In the Matter of the Search of Content Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A

Case No. 16-mc-80263-RS.

United States District Court, N.D. California.

August 14, 2017.

Google Inc., Movant, represented by Julie Erin Schwartz, Perkins Coie, LLP.

Google Inc., Movant, represented by John Randall Tyler, Perkins Coie LLP, pro hac vice & Todd M. Hinnen, Perkings Coie LLP, pro hac vice.

Microsoft Corporation, Interested Party, represented by Brian Philip Goldman, Orrick, Herrington Sutcliffe LLP, Robert M. Loeb, Orrick Herrington Sutcliffe LLP, pro hac vice, Alexander Berengaut, Covington and Burling LLP, pro hac vice, Devon Lee Mobley-Ritter, Covington Burling LLP, E. Joshua Rosenkranz, Orrick Herrington Sutcliffe LLP, pro hac vice, Evan Michael Rose, Orrick, Herrington, and Sutcliffe, Hannah Garden-Monheit, Orrick Herrington Sutcliffe LLP, pro hac vice, James M. Garland, Covington and Burling LLP, pro hac vice & Katharine Reams Goodloe, Covington and Burling LLP, pro hac vice.

Amazon.Com, Inc., Interested Party, represented by James M. Garland, Covington and Burling LLP, pro hac vice, Alexander Berengaut, Covington and Burling LLP, pro hac vice, Devon Lee Mobley-Ritter, Covington Burling LLP & Katharine Reams Goodloe, Covington and Burling LLP, pro hac vice.

Apple Inc., Interested Party, represented by Brian Philip Goldman, Orrick, Herrington Sutcliffe LLP, Robert M. Loeb, Orrick Herrington Sutcliffe LLP, pro hac vice, E. Joshua Rosenkranz, Orrick Herrington Sutcliffe LLP, pro hac vice, Evan Michael Rose, Orrick, Herrington, and Sutcliffe & Hannah Garden-Monheit, Orrick Herrington Sutcliffe LLP, pro hac vice.

Cisco Systems, Inc., Interested Party, represented by Brian Philip Goldman, Orrick, Herrington Sutcliffe LLP, Robert M. Loeb, Orrick Herrington Sutcliffe LLP, pro hac vice, E. Joshua Rosenkranz, Orrick Herrington Sutcliffe LLP, pro hac vice, Evan Michael Rose, Orrick, Herrington, and Sutcliffe & Hannah Garden-Monheit, Orrick Herrington Sutcliffe LLP, pro hac vice.

United States of Amreica, Miscellaneous, represented by Brian Joseph Stretch, U.S. Attorney's Office, Andrew Sun Pak, U.S. Department of Justice, Catherine Alden Pelker, Department of Justice, Kathryn R. Haun, Merry Jean Chan, U.S. Attorney's Office & William Frentzen, U.S. Attorney's Office, NDCA.

ORDER DENYING GOOGLE'S MOTION FOR *DE NOVO* DETERMINATION OF DISPOSITIVE MATTER REFERRED TO MAGISTRATE JUDGE

RICHARD SEEBORG, District Judge.

I. INTRODUCTION

Google objects to the magistrate judge's order denying its motion to quash a search warrant seeking foreign-stored e-mails. It claims execution of the warrant would be an impermissible extraterritorial application of the Stored Communications Act ("SCA" or "the Act"), 18 U.S.C. § 2701 *et seq.* For the reasons that follow, the magistrate judge's order is affirmed and Google is ordered to comply fully with the terms of the warrant.

II. BACKGROUND

A. Factual Background

Google is a domestic company incorporated in Delaware with a principal place of business in California. It offers users a variety of different online and communications services. Google stores user data in various locations, some inside the United States and some elsewhere. Google's network automatically moves data from one storage location to another as frequently as needed to optimize performance, reliability and other efficiencies. As a result, the countries in which specific user data is stored may change over time. It is possible, for example, that the network will change the location of data between the time when the legal process is sought and when it is served. Only Google personnel in Google's Legal Investigations Support team are authorized to access the content of communications in order to produce it in response to legal process. All such Google personnel are located in the United States.

