EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION	13 Mag. 2814

MEMORANDUM OF LAW OF *AMICUS CURIAE* AT&T CORP. IN SUPPORT OF MICROSOFT CORPORATION

Charles W. Douglas*
SIDLEY AUSTIN LLP
One South Dearborn
Chicago, Illinois 60603
(312) 853-7000
cdouglas@sidley.com
* *Of Counsel*
Attorneys for AT&T Corp.

Alan Charles Raul
Kwaku A. Akowuah
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
(202) 736-8000
araul@sidley.com
Attorneys for AT&T Corp.

TABLE OF CONTENTS

INTEREST OF THE AMICUS 1

INTRODUCTION 4

ARGUMENT 7

I. The SCA Does Not Authorize U.S. Courts To Issue Warrants Requiring Providers To Disclose Information Stored In A Foreign Country Absent A Substantial Nexus To The United States. 7

A. The Presumption Against Extraterritoriality Controls This Question. 7

B. Congress's Choice Of The Word "Warrant" Underscores That Congress Did Not Intend These Provisions To Have Global Scope. 12

II. Any Extraterritorial Application Of The SCA's Warrant Provisions Must Be Consistent With Principles Of International Comity. 15

CONCLUSION 20

TABLE OF AUTHORITIES

Page(s)

CASES

Am. Libraries Ass'n v. Pataki,
969 F. Supp. 160, 168–69 (S.D.N.Y. 1997) 2

E.E.O.C. v. Arabian Am. Oil Co.,
499 U.S. 244 (1991) 9, 10

F. Hoffmann-La Roche Ltd. v. Empagran S.A.,
542 U.S. 155 (2004) 7

Foley Bros., Inc. v. Filardo,
336 U.S. 281 (1949) 10

In re Grand Jury Subpoena Dated August 9, 2000,
218 F. Supp. 2d 544 (S.D.N.Y. 2002) 17, 18

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.,
No. 13 Mag. 2814, 2014 U.S. Dist. LEXIS 59296 (S.D.N.Y. Apr. 25, 2014) ..... *passim*

Kiobel v. Royal Dutch Petroleum Co.,
133 S. Ct. 1659 (2013) 8, 10

Microsoft Corp. v. AT&T Corp.,
550 U.S. 437 (2007) 8, 15

Morissette v. United States,
342 U.S. 246 (1952) 13

Morrison v. Nat'l Australia Bank Ltd.,
561 U.S. 247 (2010) ..... *passim*

Murray v. Schooner Charming Betsy,
6 U.S. (2 Cranch) 64 (1804) 12

Sale v. Haitian Ctrs. Council, Inc.,
509 U.S. 155 (1993) 9

Sekhar v. United States,
133 S. Ct. 2720 (2013) 7, 12

Smith v. United States,
507 U.S. 197 (1993) 9

Société Nationale Industrielle Aérospatiale v. United States Dist. Court for the S. Dist. of Iowa,
482 U.S. 522 (1987) 17, 18

United States v. Bach,
310 F.3d 1063 (8th Cir. 2002) 14

United States v. Bin Laden,
126 F. Supp. 2d 264 (S.D.N.Y. 2000) 13

United States v. Colasuonno,
697 F.3d 164 (2d Cir. 2012) 13

United States v. First Nat'l City Bank,
396 F.2d 897 (2d Cir. 1968) ..... *passim*

United States v. Gorshkov,
No. CR00-550C, 2001 WL 1024026 (W.D. Wash., May 23, 2001) 10–11

United States v. Odeh,
552 F.3d 157 (2d Cir. 2008) 13

United States v. Vilar,
729 F.3d 62 (2d Cir. 2013) 11

STATUTES

18 U.S.C. §2702.....11

18 U.S.C. §2703.....4, 11

18 U.S.C. §2703(a) 4, 8

18 U.S.C. §2703(b) 8

18 U.S.C. §2703(b)(1) 4

18 U.S.C. §2703(b)(1)(B) 15

18 U.S.C. §2703(b)(2) 8

18 U.S.C. §2704.....11

18 U.S.C. §2705.....11

OTHER AUTHORITIES

AT&T Transparency Report, *available at* http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html 1

Apple Report on Government Information Requests, *available at* http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf.....1

Declaration of Independence (U.S. 1776).....16

Facebook Information for Law Enforcement Authorities, *available at* https://www.facebook.com/safety/groups/law/guidelines/ 1

