UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation	Case No. 13-MAG-2814

Memorandum of Law in Support of
Verizon Communications Inc.'s Motion to Participate as *Amicus Curiae* and
Microsoft Inc.'s Motion to Vacate Search Warrant

Michael Vatis (*pro hac vice* to be submitted)
Jeffrey A. Novack
STEPTOE & JOHNSON LLP
1114 Avenue of the Americas
New York, New York 10036
(212) 506-3900

Counsel for Verizon Communications Inc.

Verizon Communications Inc. ("Verizon") respectfully submits this memorandum of law in support of: (1) its motion to participate as *amicus curiae* in Case No. 13-MAG-2814; and (2) Microsoft Inc.'s Motion to Vacate Search Warrant in the above-referenced case.

I. The District Court Should Permit Verizon to Participate as Amicus Curiae

Verizon moves for leave to file an *amicus* brief in support of Microsoft's motion to vacate a search warrant seeking an individual's email content stored in Ireland. Verizon has a substantial interest in judicial interpretations of the Stored Communications Act that would affect whether and how the U.S. government can obtain customer data stored abroad. Verizon subsidiaries operate "cloud" storage services internationally, which allow business customers in other countries to store their data on servers located abroad. Verizon highly values the privacy of its customers and the confidentiality of their information, and makes great efforts to protect its customers' interests. While Verizon complies with lawful government demands for information, the extraordinary reach of the demand here raises serious questions about its legitimacy. In addition, because Verizon operates in multiple countries, it must be particularly sensitive to the risk of conflicts between the laws of the countries in which it operates. Verizon is filing this brief because the magistrate's ruling conflicts with these core principles.

The logic of the ruling below has an extraordinary and unprecedented sweep, and extends far beyond providers of email services. Many companies offer various types of cloud storage services. The burgeoning availability of cloud storage services is a driver of global efficiency and commerce. But if the Court were to permit the U.S. government to obtain, in a manner contrary to both U.S. and foreign law, customer data stored abroad, it would have an enormous

detrimental impact on the international business of American companies, on international relations, and on privacy.[1]

Relatedly, Verizon can offer a different perspective on this case, and can shed light on the broader implications for the cloud industry of the position taken by the government, because Verizon's cloud computing and storage business is different from Microsoft's email service at issue here. Unlike email providers that serve individual customers and may store data in or access it from the United States, many cloud businesses store their overseas enterprise customers' data directly in servers located abroad or have no or limited access to that data from the United States. Verizon therefore respectfully requests that the Court permit it to file this amicus brief.[2]

II. The Stored Communications Act Should Not be Given Extraterritorial Effect

This case should begin and end with the "longstanding principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 248 (2010) (citations and internal quotation marks omitted). The Supreme Court has reiterated many times that a statute is presumed *not* to have extraterritorial application "'unless there is the affirmative intention of the Congress clearly expressed' to give [the] statute extraterritorial

---

[1] Verizon publicly stated well before the ruling below that the U.S. government cannot compel a company in the United States to produce its customers' data stored in data centers abroad. http://publicpolicy.verizon.com/blog/entry/thoughts-on-foreign-data-storage-and-the-patriot-act.

[2] This Court has inherent authority to permit the participation of amici. *See, e.g., In re Bayshore Ford Truck Sales, Inc.*, 471 F.3d 1233, 1249 n.34 (11th Cir. 2006) ("district courts possess the inherent authority to appoint 'friends of the court' to assist in their proceedings"); *see also Neonatology Assocs. v. Comm'r*, 293 F.3d 128, 133–34 (3d Cir. 2002) (Alito, J.) (party should be permitted to participate as amicus when it has stated an "interest in the case" and makes "relevant" assertions); *id*. at 133 (it is "preferable to err on the side of granting leave.").

effect." *Id.* (citations omitted). "When a statute gives no indication of an extraterritorial application, it has none." *Id.*

Congress did not clearly express its affirmative intention that the Stored Communications Act (the "SCA" or the "Act") have extraterritorial effect. There is nothing in the plain language of the statute that clearly expresses such an intention. *See Zheng v. Yahoo! Inc*., No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 2, 2008) (finding that the Electronic Communications Privacy Act does not apply extraterritorially). Nor is there any such expression in the legislative history. To the contrary, the legislative history makes plain that Congress intended that the Act *not* apply extraterritorially:

> By the inclusion of the element "affecting (affects) interstate or foreign commerce" in these provisions the Committee does not intend that the Act regulate activities conducted outside the territorial United States. Thus, insofar as the Act regulates the "interception" of communications, for example it…regulates only those "interceptions" conducted within the territorial United States. Similarly, the controls in Section 201 of the Act [which became the SCA] regarding access to stored wire and electronic communications are intended to apply only to access within the territorial United States.

