IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

In re Search Warrant No. 16-960-M-1 to Google	**:**	**Magistrate No. 16-960-M-1**
	:	
In re Search Warrant No. 16-1061-M to Google	**:**	**Magistrate No. 16-1061-M**
	:	

Brief of Google Inc. In Support of Objections to Magistrate Judge's Order Granting the Government's Motions to Compel

I. Introduction

This matter involves two warrants issued under the Stored Communications Act ("SCA") that purport to require Google Inc. ("Google") to search for customer communications and seize them for the government. Google has, to the best of its current capabilities, searched its data centers in the United States, seized the customer communications within the scope of the warrants, and produced those communications to the government. The question raised by this matter is whether those warrants also require Google to search for customer communications stored in data centers located outside the United States, and seize those communications for the government despite the fact that the warrant does not and could not authorize the government to conduct directly that same search and seizure.

The United States Court of Appeals for the Second Circuit, the only Circuit Court to have addressed the issue, properly held that an SCA warrant cannot compel a service provider to search data centers and seize customer communications located outside the United States. Congress did not consider when enacting the SCA the complex policy issues that such foreign searches and seizures raise, and the statute gives no indication that a warrant issued under its terms requires a provider to engage in extraterritorial searches and seizures. Under the

presumption against extraterritoriality, a well-established canon of statutory interpretation, a statute does not apply to conduct outside the United States absent clear indication that Congress intended it to do so.

Despite the Supreme Court's repeated emphasis in recent years on the importance of the presumption against extraterritoriality, the magistrate judge's decision fails to apply that presumption properly. He held that a provider's search and seizure of customer communications stored outside the United States did not constitute extraterritorial conduct relevant to the focus of the SCA. That holding is incorrect. The SCA is focused on protecting the privacy of electronic communications entrusted to service providers by regulating the conditions under which access to those communications may or may not occur. The invasion of privacy occasioned by the execution of a warrant to access and retrieve such communications is certainly relevant to that statutory focus.[1]

That interpretation no doubt implicates many policy questions, as do the interpretations the government and the magistrate judge have offered. Thirty-one years ago, when Congress enacted the SCA, the Internet was in its infancy. Public access to the Internet would not be available for another three years. *See* InfoWorld, Vol. 11, Issue 39 at 32 (Sept. 25, 1989) (reporting availability of first public gateways to the Internet). Congress did not foresee the

[1] Congress established in the SCA *independent statutory restrictions* on the government's ability to compel providers to access, retrieve, and disclose customers' private communications. *See Sams v. Yahoo*, 713 F. 3d 1175, 1179 (9th Cir. 2013) (the purpose of the SCA is "to protect the privacy of electronic communications" in part by "placing limits on the government's ability to compel network service providers to disclose information they possess about their customers and subscribers [via] 18 U.S.C. § 2703"); *see also U.S. v. Graham*, 824 F. 3d 421, 438 (4th Cir. 2016) (the SCA "creates a set of Fourth Amendment-like privacy protections by statute") (quoting *Sams*). The key question therefore is whether the warrants required Google to engage in conduct relevant to those statutory restrictions outside the United States.

more-than-3-billion-user global network supporting myriad communication, personal, and commercial services that the Internet has become, nor did it consider the complex and conflicting policy and international diplomatic issues raised by government requests for communications stored on such a worldwide network.

Congress should consider these difficult policy issues, hear from all stakeholders in an open, public debate, and reform and modernize the statute. A court, confined as it is to the single case or controversy before it, has neither the institutional competence nor the constitutional authority to amend the law. The magistrate judge overstepped these bounds when he read into the statute an extraterritorial application -- the ability to require a provider to assist the government in executing a warrant to search and seize private customer communications stored outside the United States -- that Congress did not inscribe there.

The Court should leave to Congress the legislative responsibility of amending the SCA, give effect to its plain language, and hold that a warrant issued pursuant to its terms cannot require a service provider to search and seize customer communications stored in data centers located outside the United States.