F. Frankfurter, *Some Reflections on the Reading of Statutes*, 47 Colum. L. Rev. 527 (1947) 12

Foreign Intelligence Surveillance Act (FISA) Reforms: Hearing Before the Sen. Select Comm. on Intelligence Before S. Select Comm. on Intelligence, 112th Cong. (Comm. Print 2014) (statement of Dean C. Garfield, President & CEO, Information Technology Industry Council), *available at* http://www.intelligence.senate.gov/140605/garfield.pdf.....19–20

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., No. 13 Mag. 2814, Dkt. No. 9, Govt's Mem. In Opposition to Microsoft's Motion to Vacate Email Account Warrant (S.D.N.Y. Apr. 25, 2014) 9, 11, 14

Kashmir Hill, *How The NSA Revelations Are Hurting Businesses*, Forbes (Sept. 10, 2013), *available at* http://www.forbes.com/sites/kashmirhill/2013/09/10/how-the-nsa-revelations-are-hurting-businesses/.....19

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 (2004) 13

Resolution & Report of the American Bar Association, No. 103 (Feb. 6, 2012).....16

Restatement (Third) Foreign Relations Law of the United States §402(1)(b) (1987) 6

Restatement (Third) Foreign Relations Law of the United States §403(2) (1987).....12

Restatement (Third) Foreign Relations Law of the United States §442(1)(c) (1987) 17

Restatement (Third) Foreign Relations Law of the United States §473(1) (1987).....6

S. Exec. Rep. No. 110-13, *Mutual Legal Assistance Treaties with the European Union* (Sept. 11, 2008), *available at* http://www.foreign.senate.gov/imo/media/doc/executive_report_110-13.pdf 18

Schwartz & Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. __ (2014), *forthcoming, available at* http://ssrn.com/abstract=2271442 16

Verizon Transparency Report, *available at* http://transparency.verizon.com/international-data 1

Vodafone Law Enforcement Disclosure Report, *available at* http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html 4, 19

INTEREST OF THE AMICUS

Amicus curiae AT&T Corp., together with its affiliates (collectively, "AT&T"), is one of the world's largest providers of telecommunications and information services, and as a result frequently engages with law enforcement officials about ongoing investigations. As set forth in a recent "transparency report," AT&T receives numerous demands for information in relation to civil and criminal matters from federal, state and local law enforcement agencies in the United States.[1] As it must, AT&T complies with the Stored Communications Act (SCA) in responding to those demands. In addition, AT&T received a number of requests last year from foreign law enforcement agencies for information that is stored in the United States.[2] AT&T refers such international requests to the applicable Mutual Legal Assistance Treaty (MLAT) process for the requesting country.[3] Pursuant to that MLAT process, AT&T works with the Federal Bureau of Investigation to ensure that any resulting data transfer occurs pursuant to a warrant or other form of process specified by the SCA, and is otherwise consistent with U.S. law. This practice rests on an understanding that when it comes to data storage and privacy protections, location matters. AT&T and AT&T's domestic operating affiliates have relationships with millions of individual U.S. persons and businesses that are rooted in the United States, where their data also sits. U.S. law should govern access to that data. Like other multinational information service providers, AT&T also has business relationships with non-U.S. persons, and in many such cases, access to

---

[1] *See* AT&T Transparency Report, *available at* http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html.

[2] *See id.*

[3] AT&T's understanding is that other U.S. companies, including Verizon, Apple, and Facebook, have adopted similar practices. *See* Verizon Transparency Report, available at http://transparency.verizon.com/international-data; Facebook Information for Law Enforcement Authorities, *available at* https://www.facebook.com/safety/groups/law/guidelines/; Apple Report on Government Information Requests, *available at* http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf, at 3 n.2 (Nov. 5, 2013).

the relevant data should not necessarily be governed by U.S. law – even though the data may be technically accessible to AT&T in the United States.

The decision reached by Magistrate Judge Francis is troubling because it makes the provider's status as a U.S. entity the only factor relevant to whether U.S. authorities may use U.S. procedures to require disclosure of customer information. Under that approach, a court would not consider, for example, whether the relationship between the customer and provider is centered abroad, whether the customer has any tie to the United States apart from a relationship with an information service provider, or whether foreign law imposes different or additional data protections. AT&T believes that approach is inconsistent with bedrock principles of statutory construction, including the presumption against extraterritoriality. The nationality of the provider cannot be the only factor that determines whether an application of U.S. law is extraterritorial, because that approach disregards factors fundamental to any practical analysis of whether in a particular case, U.S. law is reaching for "data" that is fundamentally foreign. The Court should instead ask whether, considering all relevant factors, the relationship between the provider, the customer and the data at issue has a substantial nexus to the United States.