H.R. Rep. No. 99-647, at 32–33 (1986).

Contrary to the magistrate's view (*see* Op. at 16), there is nothing ambiguous about this passage. Even if it were ambiguous, and even if "ambiguity" in legislative history were of any weight, the presumption against extraterritoriality requires that the SCA be interpreted as applying only to information in the United States, absent some express statement by Congress to the contrary. There is no such statement in the SCA.[3]

[3] In lieu of any express statement by Congress that the Act applies extraterritorially, the magistrate took into account certain "practical considerations"—specifically, the magistrate's view of what the practical effect on law enforcement would be of not applying the SCA extraterritorially. *See* Op. at 18. These are precisely the sorts of considerations that the Supreme Court disallowed in *Morrison*. *See Morrison*, 561 U.S. at 261. Moreover, as discussed in

The ruling below also runs afoul of the Supreme Court's longstanding rule that U.S. laws should be interpreted "to avoid unreasonable interference with the sovereign authority of other nations." *F. Hoffman-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164 (2004); s*ee also Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804) ("[A]n act of Congress ought never to be construed to violate the law of nations if any other possible construction remains."). In *F. Hoffman-La Roche*, the Supreme Court reiterated that courts should "assume that legislators take account of the legitimate sovereign interests of other nations when they write American laws." 542 U.S. at 164. This assumption "helps the potentially conflicting laws of different nations work together in harmony—a harmony particularly needed in today's highly interdependent commercial world." *Id.* at 164–65.

But if a U.S. search warrant could be used to obtain the content of customer data or communications stored abroad, it would create a dramatic conflict with foreign data protection laws. Indeed, in response to the magistrate's decision, the European Commission spokeswoman for justice, fundamental rights, and citizenship stated: "The commission's position is that this data should not be directly accessed by or transferred to US law enforcement authorities outside formal channels of co-operation, such as the mutual legal assistance agreements or sectoral EU–US agreements authorising such transfers . . . . The European Parliament reinforced the principle that companies operating on the European market need to respect the European data protection rules - even if they are located in the US." *Microsoft 'must release' data held on Dublin server*, BBC.COM, Apr. 29, 2014, http://www.bbc.com/news/technology-27191500.

This is not just rhetoric. For example, when European regulators learned that the Society for Worldwide Interbank Financial Telecommunications ("SWIFT"), the Belgium-based

---

Section III, *infra*, the magistrate left out of the analysis a host of "practical considerations" that militate strongly *against* extraterritorially.

international bank consortium, had been complying with U.S. subpoenas and providing data to the U.S. government about the financial transactions of European residents, SWIFT was subjected to numerous investigations by European and other governments for violations of their data protection and privacy laws.[4] Ultimately, SWIFT was forced to restructure its network to prevent the passage of intra-European data through the U.S.[5] *See also In re Avocat "Christopher X"*, Cour de Cassation [Cass.] [supreme court for judicial matters] crim, Dec. 12, 2007, Bull. crim., No. 7168 (Fr.), http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000017837490&fastReqId=2062651721&fastPos=1 (finding American-trained lawyer liable for violating France's "blocking" statute by contacting witness in France and obtaining economic information in support of investigation by California Insurance Commissioner).

The obvious incompatibility between what the government seeks here and foreign privacy laws bolsters the presumption that the Act does not apply to customer data stored abroad. *See Morrison*, 561 U.S. at 269 ("The probability of incompatibility with the applicable laws of other countries is so obvious that if Congress intended such foreign application 'it would have addressed the subject of conflicts with foreign laws and procedures.'").

---

[4] John Rega & Jones Hayden, *Swift's bank-data transfers to U.S. violated privacy rules, EU says; Swift ordered to stop infringement Action highlights security rift*, TORONTO STAR, Nov. 24, 2006, 2006 WLNR 20358390; Dan Bilefsky, *Belgian leader orders bank inquiry Ministry to investigate release of details on money transfers*, INTERNATIONAL HERALD TRIBUNE, June 27, 2006, 2006 WLNR 11105900.

[5] *SWIFT to stop processing EU banking data in the US*, THE REGISTER, Oct. 15, 2007, http://www.theregister.co.uk/2007/10/15/swift_processing_halt/.

III. The Magistrate's Ruling Would Harm American Businesses, Undermine International Agreements and Understandings, and Spur Retaliation by Foreign Governments.

While the magistrate expressed concern that *not* permitting the government to use a search warrant to obtain the content of customer communication data stored abroad would make criminal investigations involving foreign-based evidence more difficult, he paid no heed to the enormous harm that *allowing* the U.S. government unilaterally to obtain customer data stored abroad would have. The magistrate's ruling, if left standing, could cost U.S. businesses billions of dollars in lost revenue, undermine international agreements and understandings, and prompt foreign governments to retaliate by forcing foreign affiliates of American companies to turn over the content of customer data stored in the United States.