II. Argument

A. The SCA's Warrant Provision Does Not Apply Extraterritorially.

"[L]egislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 254 (2010). The magistrate judge held, and the government concedes, that the SCA's warrant provision indicates no such contrary intent and was meant to have no application outside the United States. *See In re Search Warrant No. 16-960-01 to Google*, 2017 WL 471564 at *7 (E.D.Pa. Feb. 3, 2017); United States Reply to Google's Response ("Reply") at 13.

Congress did not intend the SCA's warrant provision to apply outside the United States. As the Second Circuit observed, "a globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future" when Congress passed the SCA. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197, 206 (2d Cir. 2016) ("*Microsoft*"). Congress therefore had no occasion to extend the SCA's warrant provision outside the United States, and nothing in the SCA's text or legislative history indicates that it intended to do so.

To the contrary, Congress distinguished between a "warrant," which it generally required the government to obtain before compelling a provider to search, retrieve, and disclose customers' private communications, and a "subpoena" or an "order," which it required the government to obtain before compelling a provider to disclose its own business records. *Compare* 18 U.S.C. § 2703(a) *with* § 2703(c). The distinction was designed to do more than require the government to make a probable cause showing to obtain user content; the Wiretap Act, amended by the legislation that created the SCA, had addressed a similar concern regarding the interception of customers' communications by setting forth a procedure by which the government can apply for, and a court can grant, *an order issued on a finding of probable cause* requiring a provider to intercept communications. *See* 18 U.S.C. § 2518(3).[2]

Instead, Congress used the term of art "warrant" to invoke the traditional limitations and protections long associated with that term. *See F.A.A. v. Cooper*, 132 S. Ct. 1441, 1449 (2012) ("[W]hen Congress employs a term of art, 'it presumably knows and adopts the cluster of ideas

[2] Congress also demonstrated in the SCA that it could create specialized types of orders requiring providers to disclose information about their customers. *See* 18 U.S.C. § 2703(d). If it intended to create a probable cause order for the disclosure of communications content in the SCA, it would have done so.

that were attached to each borrowed word in the body of learning from which it was taken.'") (quoting *Molzof v. United States*, 502 U.S. 301, 307 (1992)). Congress understood that the private content of stored communications was protected by the Fourth Amendment, and that accessing them would entail a search and seizure. *See* H.R. Rep. No. 99-647, at 68 (1986) ("The Committee required the government to obtain a search warrant because it concluded that the contents of a message in storage were protected by the Fourth Amendment."). Among the traditional limitations and protections associated with warrants are their territorial limitations; they may only authorize searches and seizures to be conducted in the United States. *See U.S. v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990) (holding that a warrant "would be a dead letter outside the United States"); *Microsoft*, 829 F.3d at 212 ("a warrant protects privacy in a distinctly territorial way"). It 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.[3]

To the extent subsequent amendments to the SCA's warrant provision are relevant to its interpretation, they confirm that the traditional territorial limitations associated with warrants are

[3] While Rule 41 was modified on December 1, 2016, to permit magistrate judges to issue warrants to search out-of-district electronic information in certain circumstances not relevant here, nothing in the amended Rule contemplates a search of property that is or may be located outside the country. As the Department of Justice acknowledged in a letter to Advisory Committee on the Criminal Rules, "[i]n light of the presumption against international extraterritorial application, and consistent with the existing language of Rule 41(b)(3), this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries." Letter from Mythili Raman, Acting Assistant Attorney General, to Judge Reena Raggi, Chair Advisory Comm. on the Criminal Rules (Sep. 18, 2014) (available at https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf). Accordingly, the government cannot obtain a search warrant to search property outside the United States.

incorporated into the SCA's warrant provision. In 2001, Congress amended the SCA to extend the authority of SCA warrants issued by federal courts from their traditional territorial limits with the federal district of the issuing court to anywhere within the United States. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107-56, § 220 (codified as amended at 18 U.S.C. § 2711(3)) (requiring provider to comply with warrant issued by any federal court with jurisdiction over offense being investigated). Congress did not, however, extend the authority of SCA warrants to require retrieval of communications stored outside the United States. Where Congress intended to alter or modify the established practices applicable to a warrant, it did so expressly. *See* 21st Century Department of Justice Appropriations Authorization Act, Pub. L. No. 107-273, § 11010 (codified at 18 U.S.C. § 2703(g)) (providing that law enforcement officer does not have to be present for service or execution of SCA warrant). The SCA's use of the term of art "warrant" and its legislative history reflect a clear intent by Congress to limit the searches and seizures that may be required under the SCA to locations in the United States.

