indicate that an SCA warrant is territorially limited. Second, as the government argues, the Wiretap Act's explicit reference to probable cause is necessary because the statute also requires a showing that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3)(c). Mere reference to the Federal Rules of Criminal Procedure in the Wiretap Act would have been insufficient to effectuate the additional procedural safeguards required to intercept real-time communications under the Wiretap Act. Finally, relatedly, the Wiretap Act applies to *prospective* interception of live communications, whereas the SCA is *retrospective*, applying to existing stored electronic communications, just

Accordingly, the SCA legislative history illustrates that Congress intended an SCA warrant to be unlike a traditional Rule 41 warrant. In particular, by 2001, Congress ensured that an SCA warrant was not bound by Rule 41(b)'s venue restrictions. If Congress had meant an SCA warrant to be a traditional search warrant, following *all* of the requirements of Rule 41, then it would have said so; instead, "Congress said what it meant and meant what it said." *Loughrin v. United States*, 134 S. Ct. 2384, 2391 (2014) (citing *Connecticut Nat. Bank v. Germain*, 503 U.S. 249, 254 (1992)).

* * *

The text, structure, and history of the SCA show that Congress meant to create a distinct procedural mechanism with some substantive and procedural requirements of a warrant and the reach of a subpoena, to compel a service provider to disclose communications in its possession. Electronic communications content in storage 180 days or less was afforded the added privacy safeguard of a "probable cause" requirement but with the omission of any user notification requirement.

3. The SCA Warrant At Issue is a Domestic Application of the SCA

Notwithstanding the fact that the SCA warrant in this case was executed domestically and does not implicate extraterritorial concerns at all, Google nonetheless argues—echoing the position taken by the *Microsoft* panel—that the SCA warrant is an extraterritorial application of the SCA. Even assuming the presumption against extraterritorial application of statutes were implicated in this case—and it is not—the presumption would not bar the order in this case compelling Google to comply fully with the SCA warrant.

---

as Rule 41 warrants apply to existing evidence. Using the term "warrant" in the Wiretap Act would thus be inapt and, as the government puts it, "more confusing than helpful." Gov't Opp'n at 23 n.8.

"Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2100 (2016) (citing *Morrison* v. *National Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010)). Generally, then, statutes are presumed not to apply extraterritorially. *Id.* (citing *Morrison*, 561 U.S. at 255). "When a statute gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255; *see also EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991). *Morrison* and *RJR Nabisco* establish a two-step framework for analyzing extraterritorial application of statutes. First, a court must determine "whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially." *RJR Nabisco*, 136 S. Ct. at 2101. Here, the parties do not dispute the fact that the SCA does not apply extraterritorially. Gov't Opp'n at 35; Google's Reply at 3. "If the statute is not extraterritorial, then at the second step [the court] determine[s] whether the case involves a domestic application of the statute, and [does] this by looking to the statute's 'focus.'" *Id.* "If the *conduct relevant to the statute's focus* occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory." *Id.* (emphasis added). Thus, the second step of the *Morrison/RJR Nabisco* framework itself requires two distinct determinations: (1) a court must determine the statute's "focus," and (2) a court must then determine whether the conduct "relevant" to that focus occurred in the United States or occurred abroad. *See id.*

a) The "Focus" of § 2703 is "Disclosure"

Google insists that the *Microsoft* panel was correct and that the "focus" of the SCA for the purposes of the extraterritoriality analysis is "privacy" because "Congress enacted the SCA to ensure that the privacy of electronic communications is appropriately protected, including when the government seeks to compel a provider to access and disclose those communications." Objs. at 12. This Court concurs with the conclusion of the Magistrate Judge that "the focus of the SCA's warrant provisions—§ 2703—is on the *disclosure* of customer records and information to law enforcement," and not privacy, as Google argues, *see* Objs. at 12–13, and as the *Microsoft* panel held, *see* Mem. Op., 2017 WL 2480752, at *8–9.