That analysis may in some circumstances be difficult to perform, precisely because modern information technology practices do not always map easily onto traditional notions of geography. *See Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 168–69 (S.D.N.Y. 1997). But it is no answer to say, as the magistrate judge did, that *all* information that as a technological matter could be accessed from the United States therefore should be treated as subject to U.S. law enforcement demands. That conclusion would transform the SCA's warrant provisions into a global information access tool without bounds. There is no indication that Congress intended the SCA to have that sort of sweeping extraterritorial application. Indeed, the contrary is true –

there is every indication that Congress intended the scope of search warrants to be limited to material that is already grounded in the United States at the time the warrant is issued. This Court accordingly should reject the interpretation adopted by Magistrate Judge Francis.

If the Court does not accept that position, however, it nonetheless should hold that considerations of international comity limit the circumstances in which a warrant should issue for information stored abroad. By any measure, governments have a strong interest in ensuring that their communications privacy and other data protection laws govern relationships between providers and customers that are fundamentally rooted within their borders. Many customers will share a similar expectation that familiar local laws ordinarily will control whether government investigators or others may access their accounts. These and other competing interests ordinarily are addressed through MLAT procedures, which effectively convert a foreign law request for information into a request that conforms to the domestic law requirements of a second country. As such, where the United States has ratified an MLAT applicable to the country where the requested information is stored, the government ordinarily should be required to use the procedures set out in those treaties to obtain the information that it seeks. In other circumstances, the government should be required to make some showing that it cannot satisfactorily obtain the needed information by coordinating with appropriate foreign authorities.

AT&T is concerned that a contrary result could be viewed as a sign that neither the Congress, nor the Executive Branch, nor the courts of the United States respect the data privacy and information law interests of other countries. Given basic notions of reciprocity, that result could work significant harm to U.S. consumers, who rely on an analogous understanding that U.S. privacy and consumer protection laws, rather than foreign laws, control access to data that is stored in this country and does not have a substantial nexus to any other. The Electronic

Communications Privacy Act, which includes the SCA, contains numerous substantive and procedural limitations, as well as transparency, due process and litigation rights, that are not necessarily replicated in foreign laws.[4] U.S. data privacy interests would thus be prejudiced if the magistrate judge's ruling were generalized internationally, and other countries demanded production of all data stored in the United States whenever such data was technically accessible by affiliates subject to foreign jurisdiction. In any event, U.S. businesses could face a significant competitive disadvantage if U.S. law enforcement access to foreign-located data were perceived as unrestrained and disrespectful of foreign interests.

INTRODUCTION

No one doubts that in the Internet Age, information stored by communications providers often is pivotal in law enforcement investigations. For that reason, although the SCA's general purpose is to protect the privacy of electronic data, the statute also requires providers to disclose information about a wire or electronic communication to appropriate government authorities when presented with a warrant, court order, or subpoena, as appropriate. *See* 18 U.S.C. §2703. As relevant here, the SCA authorizes government officials to compel disclosure of content information by obtaining "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." *Id.* §2703(a); *id.* §2703(b)(1). It is undisputed that the SCA does not in express terms mandate compulsory access to information that foreign customers

[4] *See* Vodafone Law Enforcement Disclosure Report, *available at* http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html. ("Laws designed to protect national security and prevent or investigate crime vary greatly between countries, even within the EU…. All countries have a wide range of domestic laws which govern how electronic communications networks must operate and which determine the extent to which law enforcement agencies and government authorities can intrude into or curtail privacy or freedom of expression.... However enacted, these powers are often complex, opaque and convoluted.").

maintain with providers for commercial or personal use outside the United States. In fact, as Magistrate Judge Francis observed, the legislative history of the SCA states that the Act was "intended to apply only to access within the territorial United States." *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 13 Mag. 2814, 2014 U.S. Dist. LEXIS 59296, at *20 (S.D.N.Y. Apr. 25, 2014) (hereinafter "MJ Op.") (quoting H.R. Rep. 99-647, at 32-33 (1986)).