The SCA's warrant provision therefore compels a service provider to search and seize electronic communications only within the territorial jurisdiction of the United States. The SCA's warrant provision has no force or effect outside the United States. *See Morrison*, 561 U.S. at 254. ("When a statute gives no clear indication of an extraterritorial application, it has none.").

B. Requiring a Provider to Execute a Warrant to Search and Seize Data Outside the United States is an Impermissible Extraterritorial Application of the SCA.

When a statutory provision such as the SCA warrant provision has no extraterritorial reach, any application of it to conduct outside the United States that is relevant to the statute's focus constitutes "an impermissible extraterritorial application regardless of any other conduct

that occurred in U.S. territory." *RJR Nabisco, Inc. v. European Community*, 136 S.Ct. 2090, 2101 (2016). The SCA's focus is on protecting the privacy of electronic communications by ensuring that intrusions on that privacy occur only pursuant to the detailed requirements and limitations of the statute. When a warrant requires a provider to assist in its execution by searching and seizing customer communications, that search and seizure is conduct relevant to the SCA's focus. Requiring Google pursuant to the warrants to search and seize customer communications located on its servers outside the United States would thus constitute an impermissible extraterritorial application of the SCA.

1. The SCA's Focus Is Protection of the Privacy of Electronic Communications.

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. Senator Leahy, one of the SCA's authors, described its purpose as "update[-ing] our legal privacy protections [to] bring[] them in line with modern telecommunications and computer technology." 132 Cong. Rec. S7991 (daily ed. June 19, 1986) (statement of Sen. Leahy). As the Department of Justice observed in guidance issued prior to this litigation, the SCA "sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers." *See Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. Department of Justice, Executive Office of the United States Attorneys at 115 (Aug. 2009); *see also* S. Rep. No. 99-541, at 5 (1986) ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment."), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

To achieve this purpose, Section 2701 protects the privacy of electronic communications by criminalizing unauthorized access to such communications stored by a service provider. *See*

18 U.S.C. § 2701. Section 2702 protects the privacy of electronic communications by prohibiting service providers from voluntarily disclosing such communications, except under expressly enumerated circumstances. *See id.* § 2702. And Section 2703 protects the privacy of electronic communications by requiring the government to obtain a subpoena, an order, or a warrant before compelling a provider to disclose subscriber information, records regarding the use of a communications service, or the contents of communications, respectively. *See id.* § 2703. "The privacy protections contained in 18 U.S.C. §§ 2702 and 2703 provide the heart of the SCA." Kerr, *A User's Guide*, at 1218.[4] Privacy is, in the words of the *Morrison* Court, "the object[] of the statute's solicitude." *Morrison*, 561 U.S. at 267 (identifying certain transactions as the object of the Exchange Act's solicitude); s*ee also Microsoft*, 829 F.3d at 217 (privacy is the focus of the SCA).

2. Executing an SCA Warrant Is Conduct Relevant to the Focus of the SCA.

Section 2703, under which the warrants were issued, protects the privacy of electronic communications by requiring that the government may compel a provider to search, seize, and disclose such communications to the government only pursuant to a warrant issued upon a showing of probable cause.[5] The searching, accessing, and retrieval of communications compelled by the warrant affect users' privacy, and they are an essential part of the statutory prerequisites for disclosing customer communications to the government.

---

[4] The court should not, as the government has suggested, narrowly confine its inquiry regarding the focus of the statute to a single, isolated subsection, but rather can take into account the whole statute and related legislation. *See Morrison* at 267 (taking into account the prologue of the Exchange Act in determining its focus); 268 (taking into account the related Securities Act of 1933).