The recent revelations about U.S. intelligence practices have heightened foreign sensitivities about the U.S. government's access to data abroad, generated distrust of U.S. companies by foreign officials and customers, and led to calls to cease doing business with U.S. communications and cloud service providers.[6] Studies have estimated that this distrust will result in tens of billions of dollars in lost business over the next few years.[7] The magistrate's ruling, if left standing, will dramatically increase the harm to American businesses. It would mean that foreign customers' communications and other stored data would be available to hundreds or thousands of federal, state, and local law enforcement agencies, regardless of the laws of the countries where the data is held. Foreign customers will respond by moving their business to foreign companies without a presence in the United States.

---

[6] 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.

[7] *Id.*

Permitting the U.S. government unilaterally to obtain the content of customer data stored abroad would also upset the structure of formal and informal cooperation set up by law enforcement agencies worldwide. For example, Mutual Legal Assistance Treaties ("MLATS") between the U.S. and foreign governments typically have specific provisions requiring the "requested" party to obtain evidence on behalf of the "requesting" party, including by using search warrants or other court orders. These provisions presuppose that the requesting party will not bypass the MLAT and unilaterally obtain evidence in the territory of the requested state, but will do so only in compliance with the law of the requested state. For instance, Ireland, where the data sought by the government here is stored, specifically added language to the U.S.-Ireland MLAT providing that searches be carried out in accordance with the law of the requested party. *See* S. Exec. Rep. 107-15, Oct. 17, 2002, *available at* http://www.gpo.gov/fdsys/pkg/CRPT-107erpt15/pdf/CRPT-107erpt15.pdf; Treaty Between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, U.S.–Ir., Jan. 18, 2001, T.I.A.S. 13137 at Art. 14, *available at* https://www.unodc.org/tldb/showDocument.do?document Uid=5944&cmd=add&node=docs&country=&pageNum=90. And Irish law requires authorization from an Irish District Court Judge to obtain the content of emails from an electronic communications provider. Criminal Justice Act 2011 (Act No. 22/2011) (Ir.) § 15, *available at* http://www.irishstatutebook.ie/pdf/2011/en.act.2011.0022.pdf.

These MLATs are expressions of longstanding, basic principles of state sovereignty. As the Restatement (Third) of Foreign Relations Law puts it: "It is universally recognized, as a corollary of state sovereignty, that officials in one state may not exercise their functions in the territory of another state without the latter's consent." Restatement (Third) of the Foreign

Relations Law of the United States § 432, cmt. b (1987). This principle specifically applies to law enforcement investigations: one state's "law enforcement officers . . . can engage in criminal investigation in [another] state only with that state's consent." *Id.*

The fact that a search is conducted via a computer connection does not eliminate the infringement on state sovereignty. "A search of one's hard drive by a foreign law enforcement agency from abroad…has the same effect as a traditional search of premises, a law enforcement measure reserved to the territorial sovereign . . . . As territorial sovereignty serves, inter alia, to protect the residents from physical persecution of other states, this protection must be extended when persecution no longer needs to physically enter foreign territory." Stephen Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED COMM. L.J. 117, 174 (1997).

Such international understandings are not mere niceties to reassure foreigners. They protect Americans, too, in ways that the magistrate's decision would undermine. If U.S. law enforcement may now obtain the content of foreign customers' data stored abroad by serving a search warrant on a provider in the United States, foreign governments will be certain to assert the same authority.[8] The Russian government, for example, might demand that a local affiliate of a U.S. cloud services provider disclose the data of a U.S. company negotiating a large corporate transaction with a Russian state-owned enterprise, or that of an American human rights group that has challenged an action of the Russian government in a fashion deemed to violate

[8] This concern is not hypothetical. David E. Sanger & Nicole Perlroth, *Internet Giants Erect Barriers to Spy Agencies*, N.Y. TIMES, June 6, 2014, http://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html?_r=0 ("One of the biggest indirect consequences from the Snowden revelations, technology executives say, has been the surge in demands from foreign governments that saw what kind of access to user information the N.S.A. received — voluntarily or surreptitiously. Now they want the same.").

Russian law. Following the magistrate's reasoning, Russian officials could order the provider's Russian affiliate to obtain the target's data from the U.S. and turn them over to the Russian authorities in Moscow. This is not a result that the U.S. government—or American companies or citizens—would find tolerable. Yet it is precisely what the magistrate's decision invites.[9]

Moreover, these effects would not be limited to American companies or citizens. If the government's position in this case were adopted, the U.S. government also could require foreign-based companies with a presence in the U.S. to turn over customer data stored abroad. Similarly, applying the same principles, foreign governments could force any companies doing business in their territory to disclose customer data stored outside that territory, regardless of where the companies are based. The government's position would result in an international free-for-all, with conflicts of law becoming the norm rather than the exception.

