PRIVACY LAW — STORED COMMUNICATIONS ACT — DISTRICT COURT HOLDS THAT SCA WARRANT OBLIGATES U.S. PROVIDER TO PRODUCE EMAILS STORED ON FOREIGN SERVERS. — *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

The 1986 Stored Communications Act[1] (SCA) allows the government to obtain a warrant (SCA Warrant) that requires an Internet Service Provider (ISP) to produce customer information, emails, and other materials upon a showing of probable cause.[2] While the Internet has transformed since 1986, the Act remains mostly unchanged. Recently, in *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*,[3] a magistrate judge in the Southern District of New York ruled — and a district judge affirmed[4] — that an SCA Warrant obligates an ISP like Microsoft[5] to produce information stored on overseas servers.[6] SCA Warrants, the magistrate judge explained, are part-subpoena, part-warrant hybrids and so are not bound by the same territorial constraints that restrict traditional warrants.[7] While the decision is well reasoned, the territorial question raised by this litigation underscores the potential risks of judicial application of the SCA and the corresponding need for Congress to reform the outdated statute by clarifying its application to data stored abroad.

---

[1] 18 U.S.C. §§ 2701–2712 (2012). The SCA was passed as part of the Electronic Communications Privacy Act of 1986 (ECPA). *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). As the Fourth Amendment does not protect information that individuals have voluntarily turned over to a third party, *see* Smith v. Maryland, 442 U.S. 735, 745–46 (1979), the SCA was passed to provide privacy protections that would otherwise be absent.

[2] *See* 18 U.S.C. § 2703. The SCA authorizes three means of obtaining electronic communications, such as emails, from an ISP: subpoena, court order, and warrant (listed in ascending order of breadth). *See id.* Each tier grants the government greater investigatory privileges in exchange for higher procedural and evidentiary barriers. For example, a subpoena requires that the customer receive prior notice, a court order demands a reasonable basis to believe the desired content is relevant to a criminal investigation, and an SCA Warrant requires probable cause, but unlike the other two allows for the production of all of a user's emails rather than a subset. *See id.* § 2703(a)–(d).

[3] 15 F. Supp. 3d 446 (S.D.N.Y. 2014).

[4] Order at 1, *In re Warrant*, 15 F. Supp. 3d 446 (No. 13-MJ-2814), ECF No. 80.

[5] Because the magistrate judge's opinion uses "ISP" to refer to Microsoft, this comment does as well. However, "service provider" and "electronic communication service" are more accurate terms because Microsoft does not provide subscribers with an Internet connection, but only a means of email communication.

[6] *In re Warrant*, 15 F. Supp. 3d at 477.

[7] *See id.* at 471–72.

In December 2013, as part of a presently undisclosed criminal investigation, federal prosecutors in the Southern District of New York sought and obtained an SCA Warrant authorizing "the search and seizure of information" — including emails — "associated with a specified web-based e-mail account" stored by Microsoft.[8] The warrant, granted by Magistrate Judge Francis, requested the production of responsive material within two weeks and delayed notification to the subscriber for thirty days.[9]

Upon receipt of the SCA Warrant, Microsoft's Global Criminal Compliance team determined that while some of the responsive account information was stored on U.S. servers,[10] the corresponding emails were stored on servers located in Dublin, Ireland.[11] Microsoft handed over the data stored in the United States, but moved to "quash the warrant to the extent that it direct[ed] the production of information stored abroad."[12] Microsoft's argument hinged on the fact that the government here, as required by the SCA, sought the account information pursuant to "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure."[13] Because according to Rule 41 "[f]ederal courts are without authority to issue warrants for the search and seizure of property outside the territorial limits of the United States,"[14] Microsoft contended that SCA Warrants do not reach data abroad.[15]

Microsoft's motion to quash came before Magistrate Judge Francis, who first turned to the text of the SCA to determine whether it permitted the government to demand data stored abroad. He determined

---

[8] *Id.* at 468. In addition to emails associated with the account, the warrant requested information concerning the identity of the owner of the account in question, her address book, and any communications between Microsoft and the owner. *See id.*

[9] Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant at Exhibit A, *In re Warrant*, 15 F. Supp. 3d 446 (No. 13-MJ-2814), ECF No. 9 [hereinafter Government's Memorandum of Law].