A court determines the focus of a particular statutory provision by identifying the acts that the provision "seeks to 'regulate'" and the parties or interests that it "seeks to 'protect.'" *Morrison*, 561 U.S. at 267 (quoting *Superintendent of Ins. of N.Y. v. Bankers Life & Cas. Co.*, 404 U.S. 6, 10, 12 (1971)); *RJR Nabisco*, 136 S. Ct. at 2100–01. In finding that "privacy" is the focus of § 2703, Google errs (and the *Microsoft* panel erred) by looking at the SCA as a whole rather than by looking at the specific warrant provision in § 2703.[25] *See Microsoft II*, 855 F.3d at 75 (Droney, J., dissenting) ("When determining whether a statute applies extraterritorially, a court must read the statute provision by provision, not as a whole."). Consistent with the Supreme Court's stress on the specific statutory provision under review, the D.C. Circuit has

[25] Using "privacy" as the focus for an extraterritoriality analysis is as counterintuitive as it is wrong. As Judge Lynch wrote in his concurrence, privacy "is an abstract concept with no obvious territorial locus," and the panel majority's opinion thus "does not really help us to distinguish domestic applications of the statute from extraterritorial ones." *Microsoft I*, 829 F.3d at 230 n.7 (Lynch, J., concurring); *see also Microsoft II*, 855 F.3d at 61 (Jacobs, J., dissenting) ("But privacy, which is a value or a state of mind, lacks location, let alone nationality. Territorially, it is nowhere. Important as privacy is, it is in any event protected by the requirement of probable cause; so a statutory focus on privacy gets us no closer to knowing whether the warrant in question is enforceable." (footnote omitted)). Further, as discussed *infra*, even if the focus of the statute is "privacy," the conduct relevant to that focus is disclosure, *i.e.* where the provider responds to the government's demand and makes the customer's information available to the government.

noted that "[u]nder the presumption against extraterritoriality, the extraterritorial reach of a particular provision will not necessarily be imputed to an entire statute." *United States v. Ballestas*, 795 F.3d 138, 144 (D.C. Cir. 2015).

Contrary to the clear direction from the Supreme Court to examine the specific provision at issue, Google argues that the Court "should not narrowly confine its inquiry regarding the focus of the statute to a single, isolated subsection, but rather take into account the whole statute and related legislation," noting that in *Morrison*, the Supreme Court considered the prologue of the Securities Exchange Act, as well as the Securities Act of 1933, in determining the focus of § 10(b). *See* Objs. at 13 n.5 (citing *Morrison*, 561 U.S. at 267, 268). As the government points out, however, the *Morrison* court "looked beyond the specific provision for the express purpose of determining the focus of *that* section, § 10(b), not to determine the focus of the Exchange Act" as a whole. Gov't Opp'n at 39 n.16 (citing *Morrison*, 561 U.S. at 267–68).

Indeed, making the focus of the "statute" as a whole the lynchpin for the extraterritoriality analysis defies logic. If that were the correct approach, a whole host of issues would require resolution before beginning the analysis, such as which "statute" counts, since here the warrant provision at issue, § 2703, was part of the SCA, which in turn was part of ECPA. Must a court consider just the focus of the SCA or all of ECPA and its other titles as well? Further, where, as here, § 2703 has been substantively amended several times by other pieces of legislation, including the USA PATRIOT Act, would the approach urged by Google require consideration of those amending statutes as well as an assessment of any differing focus of provisions within those statutes? Following the Supreme Court's direction, as this Court is bound to do, fortunately avoids these issues since the focus inquiry necessarily turns on

examination of only the particular provision at issue—in this case, the warrant provision of § 2703.

The focus of § 2703 is plainly the "disclosure" of records or other information and electronic communications held by the provider for customers of the service. This is apparent from the very title of the provision—"Required disclosure of customer communications or records"—but also because "disclosure" is what "the statute seeks to 'regulate.'" *Morrison*, 561 U.S. at 267 (citing *Superintendent of Ins. of N.Y.*, 404 U.S. at 12). As Judge Lynch recognized, "parallel provisions" of the SCA uniformly allow the government to require "equivalent *disclosure*" of the communications by an administrative subpoena or by a court order, as long as notice is provided to the subscriber. *Microsoft I*, 829 F.3d at 227 (Lynch, J., concurring); *see* § 2703(b)(1)(B). These provisions are "not merely parallel—they all depend on the same verbal phrase." *Microsoft I*, 829 F.3d at 227 (Lynch, J., concurring). Section 2703 requires "disclosure" when the government obtains a subpoena, when it obtains a court order pursuant to § 2703(d), or when it obtains an SCA warrant. *See* 18 U.S.C. § 2703(b),(c),(d). No matter the type of legal process is used, or the requisite showing to be made, this statutory provision requires the service provider to "disclose" records and stored electronic communications of its customers, and bars suits against the service provider for "providing information, facilities or assistance" in compliance with orders, warrants or subpoenas issued under the SCA. 18 U.S.C. § 2703(e). Service providers are also required to preserve records and electronic communications, upon government request, pending issuance of an order or other process to ensure the information is available to be disclosed at a later date. *See id.* § 2703(f). As noted, it also specifies that an officer need not be present for service or execution of an SCA warrant "requiring disclosure." *Id.* § 2703(g). The repeated references to "disclosure" in § 2703

demonstrates that this provision "seeks to 'regulate'" *disclosure* of user information and "seeks to 'protect'" the government's ability to compel such disclosure. *Morrison*, 561 U.S. at 267 (quoting *Superintendent of Ins. of N.Y.*, 404 U.S. at 10, 12). Accordingly, the "focus" of § 2703 is "disclosure."