The magistrate judge nonetheless held that a "warrant issued" by him, "using the procedures described in the Federal Rules of Criminal Procedure," compels Microsoft to disclose content information that is stored on servers located in Ireland, no matter where Microsoft's relationship with the customer at issue actually is centered, or where services for that customer are performed. *Id.* at *12. Moreover, he did so without requiring any showing from the government that it has attempted in this case to utilize appropriate MLAT procedures, and without otherwise ensuring that the order is consistent with international comity principles. That conclusion is incorrect for at least three reasons.

First, this decision is inconsistent with the presumption against extraterritoriality. That canon of construction seeks to minimize conflicts between U.S. and foreign law by requiring courts to apply statutes only to domestic matters unless Congress has provided a "clear indication" that the statute also should operate extraterritorially. *See, e.g.*, *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010). The magistrate judge appeared to agree with Microsoft that the SCA does not contain any such "clear indication," but held that this case does not involve an extraterritorial application solely because Microsoft is technically capable of retrieving the data from Ireland using computers here in the United States. MJ Op. at *27–28, 33. That holding is overly simplistic. A New York bank might well have the technical capacity

to transfer funds from a Dublin branch to Manhattan at a keystroke. But it would be implausible to say that act has no effect outside the United States, or that a U.S. law requiring a bank to move funds from Dublin to New York would have no extraterritorial application. This case may well be similar, although AT&T does not have access to sealed information that the parties have provided the Court. In general terms, however, mere technical access is an inappropriate standard because, given modern technology, vast amounts of data could be accessed from almost anywhere from a technical standpoint. And because multinational companies are subject to legal process in many locations, a technical access standard would make their customer data subject to search in places that do not have any connection at all to the customer or to the customer relationship. Put more concretely, the technical access standard endorsed by the magistrate judge has a clear potential to alter the status of information that not only is in Ireland, but has been created as part of a relationship between Microsoft and its customer that does not have a substantial nexus to the United States. Currently, it is held in confidence by Microsoft in Ireland. If the order takes effect, that same information will be transferred to the United States for review by U.S. authorities. Absent facts suggesting that the customer relationship giving rise to that storage has a substantial nexus to the United States (such as that the customer resides in the United States, the customer accesses the data in the United States, or the customer obtains substantial processing or other relevant services in the United States), a U.S. law that requires that transfer to the United States plainly would operate extraterritorially and tread on matters of concern to Irish law. *See* Restatement (Third) of Foreign Relations Law of the United States ("Restatement") §402(1)(b) (1987) (generally, "a state has jurisdiction to prescribe law with respect to … interests in things, present within its territory"); *id* §473(1) ("a state may determine the conditions for taking evidence in its territory in aid of litigation in another state").

Second, the magistrate judge failed to recognize that far from plainly authorizing extraterritorial applications, the statute affirmatively indicates that the statute's warrant provisions are territorially bounded. That textual restriction lies in the word "warrant" itself: When a statutory term like "warrant" has been "obviously transplanted from another legal source, whether the common law or other legislation, it brings the old soil with it." *Sekhar v. United States*, 133 S. Ct. 2720, 2724 (2013). And here that "old soil" includes the unbroken historical tradition that warrants issued by U.S. judges do not run to other countries.

Third, even if a warrant may reach truly extraterritorial circumstances, the magistrate judge erred in failing to qualify his sweeping ruling by applying international comity principles. Even a statute that plainly authorizes some extraterritorial applications must be interpreted so as to avoid unnecessary international friction. *See F. Hoffmann-La Roche Ltd. v. Empagran S.A.,* 542 U.S. 155, 165-66 (2004). Consistent with that principle, it is well established that when a subpoena seeks overseas compliance, a court should not enforce the subpoena without undertaking a case-specific analysis that is sensitive to the comity implications of the information demanded. *See United States v. First Nat'l City Bank*, 396 F.2d 897 (2d Cir. 1968). If the Court accepts the government's counter-textual position that under the SCA, a "warrant" is in essence a subpoena, it should accordingly apply a similar comity analysis in deciding whether to issue or enforce a warrant for information that is stored outside the United States.

ARGUMENT

I. The SCA Does Not Authorize U.S. Courts To Issue Warrants Requiring Providers To Disclose Information Stored In A Foreign Country Absent A Substantial Nexus To The United States.