B. Procedural Background

On June 30, 2016, the magistrate judge authorized a search warrant, under 18 U.S.C. § 2703(a), directing Google to produce stored content related to certain email accounts. Google moved to quash with respect to content stored outside the United States. The magistrate judge denied that motion and ordered Google to produce all content responsive to the search warrant that is retrievable from the United States, regardless of the data's actual location. *See* Dkt. No. 46. Google now moves for *de novo* review of the magistrate judge's determination. The government opposes Google's motion and requests an order to show cause why Google should not be held in contempt for failure to comply with the magistrate judge's order.

C. Statutory Background

The SCA was enacted as Title II of the Electronic Communications Privacy Act of 1986. It imposes general obligations of non-disclosure on service providers and creates several exceptions to those obligations. The first three sections of the SCA—Sections 2701, 2702, and 2703— contain its major provisions. Section 2701 criminalizes unauthorized access of a facility through which an electronic communication service is provided. Section 2702 outlines the circumstances in which service providers may voluntarily disclose information associated with and contents of electronic communications. Section 2703 sets forth procedures the government must use to require service providers to produce customer communications and records. Basic subscriber information can be obtained by an administrative subpoena. *See* 18 U.S.C. § 2703(c)(2). Other non-content records can be obtained by a court order (a "§ 2703(d) order"). *See id.* § 2703(c)(2), (d). To obtain the content of electronic communications, stored recently (i.e., for less than 180 days), the government must secure a warrant that has been issued using the procedures described in the Federal Rules of Criminal Procedure. *See id.* § 2703(a). For older electronic communications, a warrant is only required if the government does not provide notice to the subscriber or customer. *See id.*§ 2703(b)(1)(B).

III. LEGAL STANDARD

It is not obviously clear where this matter falls within the scope of 28 U.S.C. § 636 and thus which standard of review applies. The parties agree that *de novo* review should apply and, indeed, *de novo* review seems most appropriate both because the matter is analogous to a dispositive motion, *see Strong v. United States,* 57 F. Supp. 2d 908, 913-14 (N.D. Cal. 1999), and because courts have routinely held that the exercise of a magistrate judge's powers under § 636(b)(3) are accorded *de novo* review. *See In re Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.,* No. 16-MJ-00757 (BAH), 2017 WL 3445634, at *4 (D.D.C. July 31, 2017) ("*In re Search*"). Accordingly, the magistrate judge's order is reviewed *de novo.*

IV. DISCUSSION

A. Motion For *De Novo* Review

The central question here is whether the execution of a search warrant for foreign-stored communications, issued under the SCA, constitutes an extraterritorial application of that statute. The Second Circuit appears to be the only court of appeal thus far to have considered this issue. *See In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.,* 829 F.3d 197 (2d Cir. 2016) ("*Microsoft I*"), *reh'g denied en banc,* 855 F.3d 53 (2d Cir. Jan. 24, 2017) ("*Microsoft II*"). In *Microsoft I,* a unanimous panel held that such a warrant constitutes an unlawful extraterritorial application of the SCA. In a split 4 to 4 decision, the Second Circuit denied the government's petition for rehearing *en banc.*[1] Since then, apparently every other court to consider the issue has rejected the holding of *Microsoft. See In re Search,* 2017 WL 3445634, at *5.

To decide whether the presumption against extraterritoriality limits the reach of a statutory provision in a particular case, courts apply a two-part test. *See Morrison v. National Australia Bank Ltd.,* 561 U.S. 247, 261-70 (2010). At the first step, courts ask "whether the statute gives a clear, affirmative indication that it applies extraterritorially." *RJR Nabisco, Inc. v. European Cmty.,* 136 S. Ct. 2090, 2101 (2016). If not, courts determine "whether the case involves a domestic application of the statute." *Id.* They do this by looking to the statute's focus. "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.*

In this case, the magistrate judge found, at step one, that section 2703 does not contemplate or permit extraterritorial application. At step two, she decided that the conduct relevant to the SCA's focus takes place inside the United States. Not surprisingly, Google does not object to the magistrate judge's decision at step one. Rather, the parties' dispute centers on step two. Relying on *Microsoft,* Google argues that the SCA's focus is user privacy and that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed." 829 F.3d at 56. The magistrate judge, however, followed as

persuasive the analysis of the dissenters in *Microsoft II.* She reasoned that the conduct relevant to the focus of the SCA is the disclosure of the data in the service provider's possession and that such disclosure happens where Google accesses and delivers the information—i.e., in the United States. She further reasoned that, even assuming the SCA's focus is privacy, the warrant requirement protects that interest. She thus concluded that, "[i]f statutory and constitutional standards are met, it should not matter where a service provider chooses to store the 1's and 0's." Order at 8 (citing *Microsoft II,* 855 F.3d at 61-62 (Jacobs, J. dissenting)).