[5] Although section 2703(b) provides that the government may use lesser legal process for certain types of communications under certain conditions, that subsection of the SCA has been found to be unconstitutional. *See U.S. v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

Congress chose to protect the privacy of basic subscriber information, records regarding the use of an electronic communications service, and the communications themselves with three distinct forms of legal process. *See* 18 U.S.C. § 2703. For the first category, which it deemed least private, it chose a subpoena; for the second, it chose a court order; and for the third, the content of communications, which it deemed most private, it chose "the full protection of a warrant." *See* Kerr, *Next Generation* at 384.

Unlike the subscriber information obtained with a subpoena or the customer records obtained with a court order, the communications obtained with a warrant are not the provider's business records or information conveyed to the provider by the customer; they are the customer's private communications, and obtaining them entails a search and a seizure in a sense not implicated by the other two categories of data. *See U.S. v. Bach*, 310 F.3d 1063, 1067 (8th Cir. 2002) (describing Yahoo!'s fulfillment of an SCA warrant as "the search and seizure of Bach's email from Yahoo!'s server by Yahoo!'s technicians"). This distinction is critical. It renders the government's analogy between a subpoena or order used to compel production of business records and a warrant inapt, and the precedent cited in support thereof inapposite. *See* Reply at 5-8. The government does not cite a single decision supporting its argument that a warrant operates similarly. *See id.*

The 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. *See U.S. v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (distinguishing

between business records of a third party and customers' private communications held in trust by communications providers and finding the latter are entitled to Fourth Amendment privacy protections); *Stoner v. California*, 376 U.S. 483, 489 (1964) (holding that searching a hotel room without a warrant violated the Fourth Amendment). As noted above, however, a warrant cannot require the search of a foreign place and the seizure of things stored therein.[6]

As the Eighth Circuit has noted, "Congress called them warrants and we find that Congress intended them to be treated as warrants." *Bach,* 310 F.3d at 1066 n.1. Established rules of statutory interpretation require no less, *Connecticut Nat. Bank v. Germain*, 503 U.S. 249, 253-54 (1992) ("[C]ourts must presume that a legislature says in a statute what it means and means in a statute what it says there."), and the magistrate judge erred when, despite Congress's use of the term "warrant," he treated SCA warrants instead like subpoenas or court orders.

When an SCA warrant requires a provider to search, seize, and disclose to the government customer communications, the execution of the warrant by accessing and retrieving communications is "conduct relevant to the focus" of the SCA. And because the government here seeks to conscript Google to execute a warrant outside the United States, "the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory." *RJR Nabisco*, 136 S.Ct. at 2101.

---

[6] The Supreme Court has recognized that when conducting a search and seizure of private communications, location matters. In *Riley v. California*, 134 S.Ct. 2473 (2014), the Court addressed whether law enforcement could search the phone of a suspect incident to that suspect's arrest. The Court distinguished between searching communications stored locally on the suspect's phone and searching the suspect's "data located elsewhere . . . on remote servers," noting that the latter "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house." *Id.* at 2491. Like the search the Court cautioned against in *Riley*, the search the government proposes in this case of a location outside the United States raises significant and distinct policy and privacy issues that Congress has not considered or addressed.

C. The Magistrate Judge Usurped the Role of the Legislature, Weighing Policy Interests Congress Has Not Yet Considered.

This case, and others like it, raise important policy issues regarding how best to protect the privacy of electronic communications and law enforcement's ability to investigate crimes when evidence may reside within a borderless, distributed, global communications network. Adjusting the SCA to this changed landscape will require resolution of numerous policy issues. For example, Congress might choose to extend the SCA's warrant power only to U.S. citizens' data wherever stored to encourage other nations to limit their laws applied to their providers similarly, and thus protect U.S. citizen data wherever it may be stored against disclosure to foreign law enforcement. Congress might choose to extend the SCA's warrant power to data wherever located, but require the government to provide notice to the government of the customer's country of nationality or residence before serving such a warrant on the provider. Or Congress might choose to allow execution of SCA warrants overseas when ordered by a federal court, but not by state or local courts.[7] Because Congress did not consider those issues when it