b) The Conduct Relevant to § 2703's Focus is "Disclosure"

Regardless of whether the focus of § 2703 is "privacy," "disclosure," or both, however, the *conduct* relevant to that "focus" is the same: disclosure. The *Microsoft* panel erred by assuming that if the focus of the statute was "privacy," then the provider's "access" to the user's electronic information was the conduct relevant to the focus of the statute. As Judge Cabranes explained in dissent, this assumption is belied by the language and structure of the SCA. Although § 2701 prohibits "unlawful access," service providers are specifically exempt from this provision in recognition of the fact that service providers must be able to "access" a customer's records and stored electronic communications. *See* 18 U.S.C. § 2701(c) (exempting from the provisions restricting access "conduct authorized . . . by the person or entity providing a wire or electronic communications service"). In other words, the SCA expressly authorizes Google's access to its customers' information and electronic communications stored on any of its servers anywhere in the world, and thus such access for transfer of such data among servers, domestic or foreign, does not implicate any protected privacy interest of the customer. *Microsoft II*, 855 F.3d at 68 (Cabranes, J., dissenting) (noting that Google "already had possession of, and lawful *access* to, the targeted emails from its office" in California).

Nevertheless, Google posits that the "searching, accessing, and retrieval of" its customers' records and electronic communications are all an "essential part of the statutory prerequisites for disclosing customer communications to the government" and, consequently,

conduct "relevant" to the SCA's focus. Objs. at 13. In Google's view, the Magistrate Judge "erred by reducing the process of assisting in the execution of a warrant to 'access[ing]' and 'copying' data from Google's headquarters in the United States." *Id.* at 15 (citing Mem. Op., 2017 WL 2480752, at *10). Rather, Google reasons, "[s]uch access and copying involves writing a query to search databases located in countries outside of the United States; executing the query to search for files and file components stored in said databases; seizing the files and file components; reassembling the file components into files; and then retrieving those communications to the United States for production to the government." *Id.*; *see also* Google's Reply at 19 (stating that the relevant conduct includes "when the provider assists in executing a warrant by searching foreign data centers, isolating communications pertaining to the subject accounts, and retrieving foreign-stored communications"). In sum, according to Google, the conduct "relevant" to the statute's focus includes not only the primary conduct regulated by the statute—disclosure—but also any preparatory acts necessary for effectuating that conduct. This argument fails for at least three reasons.

First, even assuming that Google's premise is correct—that preparatory acts necessary to effectuate the statutory provision's relevant conduct are relevant in evaluating the location of the conduct—all of the acts described by Google occur *in the United States.* As Google explains, only its personnel in the United States are authorized to "access" customer information "in order to produce it in response to legal process." Stip. ¶ 5. Thus, even if the information is stored in servers located abroad, Google searches for the information from the United States, retrieves copies of the information from the United States, and, most importantly, *discloses* the copies in the United States. Under this analysis, then, all of the preparatory conduct that Google strains to

place abroad, actually happens in the United States and constitutes a domestic application of the statute.

Second, even if some preparatory acts occurred abroad, no case law supports Google's position that any preparatory acts that are necessary prerequisites to the relevant conduct are themselves "relevant conduct" to the statute's focus. To the contrary, *RJR Nabisco* is explicit that "[i]f the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application *even if other conduct occurred abroad*." *RJR Nabisco*, 136 S. Ct. at 2101 (emphasis added); *see also Morrison*, 561 U.S. at 266 ("For it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States." (emphasis in original)). Google insists on rewording *RJR Nabisco*'s test to read that the "*only*" conduct "a court can safely ignore is . . . conduct that is *irrelevant* to the statute's focus." Google's Reply at 19 (emphasis in original). Put differently, Google argues that *any* foreign conduct relevant to a statute's focus—however remote—must be considered in determining whether the government's conduct at issue is an extraterritorial application of the statute. This is simply not what *RJR Nabisco* says. The *RJR Nabisco* test fully contemplates that conduct regulated by a statute may be preceded by preparatory or ancillary acts that occurred outside the United States.