Before considering the propriety of the magistrate judge's extraterritoriality analysis, it must be noted that the SCA warrant here can be properly characterized as "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.'" *In re Search,* 2017 WL 3445634, at *14. Courts have the power to exercise authority on entities over whom they have personal jurisdiction, including compelling those entities to retrieve data from abroad. *See id.* (citing *Blackmer v. United States,* 284 U.S. 421, 438 (1932)). A statute may thus authorize courts to issue orders compelling an entity within its enforcement jurisdiction to produce records located abroad that are relevant to an offense committed in the United States. *See id.* at *15 (citing *United States v. Bank of Nova Scotia,* 730 F.2d 817, 828 (11th Cir. 1984)).[2] As explained in *In re Search,* "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." *Id.* at *17. Accordingly, as an initial matter, Google is obligated to comply with the warrant as a proper exercise of the court's enforcement jurisdiction.

The extraterritoriality analysis compels the same conclusion. Sections 2702 and 2703 clearly concern the disclosure of customer communications; indeed, they are titled "Voluntary Disclosure" and "Required Disclosure," respectively. While Section 2701 relates to unauthorized access, it recognizes that providers have authority to access customers' electronic communications. Thus, considering sections 2701, 2702, and 2703 together, "it is clear that the SCA protects user privacy by prohibiting unlawful access of customer communications (such as hacking), and by regulating a provider's disclosure of customer communications to third parties." *Microsoft II,* 855 F.3d at 68 (Cabranes, J. dissenting). To the extent the statute focuses on privacy, the focus is on disclosures to third parties, not on the provider's access to user data. Section 2701 expressly exempts from its prohibition of unlawful access conduct authorized by the "entity providing a wire or electronic communications service." 18 U.S.C. 2701(c)(1).

Google claims that conduct relevant to the focus of the SCA occurs outside the United States because (1) the searching, accessing and retrieval of foreign-stored communications intrudes on user privacy and (2) such acts are essential to the statutory prerequisites for disclosure. As to the intrusion on user privacy, the conduct relevant to the SCA's focus is a provider's disclosure or non-disclosure of emails to third parties, not a provider's access to a customer's data. *See* 18 U.S.C. 2701(c)(1). Moreover, Google's mere access and retrieval of foreign-stored data does not amount to an infringement of a user's reasonable expectation of privacy or a meaningful interference with a user's possessory interests, *see United States v. Jacobsen,* 466 U.S. 109, 113 (1986), and, furthermore, the warrant requirement fully protects user privacy.

As to the question of whether Google is undertaking essential aspects of compliance with section 2703 outside the United States, the answer is no. As a factual matter, the information sought by the government is easily and lawfully accessed in the United States, and disclosure of that content would likewise take place in the United States. Indeed, only personnel in Google's Legal Investigations Support team are authorized to access the content of communications in order to produce it in response to legal process and all such Google personnel are located in the United States. *See* Dkt. No. 37, 5.[3] Accordingly, the conduct relevant to the SCA's focus occurs in the United States. *See RJR Nabisco,* 136 S. Ct. at 2101 ("If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad.") The conduct allegedly occurring abroad—i.e., Google's accessing of foreign-stored e-mails—is not relevant to the focus of the SCA because section 2701 specifically excludes providers from the statute's prohibitions against access to stored communications.

Google insists the magistrate judge engaged in "judicial-speculation-made-law," *Morrison,* 561 U.S. at 261, when she decided how the SCA should apply to the world of "cloud" computing, which did not exist when Congress enacted the statute. This argument, however, conflates the two prongs of the *Morrison* analysis, *see Microsoft II,*855 F.3d at 74, and, in any event, the magistrate judge's decision is based on a reasonable statutory interpretation, not on a policy determination. Moreover, while not dispositive, the policy implications of Google's interpretation of the SCA are worth noting. Because Google automatically moves data from one location to another to optimize efficiencies, Google's interpretation would render United States warrant authority arbitrarily confined based on where the data is located pursuant to an algorithm, not any territorially meaningful storage decision. Additionally, 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 because by the time the MLAT process had begun, any electronic communications targeted in an SCA warrant could have moved to a completely different country. *See In re Search,* 2017 WL 3445634, at *26.