A. The Presumption Against Extraterritoriality Controls This Question.

"When a statute gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255. This canon of statutory construction, vital in our interconnected world, embodies a "presumption that United States law governs domestically but does not rule the world," (quoting *Microsoft Corp. v. AT&T Corp.*, 500 U.S. 437, 454 (2007)) and "helps ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches." *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013). Its application does not turn on a judicial understanding of a statute's purposes or the policy implications of a strictly territorial reading. Rather than "divin[e] what Congress would have wanted if it had thought of the situation before the court," judges must "apply the presumption in all cases, preserving a stable background against which Congress can legislate with predictable effects." *Morrison*, 561 U.S. at 261.

This principle governs the present dispute between Microsoft and the government. Under 18 U.S.C. §2703(a), a State or federal entity may compel "a provider of electronic communications services" to disclose the "contents of a wire or electronic communication, that has been in electronic storage in an electronic communications system," but only "pursuant to a warrant issued … by a court of competent jurisdiction." A related SCA provision, 18 U.S.C. §2703(b), similarly permits compelled disclosure of content information that is "held or maintained" by "a provider of remote computing service" so long as "the governmental entity obtains a warrant issued" by an appropriate State or federal court.

Nothing in these provisions speaks expressly to whether this "warrant" authority may be exercised with respect to information that is "in electronic storage in an electronic communications system" outside the United States, *id.* §2703(a), or "held or maintained" abroad by a remote computing service. *Id.* §2703(b)(2). Similarly, these provisions do not indicate how

a court should proceed if foreign law imposes different or additional requirements with respect to disclosure. *Cf. E.E.O.C. v. Arabian Am. Oil Co.,* 499 U.S. 244, 256 (1991) ("It is also reasonable to conclude that had Congress intended Title VII to apply overseas, it would have addressed the subject of conflicts with foreign laws and procedures."). There is simply *no* textual indication that Congress intended these warrant provisions to control access to customer accounts that have no substantial relationship to the United States. And because the SCA consequently "gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255.[5]

The magistrate judge nonetheless reasoned that "the concerns that animate the presumption against extraterritoriality simply are not present" because "an SCA Warrant does not criminalize conduct taking place in a foreign country; 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 is stored. At least in this instance, it places obligations only on the service provider to act within the United States." MJ Op. at *28.

Respectfully, that is an inadmissibly narrow conception of the presumption, which the Supreme Court has applied to resolve questions as diverse as whether the Attorney General must apply statutory protections for asylum seekers to persons interdicted on the high seas, *see Sale v. Haitian Centers Council, Inc.*, 509 U.S. 155, 173-74 (1993), whether the Federal Tort Claims Act authorizes suits against the United States for allegedly negligent conduct in Antarctica, *see Smith v. United States*, 507 U.S. 197, 203-04 (1993), and whether a federal statute entitled

---

[5] Indeed, Magistrate Judge Francis tacitly conceded (as has the government) that under the SCA, warranted searches are tied to U.S. interests in at least one respect: They may be directed only to U.S.-based providers. *See* No. 13 Mag. 2814, Dkt. No. 97, Govt' Mem. In Opposition to Microsoft's Motion to Vacate Email Account Warrant at 6 (S.D.N.Y. Apr. 25, 2014) ("Govt Opp.") (SCA "empowers courts to compel service providers *in the United States* to produce records.") (emphasis added)). *See also* MJ Op. at *21–23 (similar conclusion). Neither the magistrate judge nor the government explained why the SCA should be read as requiring that tie to the United States, but *only* that tie.

American private contractors to overtime pay for work performed overseas under contracts with the United States. *See Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949). In each instance, the statute at issue could have been implemented by persons acting within the United States, but that consideration did not affect the Supreme Court's analysis. Rather, the canon rests on a generally applicable "perception that Congress ordinarily legislates with respect to domestic, not foreign matters," *Morrison*, 561 U.S. at 255, and "serves to protect against unintended clashes between our laws and those of other nations which could result in international discord." *Kiobel*, 133 S. Ct. at 1664 (quoting *Arabian Am. Oil Co.,* 499 U.S. at 248). That sort of clash can occur whether or not a statute imposes criminal liability or requires a U.S. citizen to travel overseas. Thus, what matters is whether in practical application, the law regulates foreign matters. That is why the Supreme Court held in *Morrison* that the Securities Exchange Act would operate extraterritorially if a plaintiff could win damages by claiming that a false statement made in Florida caused him to trade to his detriment on an Australian stock exchange. The plaintiff contended that such a suit would only regulate conduct in Florida, but the Supreme Court rejected that position, observing that the suit would also amount to an extraterritorial regulation of the foreign exchange. *See Morrison*, 561 U.S. at 266–67. Likewise, the SCA would in practical effect regulate foreign conduct under the sweeping reading given to the statute by the magistrate judge, because it would govern access to the account of even an Irish customer who had never set foot in the United States, sent data to the United States, or accessed his, her or its data from the United States. Any such application would be quintessentially extraterritorial, even if a provider could facilitate government access by taking technical steps solely within this country. *See United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at *3 (W.D.