[10] Even when Microsoft stores most of a user's information overseas, it retains in the United States some "testing and quality control" data, address-book information, and other "non-content information . . . such as the user's name and country." *In re Warrant*, 15 F. Supp. 3d at 467.

[11] *See id.* at 467–68. In order to offer its customers high-quality email service, Microsoft stores most of a user's data in servers as close as possible to where the customer resides. *See id.* at 467. A customer's location is determined based on the "country code" entered upon registration. *Id.* Notably, Microsoft never independently confirms the location of information supplied by a customer. *See* Government's Memorandum of Law, *supra* note 9, at 20.

[12] *In re Warrant*, 15 F. Supp. 3d at 468.

[13] *Id.* at 470 (quoting 18 U.S.C. § 2703(a) (2012)); *see also id.* (outlining Microsoft's argument).

[14] *Id.* Rule 41 vests no authority in magistrate judges to issue warrants for foreign searches. *See, e.g.*, *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 171 (2d Cir. 2008) (expressing skepticism that judges can issue warrants for overseas searches). Foreign searches are instead subject to a reasonableness test that, in the Second Circuit, balances the intrusion on the individual's privacy against the government interest in the search. *See id.* at 172.

[15] *In re Warrant*, 15 F. Supp. 3d at 470.

that while Microsoft's interpretation of the SCA was reasonable, the requirement that SCA Warrants be issued "using the procedures described in the Federal Rules of Criminal Procedure"[16] could, "equally plausibly," be read to require only that SCA Warrants comply with the "procedural aspects of the [warrant] application process."[17] Deciding that the text of the SCA was ambiguous, Magistrate Judge Francis proceeded to consider the statute's structure and legislative history, as well as the practical consequences of Microsoft's argument.

In examining the structure of the SCA, the magistrate determined that an SCA Warrant "is a hybrid: part search warrant and part subpoena."[18] Like a conventional search warrant, an SCA Warrant is obtained upon application to a neutral magistrate and upon a showing of probable cause.[19] However, once an SCA Warrant is issued, it acts like a subpoena in that it is served upon an ISP with the expectation of a response and does not require the government to conduct a physical search and seizure.[20] Under subpoena doctrine, the location of the requested documents is irrelevant; what matters is that the subpoenaed party have control over the requested material.[21] Requiring an ISP to produce its records held abroad "does not implicate principles of extraterritoriality,"[22] but is considered an extension of the court's power toward a party over whom it has personal jurisdiction.[23]

Next, Magistrate Judge Francis considered the legislative history of the SCA.[24] While the Senate Report did not address the SCA's territorial reach, the House Report did, stating that instruments to "access . . . stored . . . communications are intended to apply only to access within the territorial United States."[25] This reference "suggest[ed] that information stored abroad would be beyond the purview of the SCA."[26] However, he noted that these comments more likely indicated that electronic communications intercepted abroad by foreign law enforcement apart from U.S. search and seizure procedures could still be

---

[16] *Id.* (quoting 18 U.S.C. § 2703(a)).

[17] *Id.*

[18] *Id.* at 471.

[19] *Id.* at 471–72. This procedure reflects the privacy concerns that helped motivate Congress to pass the SCA. *See id.*; *accord* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 381–82 (2014).

[20] *See In re Warrant*, 15 F. Supp. 3d at 471.

[21] *Id.* at 472 ("It has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information." (citing *In re* Marc Rich & Co. v. United States, 707 F.2d 663, 667 (2d Cir. 1983))).

[22] *Id.*

[23] *See, e.g.*, *Marc Rich*, 707 F.2d at 668–69.

[24] *See In re Warrant*, 15 F. Supp. 3d at 472–74.

[25] *Id.* at 473 (quoting H.R. REP. NO. 99-647, at 32–33 (1986)).

[26] *Id.*

admissible at trial.[27] Furthermore, the report failed to clarify whether "access" to data "meant access to the location where the electronic data was stored or access to the location of the ISP."[28] Fortunately, a House Report accompanying a 2001 amendment to the SCA provided some clarity. In describing the operation of Rule 41, that report equated "'where the property is located' with the location of the ISP, not the location of any server."[29]