Google's reading of *RJR Nabisco* would inexorably lead to an impractical rule impossible to apply. For example, as the government argues, in a prosecution for distribution of narcotics in the United States, the "cultivation, processing, manufacturing, packaging, shipping, payment for the supply, managing and supervision of the distribution" may all have occurred abroad, but such preparatory acts to the criminal conduct of illegal narcotics distribution in the United States do

not render the prosecution of drug offenses in the United States an extraterritorial application of the applicable statutes. *See* Gov't Opp'n at 48.

Third, Google's parsing of relevant conduct for the extraterritoriality analysis is impossible to square with *RJR Nabisco*'s clear text: "[i]f *the* conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if *other* conduct occurred abroad." *RJR Nabisco*, 136 S. Ct. at 2101 (emphasis added). "[T]he word 'the' was and is a definite article." *Noel Canning v. N.L.R.B.*, 705 F.3d 490, 500 (D.C. Cir. 2013) (citation omitted). "Unlike 'a' or 'an,' that definite article suggests specificity." *Id.*; *see also Am. Bus. Ass'n Slater*, 231 F.3d 1, 4–5 (D.C. Cir. 2000) ("It is a rule of law well established that the definite article 'the' particularizes the subject which it precedes. It is a word of limitation as opposed to the indefinite or generalizing force of 'a' or 'an.'"); *S.E.C. v. KPMG LLP*, 412 F. Supp. 2d 349, 387 (S.D.N.Y. 2006) ("The statute's use of the definite article 'the,' as opposed to the indefinite 'a,' 'an,' or 'any,' indicates that Congress intended the term modified to have a singular referent."). The Supreme Court could have stated that if *any* conduct relevant to the statute's focus occurred outside the United States, then an extraterritorial application of the statute occurs. The Supreme Court did not. Instead, the Supreme Court chose the definite article "the" to refer to the singular and primary conduct "relevant to the statute's focus." Thus, even if disclosure requires a series of necessary preparatory acts by the service provider, which acts may take place outside the United States, what matters for the *RJR Nabisco* and *Morrison* analysis is determining *the* conduct relevant to the statute's focus.[26] As discussed

[26] Google asserts that "the Court need not engage in the thorny question of how much of the conduct relevant to the SCA's focus must occur outside the United States before running afoul of *Morrison*: it need only hold that where a conduct is required in order for a statute to operate effectively, such conduct is relevant to the statute's focus." Google's Reply, at 23 n.8. As noted, Google provides no legal authority for this suggested holding and, for the reasons stated above, it runs directly counter to the directive of *RJR Nabisco.*

above, that conduct is the "disclosure" of customer information, and that takes place wholly inside the United States.[27]

4. The Troubling Consequences of Microsoft

Although not dispositive, the problematic repercussions of Google's and the *Microsoft* panel's interpretation of the SCA deserve comment. Under the guise of protecting privacy, Google's position undermines it, while at the same time impairing the government's ability to investigate and prosecute criminal activity. In particular, two key consequences stand out.

First, under the construction of the SCA adopted by the *Microsoft* panel and urged by Google, certain electronic communications held by providers would be impossible to obtain, thereby threatening time-sensitive criminal investigations. Under § 2703, the contents of an electronic communication that has been in electronic storage for less than 181 days may only be obtained with a warrant. 18 U.S.C. § 2703(a). While the government is generally able to use Mutual Legal Assistance Treaties ("MLATs") to obtain evidence located abroad, this process would likely be useless in seeking electronic communications held by service providers like Google.[28] Google's dynamic network architecture "automatically moves data from one location on Google's network to another as frequently as needed to optimize for performance, reliability, and other efficiencies," Stip. ¶ 4, such that the network may "change the location of data between the time when the legal process is sought and when it is served," *id.* By the time the MLAT

---

[27] The government also argues that the U.S. Senate's ratification of the Council of Europe Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (the "Cybercrime Convention"), demonstrates that Congress understands the SCA to allow the government to use SCA warrants to compel service providers to disclose information stored in servers located outside the United States. *See* Gov't Opp'n at 50–54. As it has already been determined that a such an SCA warrant is a domestic application of the SCA, the Court need not wade into the murky waters of whether the Senate's ratification of a treaty, twenty years after the enactment of a statute, can be used to interpret Congress's intent with respect to the original statute.