Wash., May 23, 2001) (remote search of Russian computer occurred in Russia even though searching officials acted from U.S.).

The government offered a different rationale for evading the presumption. It suggested that the presumption should not apply in this case because Microsoft "structured its affairs in order to place records beyond what it understood to be the reach of U.S. law enforcement." Govt Opp. 19. The magistrate judge did not credit that accusation, instead citing record evidence that Microsoft placed servers abroad for technical reasons that reflect basic properties of physics. MJ Op. at *3. But in any event, the Second Circuit has already made clear that intent evidence is "entirely irrelevant" to the presumption, *United States v. Vilar*, 729 F.3d 62, 78 n.12 (2d Cir. 2013), because a "statute either applies extraterritorially or it does not." *Id.* at 74 (citation omitted). And because the SCA does not contain a "clear indication" that its warrant provisions apply extraterritorially, they do not.

The question that follows is whether the specific application of the statute endorsed by the magistrate judge is extraterritorial, and thus beyond the scope of the statute. As the Supreme Court has noted, it is "often" the case that the presumption "is not self-evidently dispositive, but its application requires further analysis" to determine what is, and is not, a forbidden extraterritorial application. *Morrison*, 561 U.S. at 266. The requisite analysis looks to the "focus" of a statute, namely, the "objects of the statute's solicitude," and what the statute "seeks to regulate." *Id.* at 266-67. The SCA's "focus," as its text repeatedly reflects, is on regulating access to and disclosure of "subscriber or customer" information that is held by providers. *See, e.g.*, 18 U.S.C. §§ 2702, 2703, 2704, 2705. Accordingly, when requested information is stored outside the United States, the extraterritoriality inquiry should turn on whether there is a substantial reason to believe that the regulated relationship between the provider and the

customer or subscriber has a sufficient nexus to the United States. *Cf. Murray v. Schooner Charming Betsy,* 6 U.S. (2 Cranch) 64, 121–22 (1804) (U.S. law would not apply to foreign-flagged ship absent "substantial reason" to believe ship had sufficient American ties); Restatement §403(2) (setting out numerous, case-specific factors for determining when application of U.S. law abroad would be "unreasonable" and therefore inconsistent with international law despite existence of some connection to the U.S.). Frequently, that inquiry will be straightforward, as where a customer resides in one country and contractually or predominantly accesses its account from that country. At other times it will be somewhat complex, such as when a multinational company purchases cloud services for the purpose of regularly accessing data from several countries. Nonetheless, that fact-specific analysis not only squares with *Morrison*, but also avoids the sweeping and unwarranted consequences of the approach adopted by the magistrate, which concludes that any customer relationship that Microsoft may maintain with any customer anywhere in the world is necessarily governed by U.S. law. Congress nowhere indicated that the SCA's warrant provisions should sweep so broadly, and this Court should not adopt that construction.

B. Congress's Choice Of The Word "Warrant" Underscores That Congress Did Not Intend These Provisions To Have Global Scope.

A second interpretive canon further demonstrates that the SCA's warrant provisions do not authorize compelled disclosure of information that lacks a substantial nexus to the United States. That canon holds that when "a word is obviously transplanted from another legal source, whether the common law or other legislation, it brings the old soil with it." *Sekhar*, 133 S. Ct. at 2724 (quoting F. Frankfurter, *Some Reflections on the Reading of Statutes*, 47 Colum. L. Rev. 527, 537 (1947)). That is, "where Congress borrows terms of art" from one legal context, courts presume unless "otherwise instructed" that the new statute "adopts the cluster of ideas that were

attached to each borrowed word in the body of learning from which it was taken." *Id.* (quoting *Morissette v. United States*, 342 U. S. 246, 263 (1952)).