Lastly, Magistrate Judge Francis turned to the practical implications of Microsoft's interpretation, concluding that Congress could not have intended SCA Warrants to be limited to data stored in the United States.[30] First, some ISPs attempt to house a customer's data near her residence, but are not required to verify the residency information provided by customers. Therefore, if SCA Warrants were so limited, criminals could provide false information, have their data stored overseas, and thereby avoid the reach of U.S. law enforcement.[31] Second, if SCA Warrants did not allow for the production of data stored abroad, the government would have to obtain such information through Mutual Legal Assistance Treaty (MLAT) procedures, which are lengthy, cumbersome, and unreliable.[32] Since the United States is a party to such treaties with only approximately sixty countries, some data "within the control of an American service provider" would be entirely out of law enforcement authorities' reach.[33]

---

[27] *Id.* (noting that the House Report cites *Stowe v. Devoy*, 588 F.2d 336 (2d Cir. 1978), in which the Second Circuit upheld the admittance of telephone calls intercepted in Canada by Canadian authorities outside of the strictures of the Wiretap Act). The reference in the House Report to the "territorial United States" thus enhanced the power of law enforcement rather than limited it.

[28] *Id.* If the pertinent location under the SCA is the ISP, Microsoft would be bound to comply; however, if Congress intended the location of the requested information to be most important, the data's foreign storage would present issues.

[29] *Id.* at 474. Before this amendment, enacted as part of the USA PATRIOT Act, only a judge in the district where the ISP was located could issue a warrant compelling the ISP to disclose certain data. *See id.* The amendment allowed "the court with jurisdiction over the investigation to issue the warrant directly" without requiring the cooperation of a judge at the ISP's location. *Id.* (quoting H.R. REP. NO. 107-236(I), at 57 (2001)). Magistrate Judge Francis determined that this amendment clarified that "the property" mentioned in the House Report was the ISP. *Id.*; *accord* Orin Kerr, *What Legal Protections Apply to E-mail Stored Outside the U.S.?*, WASH. POST: VOLOKH CONSPIRACY (July 7, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/ [http://perma.cc/VG23-T8AC] ("The point of [the 2001 amendment] was to indicate that [SCA Warrants] did not incorporate every aspect of traditional Rule 41 search warrants . . . .").

[30] *In re Warrant*, 15 F. Supp. 3d at 474–75.

[31] *Id.* at 474.

[32] *Id.* at 474–75.

[33] *Id.* at 475. Magistrate Judge Francis devoted the last section of the order to clarifying that the presumption against extraterritoriality did not apply because it "does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. At least in this instance, it places obligations only on the service provider to act within the United States." *Id.* at 475–76.

Based on the foregoing, Magistrate Judge Francis determined that SCA Warrants function as subpoenas and require the production of all responsive information, regardless of where it is stored.[34] He thus denied Microsoft's motion to quash the warrant.[35] Microsoft appealed Magistrate Judge Francis's order to the district court. Judge Preska heard argument in July 2014 and orally affirmed Magistrate Judge Francis's order.[36]

While Magistrate Judge Francis's order accords with the SCA, the court's decision was not the only potential outcome.[37] The statute was not written for today's Internet and the huge amounts of data stored across the globe. It is startling that issues concerning the production of data stored overseas are only being raised for the first time in this litigation[38] and their importance will only continue to grow.[39] *In re Warrant* is illustrative of the problems that arise from the SCA's age and ambiguity. As it currently stands, judicial application of the vague statute carries a high risk of problematic outcomes. The SCA can, and should, be revised[40] in a way that clarifies the territorial questions raised by this case and weighs the government's legitimate law enforcement needs against valid privacy interests and practical concerns.[41]

---

[34] *See id.* at 477.

[35] *Id.*

[36] *See* Order, *supra* note 4, at 1.

[37] For example, in the case of *Zheng v. Yahoo! Inc.*, No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 2, 2009), a district court judge determined that the ECPA did not "apply outside the United States," *id.* at *4. While the circumstances of *Zheng* were significantly different from this case in that *Zheng* concerned the disclosure of data by a U.S. company to a foreign government and did not involve law enforcement or an SCA Warrant, it demonstrates that judges can interpret the statute's legislative intent differently.

[38] *See* Kerr, *supra* note 29 (describing the question in this case as "novel").

[39] This case has already attracted significant attention from other companies, with Apple, Cisco, Verizon, and AT&T submitting amicus briefs in support of Microsoft's position. *See, e.g.*, Memorandum of Law of Amicus Curiae AT&T Corp. in Support of Microsoft Corp., *In re Warrant*, 15 F. Supp. 3d 446 (No. 13-MJ-2814), ECF No. 35-1 [hereinafter AT&T Amicus Memorandum].