[28] As the government notes, the MLAT process is also "cumbersome, laborious, and time-consuming," and the United States does not have MLATs with many countries. Gov't Opp'n at 55 & n.26. Accordingly, resort to the MLAT process could "compromise time-sensitive investigations where expeditious retrieval of information is vital to the investigations' success." *Id.* at 56.

process had begun, any electronic communications targeted in an SCA warrant could have moved to a completely different country, making the effort to obtain this evidence a global game of whack-a-mole. Likewise, by virtue of the nature of Google's network, "[s]ome user files may also be broken into component parts, and different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time." *Id.* ¶ 3. Even if Google could determine where each of the different "shards" of information were located for a given customer's electronic communications, the government would be forced to seek legal process in multiple foreign jurisdictions. Most significantly, however, the MLAT process would be useless because, as Google states, the only personnel with the authority to access user communications are located in the United States. *Id.* ¶ 5; *see, e.g., In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *14 ("[I]t would be impossible for the Government to obtain the sought-after user data" stored by Google "through existing MLAT channels"). In other words, even if MLAT partners wished to help, the necessary assistance must come from U.S. based personnel.[29]

Second, the *Microsoft* decision may incentivize states to pass data localization laws to restrict their nationals from locating customer data abroad. If U.S. law does not permit U.S. law enforcement to obtain customer information stored on servers abroad, other countries may enact

[29] The *Microsoft* decision also threatens bilateral agreements for cross-border information requests. Last year, the administration transmitted to Congress a legislative proposal to amend ECPA to provide for bilateral agreements between the United States and foreign governments, primarily to effectuate a pending agreement between the United States and the United Kingdom. These agreements are meant to resolve problems posed for foreign governments investigating criminal activities in their own jurisdictions but require access to electronic evidence from U.S. service providers. *See* Letter from Peter J. Kadzik, Assistant Attorney General, to Joseph R. Biden, President, U.S. Senate, at 1 (July 15, 2016). Notably, "[i]n order for the United States to receive reciprocal benefits from such agreements, U.S. law must authorize law enforcement to obtain electronic data located abroad." *Id.* at 2. In other words, for the U.S.-U.K. agreement to take effect, and for the U.S. to receive the benefit of the agreement, U.S. law must permit law enforcement to compel service providers to disclose customer information stored in foreign servers. The *Microsoft* decision needlessly compromises such agreements by restricting the U.S. government from having access "necessary to advance important U.S. investigations that protect the safety of Americans and could not obtain reciprocal benefits from other countries." *Id.* at 3.

laws restricting where this information can be stored. Already, one major technology company is opening a data center in China to comply with the Chinese data localization law. *See* Paul Mozur, Daisuke Wakabayashi, and Nick Wingfield, *Apple Opening Data Center in China to Comply with Cybersecurity Law*, N.Y. TIMES, July 12, 2017. If *Microsoft* became the national policy, other countries may follow this path of requiring localization of data for access to electronic communications otherwise put out of law enforcement's reach, with concomitant adverse effects on network flexibility and privacy, especially since foreign surveillance laws may afford less privacy protection than U.S. law.

* * *

The Supreme Court has instructed that the lower courts may not engage in "judicial-speculation-made-law—divining what Congress would have wanted if it had thought of the situation before the court." *Morrison*, 561 U.S. at 261. The role of the courts is "to give the statute the effect its language suggests, however modest that may be; not to extend it to admirable purposes it might be used to achieve." *Id.* at 270. This admonition, however, does not mean that the courts are forbidden from emphasizing the policy outcomes of an erroneous decision and exposing the flaws in a party's reasoning. As stated above, Google's argument is premised on a notion that its position best aligns with the "privacy focus" of the SCA. It does nothing of the sort. This case is not about Google protecting customer privacy. In this case, the government complied with the probable cause standard, the most stringent form of privacy protection afforded by the Fourth Amendment, following scrutiny by a neutral magistrate. As stated by Judge Lynch in his concurrence, "[t]o uphold the warrant here would not undermine basic values of privacy as defined in the Fourth Amendment and in the libertarian traditions of this country." *Microsoft I*, 829 F.3d at 222 (Lynch, J., concurring).

This case is actually about whether courts can compel evidence stored by service providers on servers located abroad. The *Microsoft* panel's decision, and the position urged by Google, runs directly counter to well-established law that courts can do so and for good reasons. At the same time, the *Microsoft* decision does little to protect customer privacy and succeeds only in pouring molasses on the ability of the government to conduct lawful criminal investigations to protect the public.

IV. CONCLUSION

For the foregoing reasons, the Magistrate Judge's Order is AFFIRMED, as consistent with this Memorandum Opinion. The United States Attorney's Office is directed, by August 4, 2017, to review this Memorandum Opinion and advise the Court whether any portions should be redacted prior to filing on the public docket.

An appropriate order accompanies this Memorandum Opinion.

Date: July 31, 2017

BERYL A. HOWELL
Chief Judge