This rule of construction has obvious application to the SCA, which borrowed the word "warrant" from the Fourth Amendment and its common-law predecessors, in keeping with the congressional purpose to "provide a set of Fourth Amendment-like protections for computer networks." 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, 1214 (2004). It follows that the word "warrant" must be construed consistently with the "cluster of ideas" that surrounds the law of warrants. And as Microsoft has demonstrated (without dispute from the government or the magistrate judge) that body of law has long incorporated a fixed understanding that U.S. courts do not possess global warrant authority. *See, e.g.*, *United States v. Odeh*, 552 F.3d 157 (2d Cir. 2008); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000).

The magistrate judge did not apply this canon because he concluded that the SCA is "ambiguous" with respect to whether the term "warrant" was meant to incorporate "limitations on the territorial reach of a warrant." MJ Op. at *13. But of course, the very purpose of a canon of construction is to resolve uncertainties about how to read a statutory text. *See, e.g.*, *United States v. Colasuonno*, 697 F.3d 164, 173 (2d Cir. 2012). Rather than relying on notoriously fickle guides to legislative intent like inferences drawn from ambiguous statements in the legislative history (MJ Op. at *19–22) or "practical considerations" of policy (MJ Op. at *23–27), the magistrate judge should have accepted that the "warrant" provisions were not intended to apply to every customer account maintained by a U.S. service provider anywhere on earth.

The magistrate judge also declined to give the word "warrant" its ordinary meaning because he concluded that an "SCA warrant" is not a true warrant, but a "hybrid: part search

warrant and part subpoena" that is "obtained like a search warrant" and "executed like a subpoena." MJ Op. at *16. From this, the magistrate judge appeared to conclude that a warrant's application to foreign data is an aspect of the warrant's execution, and that the line of cases requiring subpoena recipients to deliver all responsive materials under their control, no matter where located, accordingly governs interpretation of the word "warrant." MJ Op. at *15–17.

This approach is flawed in several respects. First, and most fundamentally, Congress did not say that it was creating a "hybrid." What Congress said is that a "warrant" must be obtained, and that it must be obtained in the usual way, under the same "procedures" ordinarily used to procure a warrant. What that language most naturally conveys is that the "warrant" described in the SCA is an *ordinary* warrant, not some new griffin-like creation. *Cf. United States v. Bach*, 310 F.3d 1063, 1066 n.1 (8th Cir. 2002) ("While warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants [in the SCA] and we find that Congress intended them to be treated as warrants."). Second, even under the magistrate judge's "hybrid" conception, an "SCA warrant" is akin to a conventional warrant in the relevant sense. The question here is whether Congress gave courts power to issue a warrant that operates extraterritorially to compel disclosure of foreign information. That is very much a question about what kind of order the government can obtain. Any question of execution is secondary.

Below, the government likewise argued that an SCA warrant must apply extraterritorially because (1) subpoenas may be enforced in some circumstances with respect to information located abroad, and thus (2) any other view would "conflict with the SCA's general principle that information available through less rigorous legal process is also available through more demanding process." Govt Opp. 8. To be sure, courts have held that federal subpoenas may

apply extraterritorially where that effect is consistent with international comity principles, *see*, *e.g.*, *First Nat'l City*, 396 F.2d at 901-02, but that does nothing to establish that under the SCA, the same must also be true of a warrant. The government has not cited any authority for the view that if one part of a statute applies extraterritorially, related provisions must likewise apply extraterritorially to maintain purported "structural" consistency. That is no doubt because the Supreme Court has said the opposite is true. *See, e.g.*, *Morrison*, 561 U.S. at 265 ("when a statute provides for some extraterritorial application, the presumption against extraterritoriality operates to limit that provision to its terms"); *Microsoft v. AT&T*, 550 U.S. at 455-56 (similar).

There is also nothing anomalous about the idea that the SCA's "warrant" provisions would be limited in ways that do not necessarily apply to other related provisions. Under the SCA, the target of a warranted search ordinarily will not have any opportunity to contest the warrant's validity before the search occurs. In contrast, the subpoena provisions of the statute require "prior notice … to the subscriber or customer," 18 U.S.C. §2703(b)(1)(B), and thus offer the person whose account is affected an opportunity to respond, including by seeking judicial intervention. It would not likely have been lost on Congress that allowing U.S. courts to compel delivery of foreign content information without giving prior notice to an affected foreign citizen or government could provoke significant resistance from other countries. For that reason, it would not be surprising in the least if Congress decided to draw the line at subpoenas. Nothing in the text of the statute indicates otherwise.