[7] Congress might also craft legislation that takes into account the potential that allowing the U.S. government to search communications stored outside the United States "will significantly deter the use of remote data management technologies by business and individuals, particularly their use of U.S. cloud services providers, and thereby undermine a significant contributor to U.S. economic growth." Brief of BSA: the Software Alliance et al. as Amici Curiae Supporting Appellant, Microsoft Corp. v. U.S., 829 F.3d 197 (2d. Cir. 2016) (No. 14-2985), 2014 WL 7213177. Indeed, both Congress and the government have acknowledged the need for legislation to address some of these complex and conflicting policy issues. This is a fact well appreciated by the Members of Congress who have introduced a bill proposing related amendments. *See* International Communications Privacy Act, S. 2986, H.R. 5323, 114th Cong. (2016); Letter from Assistant Attorney General Peter J. Kadzik, Department of Justice Office of Legislative Affairs, to Hon. Joseph A. Biden, President of the Senate, July 15, 2016 (proposing to Congress legislation to address "potential conflicting legal obligations that U.S. electronic communications service providers . . . may face when required to disclose electronic data by foreign governments investigating serious crime, including terrorism"), available at https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf.

enacted the SCA, the statute does not address them. *See* Kerr, *Next Generation* at 410 ("ECPA simply was not written with the territoriality problem in mind."). The temptation to interpret the statute to extend beyond the scope Congress gave it in order to resolve important policy questions Congress did not anticipate is understandable, but it is not proper for a court to do so.

The magistrate judge's decision's legislative bent is revealed throughout the opinion, and in its occasional admission that the magistrate judge engaged not just in interpreting and applying statutory text, but in the broader, legislative inquiry of balancing competing policy considerations. *See In re Search Warrant No. 16-90-M-01 to Google*, 2017 WL 471564 at *12 ("Before a court bars the Government from using a judicially approved search warrant to require disclosure of user data that constitutes evidence of crimes, it would do well not to be controlled by possibilities and legal abstractions, but to focus instead on realities."); *id.* at *12 ("[N]o foreign nation's sovereign interest will be interfered with in any ascertainable way"); *id.* at *14 ("if the court were to adopt Google's interpretation of the Microsoft decision . . . it would be impossible for the Government to obtain the sought-after user data through existing MLAT channels."). The decision does not apply the plain language of the SCA; it instead engages in broad consideration of competing interests such as foreign sovereignty, comity, and the government's ability effectively to use the MLAT process.

The Supreme Court has admonished lower courts not to engage in such "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 proper role of the judiciary is instead "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. As with RICO in *RJR Nabisco*, the proper question regarding the SCA in this case is "not whether we think 'Congress

would have wanted' a statute to apply to foreign conduct 'if it had thought of the situation before the court,' but whether Congress has affirmatively and unmistakably instructed that the statute will do so." *RJR Nabisco*, 136 S.Ct. at 2100 (internal citations omitted); *see also Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957) (Congress "alone has the facilities necessary to make fairly [the] important policy decision" whether a statute applies extraterritorially). Congress has not.

Although the SCA requires modernization and reform, it is for Congress in its legislative capacity, not the courts, confined as they are to the narrow case or controversy before them, to give audience to public debate, weigh the competing policy interests, and enact a law that takes them into account.

III. Conclusion

For the foregoing reasons, the Court should decline the recommendation of the magistrate judge, interpret the SCA as its text and established canons of interpretation require, and void or modify the warrant to the extent that it requires Google to access, retrieve, and disclose to the government customer communications stored in data centers located outside the United States.

DATED: March 10, 2017

By: /s/ *Todd M. Hinnen*

Todd M. Hinnen (*pro hac vice*)
John R. Tyler (*pro hac vice*)
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101
Phone: 206.359.8000

William DeStefano
Stevens and Lee
1818 Market Street, 29th Floor
Philadelphia, PA 19103
Phone: 215.751.1941

Attorneys for Google Inc.