Of course, government requests for communications of foreign citizens or residents raise serious international relations concerns. In his concurrence in *Microsoft I,* Judge Lynch argued persuasively, while it is not clear that it matters whether the customer is a United States person or not under the rather simplistic "focus" test adopted by the Supreme Court in *Morrison,* "it *should* matter." *Microsoft I,* 829 F.3d at 230 (emphasis in original). On this basis, he suggested that the relevant conduct, for purposes of the *Morrison* step two analysis, is the invasion of privacy which occurs where the person whose privacy is invaded customarily resides. *Id.* Yet, here, as in *Microsoft,* the record does not establish the nationality of the customer whose emails are sought. Judge Lynch was ultimately persuaded that the warrant in *Microsoft* was nevertheless an extraterritorial application of the SCA because that case "could well be [] one of . . . records stored at the behest of a foreign national on servers in his own country." *Microsoft I,* 829 F.3d at 230. This case, however, is different. While Microsoft's storage algorithm is based on the user's self-reported location, Google's equivalent has no territorial tether. As such, there is no basis for concluding that this case "could well be" one involving "records stored at the behest of a foreign national on servers in his own country." *Id.* Relatedly, "the interests of foreign internet electronic communication service providers, whose headquarters are abroad and whose customers choose to subscribe to those services with the knowledge that the provider is located outside the United States are not at stake here." *Microsoft II,* 855 F.3d at 76 (Droney, J. dissenting). While the policy concerns raised by the parties are significant and require the attention of Congress, Google has failed to show that it is being compelled to perform conduct relevant to the SCA's focus outside the United States.

B. Request for Order to Show Cause

The government asks the court to issue an order to show cause why Google should not be held in contempt for refusing to comply with the search warrant and the magistrate judge's order. The government made a similar request to the magistrate judge and she declined to grant it. *See* Dkt. No. 31 ("The court is confident that the parties can work out their differences without court intervention but remains available to help if they cannot. The parties must raise any disputes via the joint letter process in the court's standing order, which is attached."). The government did not seek review of the magistrate judge's order, nor has it sought to avail itself of the joint letter process described in the standing order. Further, Google sought review of the magistrate judge's order less than one week after the magistrate judge issued her amended order. In light of the Second Circuit decision in *Microsoft* and the absence of relevant Ninth Circuit precedent, Google's diligent, good faith efforts to comply with current law do not warrant contempt at this stage of the proceedings.

V. CONCLUSION

The magistrate judge's order is affirmed and Google is ordered to produce all content responsive to the search warrant that is accessible, searchable, and retrievable from the United States pursuant to the terms of the warrant. The government's request for an order to show cause is denied.

IT IS SO ORDERED.

[1] Given the recent wave of motions being filed in analogous cases across the country, basic familiarity with the *Microsoft* decision is assumed and the arguments presented therein are not described in detail here.

[2] Google argues that Congress used the term "warrant" in section 2703 to convey a territorial limitation. As others have noted, however, an SCA warrant does not appear to be a traditional search warrant. "The SCA does not describe the warrant as a search warrant. Nor does it 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). "Rather, the statute expressly requires the `warrant' not to authorize a search or seizure, but as the 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." *Id.* at 227. Moreover, the nature of the records demanded is different from that of the physical documents sought by traditional search warrants. *See id.; see also Microsoft II,* 855 F.3d at 61 (Jacobs, J. dissenting) ("At stake in this case is not whether Microsoft can be compelled to import and deliver a disk [], but whether Microsoft can be compelled to deliver information that is encoded on a disk in a server and that Microsoft can read.").

[3] The government argues that the Senate's ratification of the Cybercrime Convention in 2006 further suggests that Congress intended the SCA to require a provider in the United States to disclose foreign-stored data in its custody or control. Google responds that ratification of a treaty expresses the will of the Senate only and that "`the views of a subsequent Congress form a hazardous basis for inferring the intent of an earlier one,'" *Waterman S.S. Corp. v. United States,* 381 U.S. 252, 269 (1965), especially where, as here, so much time has passed between enactment of the SCA and ratification of the Convention. Because the magistrate judge's decision rests on sound statutory analysis, this secondary argument need not be reached.

End of Document.