[40] *See, e.g.*, Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1458 (2004); *cf.* Orin S. Kerr, Essay, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 308 (2005) (discussing the greater flexibility of the legislative and executive branches compared to the courts). In fact, in September 2014, a bipartisan group of Senators introduced an SCA reform bill inspired by this litigation, the Law Enforcement Access to Data Stored Abroad Act. John Ribeiro, *Senate Bill Would Limit Access to Emails Stored Abroad*, COMPUTERWORLD (Sept. 18, 2014, 11:54 PM), http://www.computerworld.com/article/2686099/senate-bill-would-limit-access-to-emails-stored-abroad.html [http://perma.cc/VYF9-ZWMN]. Under the proposed legislation, SCA Warrants would require the production of the data of Americans stored abroad by U.S. companies, but foreigners' data would be off limits. *Id.*

[41] While numerous articles have proposed various means of reforming the SCA, they have not considered the issue presented by this case's fact pattern: what privacy protections are required when U.S. law enforcement seeks information stored abroad by a U.S. provider? For a discussion of how the SCA can be reformed to better protect the privacy interests of American subscribers, see *Our Principles*, DIGITAL DUE PROCESS, http://www.digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Nov. 23, 2014) [http://perma.cc/QHV4

When Congress passed the Electronic Communications Privacy Act of 1986[42] (ECPA), which included the SCA, the Internet was in its infancy. It was unclear whether existing Fourth Amendment doctrine would apply to stored electronic communications,[43] and there was a concern that emails would not be subject to any privacy protections whatsoever. As a result, the ECPA was intended to balance privacy concerns with law enforcement needs.[44] It also included provisions granting law enforcement investigatory tools to legally gather stored communications.[45] While the SCA was amended in 1994 and 2001, "the basic structure of the 1986 statute remains in place today."[46]

There is no doubt the Internet has changed dramatically in the nearly thirty years since the SCA was enacted. Two of the most transformative technological shifts were integral to this litigation. First, because at the time of the SCA's passage, storage of data was prohibitively expensive and rare, Congress did not envision stored communications as a central privacy concern.[47] Since the 1980s, however, the cost of storing data has decreased exponentially and the amount of stored personal data has increased commensurately.[48] Second, the Internet has evolved from a predominantly American network into a global one, both in usage and infrastructure.[49] As a result of these unforeseen developments, the stakes of misapplying the ambiguous SCA have ballooned. Stored electronic communications have assumed a pivotal importance that the statute can no longer adequately manage.

If Magistrate Judge Francis had come to a different, but permissible, interpretation of the SCA Warrant and the vague text authorizing it, the outcome could have been highly problematic. Relying on na-

---

-5D7X]; *see also* Bellia, *supra* note 40, at 1434–58; Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1233–44 (2004); Kerr, *supra* note 19, at 411–18.

42 Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

43 *See* Kerr, *supra* note 19, at 381–82.

44 *See id.* at 382; Kerr, *supra* note 41, at 1209–13.

45 The dual privacy and law enforcement concerns of the statute have led Professor Orin Kerr to describe the SCA "as both a shield and a sword." Kerr, *supra* note 29.

46 Kerr, *supra* note 19, at 385. For an extensive discussion of how the SCA's framework and the categories set forth in the statute have become outdated, see *id.* at 390–410. As Kerr writes, "[t]he old categories no longer work." *Id.* at 390.

47 *Id.* at 391–92.

48 *See id.* at 391–95 ("The ability to store everything makes storage the greater privacy threat. Real-time surveillance becomes only a slice of the world that access to stored contents can produce." *Id.* at 393.).

49 *See id.* at 404–08 ("In today's networked environment, company headquarters can be located in one country; employees with access to the data can be located in a second country; the data can reside in a third country; and the party seeking access to the company's data could be located in a fourth country." *Id.* at 407.); *see also* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1628–29 (2013).

tional borders in today's cloud-based Internet is untenable.[50] Microsoft, in particular, stores data around the world.[51] This is particularly problematic because there is no obligation that an ISP verify a customer's professed residence, which can dictate where her data is stored.[52] Tying an SCA Warrant to the location of the requested data rather than the location of a provider would severely hinder the efforts of law enforcement and draw a nonsensical distinction. Furthermore, Microsoft's position is incongruous when set against Fourth Amendment doctrine. Courts have already determined, in the context of conventional search warrants, that when a search occurs outside of the United States, non-U.S. persons have no Fourth Amendment rights[53] while U.S. persons are shielded only by a "reasonableness" requirement.[54] Because individuals already have fewer or no constitutional privacy protections abroad, it would be strange for Magistrate Judge Francis to have ruled that a search that would be legal if conducted on U.S. soil is prohibited if conducted abroad.