It is possible that Congress *could* decide that making it easier for U.S. law enforcement to obtain customer data stored abroad is worth these significant costs. But Congress has not made that decision. Instead, at the Administration's request,[10] it has taken steps to reinforce and streamline existing mechanisms for law enforcement-to-law enforcement cooperation. And the

---

[9] The government has previously recognized these concerns, even if the prosecutors in this case have not. *See, e.g.*, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, A Report of the Presidents Working Group on Unlawful Conduct on the Internet (February 2000), *available at* http://www.politechbot.com/docs/unlawfulconduct.html ("If law enforcement agents in the United States . . . remotely access a Canadian computer (from the United States), might this constitute a criminal act under Canadian law notwithstanding the existence of the U.S. warrant? . . . [C]onsider how we would react to a foreign country's 'search' of our defense-related computer systems based upon a warrant from that country's courts.").

[10] Congress took steps in 2009 to streamline the MLAT process by making it easier for the Justice Department to obtain evidence on behalf of foreign counterparts. It did so in part to encourage foreign law enforcement to similarly streamline their processes for assisting U.S. agencies. *See DoJ Letter to Senator Whitehouse*, 155 Cong. Rec. S6810 (daily ed. June 18, 2009).

Administration is considering new legislative proposals to further expedite the MLAT process.[11] It is not the province of a magistrate to upset the international balance set by Congress. Unless and until Congress makes an express decision to extend the SCA extraterritorially, law enforcement-to-law enforcement cooperation should remain the means for the U.S. government to obtain such data.

IV. A Search and a Seizure Take Place Where the Data Is Looked for and Retrieved, Not Where The Data Is Viewed By Law Enforcement.

The magistrate circumvented the presumption against extraterritoriality in part by finding that the search of the emails stored in Ireland would not take place until the emails were viewed by law enforcement in the United States. *See* Op at 13. But he cited no judicial authority for this novel proposition. In fact, the authority is to the contrary. *See, e.g.*, *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013)(rejecting government's argument that no search would occur outside the district because the electronic information would first be examined within the district, reasoning that "[i]f such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found.").

Moreover, even if the emails would be "searched" only when they are read by law enforcement, the *computer* on which the emails are stored would be searched when someone tried to find them. In this case, that computer is in Ireland. *See* Op. at 5. Additionally, those

---

[11] United States Department of Justice, *Attorney General Holder Announced President Obama's Budget Proposes $173 Million for Criminal Justice Reform*, Mar. 4, 2014, http://www.justice.gov/opa/pr/2014/March/14-ag-224.html; The White House, *Fact Sheet: Review of U.S. Signals Intelligence*, Jan. 17, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/fact-sheet-review-us-signals-intelligence.

emails or the computer they are stored on, or both, would be *seized* when the original emails were copied. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 561 (2005). A search and a seizure thus would necessarily take place in Ireland. *Cf. United States v. Auernheimer*, No. 13-1816, 2014 WL 1395670, at *11 (3d Cir. Apr. 11, 2014) ("computers still exist in identifiable places in the physical world," and normal rules regarding jurisdiction still apply).

Although courts and lawyers often use the shorthand term "search warrants," the warrants are, of course, actually "search and seizure warrants," since the government generally needs a warrant to effect a seizure as well as a search. The warrant in this case, not surprisingly, is titled, "Search and Seizure Warrant," and it lists the "Particular Things to be Seized." ECF No. 96 at Ex. 1. There is thus no escaping the fact that a search *and* a seizure would take place in Ireland, regardless of where the emails themselves are "searched."[12]

V. Conclusion

The search warrant at issue in this case is no run-of-the-mill investigative measure. If enforced, it would violate international understandings, harm American business, subject Americans to potential liability abroad, and invite foreign governments to unilaterally obtain electronic communications and data of Americans in the United States. There is no reason to believe that Congress intended these results when it enacted the SCA. Certainly nothing in the SCA clearly expresses such an intention. The warrant should therefore be vacated.

[12] Nor does it matter that Microsoft employees would be performing the search of the computer in Ireland and the seizure of the emails there. They would be performing these actions on behalf of the government, thus acting as the government's agents. Of course, the SCA permits the government to demand that a communications provider search and seize a computer and the data stored on it (if the computer and the data are stored in the U.S.). But the SCA does not change the fact that a search and a seizure occur where the computer and the data are located.

Respectfully submitted,

/s/ Jeffrey A. Novack

Michael Vatis (*pro hac vice* to be submitted)
Jeffrey A. Novack
Steptoe & Johnson LLP
1114 Avenue of the Americas
New York, NY 10036
(212) 506-3900

Counsel for Verizon Communications Inc.

Dated: June 10, 2014