At the same time, however, an extraterritorial SCA Warrant does raise privacy and practical concerns, particularly for foreign subscribers. For example, Microsoft and other technology companies have received complaints from "both current and potential customers overseas about the U.S. Government's extraterritorial access to their user information" that might "substantially undermine[]" the companies' positions in cloud computing.[55]

The resolution of the SCA's territorial reach should fall to Congress as the body most capable of clarifying the statute to better regulate access to stored communications in light of such communications' current outsized importance. The government has a legitimate interest in uncovering and combating criminal activity that should not be hindered by the location of a company's servers or other factors unrelated

---

[50] *Cf.* Schwartz, *supra* note 49, at 1629 ("[C]loud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data centre at 2pm and on the other side of the world at 4pm." (quoting Article 29 Data Prot. Working Party, Opinion 05.2012 on Cloud Computing 17, (EC) No. 01037/12/EN, WP 196 (July 1, 2012), http://idpc.gov.mt/dbfile.aspx/WP196.pdf [http://perma.cc/53GJ-C52X])).

[51] By Microsoft's own account it stores the data of more than one billion customers and twenty million businesses in one hundred storage facilities across forty countries. Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States at 8, *In re Warrant*, 15 F. Supp. 3d 446 (No. 13-MJ-2814), ECF No. 15 [hereinafter Microsoft's Objections].

[52] *See supra* note 11.

[53] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 265–71 (1990).

[54] *E.g.*, *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 167 (2d Cir. 2008).

[55] Microsoft's Objections, *supra* note 51, at 30; *accord* AT&T Amicus Memorandum, *supra* note 39, at 19–20; Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES, Mar. 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

to an individual's privacy interests. To the extent that the SCA's language referencing the Federal Rules of Criminal Procedure is ambiguous, it should be revised to more closely align with the tool it authorizes: a subpoena requiring a showing of probable cause to a neutral magistrate. Additionally, because this issue is bound to reappear, the revision should include precise wording that clearly specifies the obligation of an American service provider when the data requested is stored overseas. With cloud-computing systems, data, including fragments and copies, can be stored everywhere; it is important that the SCA explicitly acknowledge that the location of the data is not the crucial consideration.[56] Rather, the location of the service provider should govern. Finally, because at least in the case of Microsoft, where a customer's data is stored is based on user-provided information that is never independently verified, Congress could mandate a vetting requirement that obligates a service provider to base the location of storage upon a subscriber's IP address, rather than her self-reported location.

Despite the importance of law enforcement prerogatives, Congress should also endeavor to safeguard privacy and U.S. business interests to the extent possible. First, any revised policy should include a heightened burden on the government when seeking a warrant for the information of non-U.S. persons. A reviewing court can look to see if the prosecutor met a substantial evidence burden rather than probable cause.[57] Second, Congress can specify the types of crimes where an SCA Warrant can be used to obtain data belonging to non-U.S. persons and those where MLATs must be used. Thus, SCA Warrants can be reserved only for the most serious and time-sensitive crimes. While this proposal may not be sufficient to satisfy all privacy concerns expressed by foreign customers of an American provider, it would be an important step. Such a limitation would strengthen the privacy considerations of the statute without severely impacting its law enforcement prerogatives.

An SCA Warrant allows the government to obtain private emails upon a showing of probable cause. Despite its moniker, an SCA Warrant is akin to a subpoena in that the location that matters is that of the service provider and not the requested data. Despite the ruling in this case, the transformations in communications technology and the ubiquity of data stored across the globe demand a clarification of the SCA only Congress can provide.

---

[56] *See* Kerr, *supra* note 19, at 407–08 (discussing the difficulties of reconciling a data-location-driven regime with the realities of the global Internet).

[57] The substantial evidence standard is borrowed from administrative law and would require more conclusively linking the individual in question to the crime alleged. *See, e.g.*, Smolen v. Chater, 80 F.3d 1273, 1279 (9th Cir. 1996) (describing the standard).