II. Any Extraterritorial Application Of The SCA's Warrant Provisions Must Be Consistent With Principles Of International Comity.

The magistrate judge's decision is also flawed in a third, independent respect. In sweeping fashion, the ruling directs Microsoft to disclose any and all account information within the four corners of the warrant without regard to whether doing so would violate any substantive

or procedural law of Ireland or whether that information could be obtained through other channels, such as an MLAT request. If the Court concludes that the magistrate judge was right as an initial matter to hold that the SCA authorizes the use of U.S. warrants to compel disclosure of fundamentally foreign material, it should correct that aspect of the decision below.

For decades, courts in the Second Circuit and elsewhere have recognized that cross-border discovery demands in criminal and civil cases can raise serious international comity concerns because nations frequently have "diametrically opposed positions with respect to the disclosure of a wide range of information." *First Nat'l City Bank*, 396 F.2d at 901. That is certainly true where data privacy is concerned – many countries, including nations of the European Union, have adopted conceptions of data privacy interests that differ in some respects from those reflected in American law. *See, e.g.*, Schwartz & Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev., at *3-5 (Sept. 6, 2013) (forthcoming, *available at* http://ssrn.com/abstract=2271442); Resolution & Report of the American Bar Association, No. 103, at 2-6 (Feb. 6, 2012) (describing differing approaches and calling on U.S. courts to "consider and respect, as appropriate, the data protection and privacy laws of any applicable foreign sovereign, and the interests of any person who is subject to or benefits from such laws, with regard to data sought in discovery in civil litigation"). As such, there is a clear risk that an unwarranted, unduly aggressive and extraterritorial application of the SCA will produce conflicts with foreign data privacy laws. In such a circumstance, consistent with the understanding of the Founding Generation that our government should accord a "decent Respect to the Opinions of Mankind," *see* Declaration of Independence ¶ 1 (U.S. 1776), international comity principles dictate that "each nation should make an effort to minimize the potential conflict flowing from their joint concern with the prescribed behavior." *First Nat'l City*

Bank, 396 F.2d at 901. Where "a subpoena is directed at information abroad," courts in the Second Circuit typically address that risk of conflict by examining four factors relevant to "whether to order compliance or excuse it." *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544, 553-54 (S.D.N.Y. 2002). These factors are "(1) the competing interests of the nations whose laws are in conflict, (2) the hardship of compliance on the party or witness from whom discovery is sought, (3) the importance to the litigation of the information and documents requested, and (4) the good faith of the party resisting discovery." *Id.* at 554. The Supreme Court has likewise described a similar list of factors, notably including "whether the information originated in the United States," and "the availability of alternative means of securing the information," as being "relevant to any comity analysis." *See Société Nationale Industrielle Aérospatiale v. United States Dist. Court for the S. Dist. of Iowa*, 482 U.S. 522, 544 n.28 (1987); *see also* Restatement §442(1)(c).

The magistrate judge considered none of these factors – perhaps due to his conclusion that the warrant "places obligations only on [Microsoft] to act within the United States." MJ Op. at *28. But as previously noted, applying the warrant to information now stored in Ireland plainly would implicate interests in Ireland, even if Microsoft ultimately were to transmit the information using a computer located in the United States. It also bears emphasis that the government's argument is in essence that the warrant issued by the magistrate judge should be viewed as a subpoena. If the government prevails on that point, it should have no ground to object to applying a comity analysis drawn from the law of subpoenas.

Thus, if the Court finds that a warrant obtained under the SCA can be used extraterritorially to compel disclosure of foreign data, and if an objection were timely raised that disclosure of the information sought by the United States would conflict or compete with

applicable foreign law, the magistrate judge should consider the case-specific comity implications of the government's demand, and decide on that basis "whether to order compliance or excuse it." *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d at 554.

Consistent with the Supreme Court's statement in *Aérospatiale* that "the availability of alternative means of securing the information," is "relevant to any comity analysis," 482 U.S. at 544 n.28, one other factor should take on special importance in this and future cases of this kind: if the information sought by the government is stored in a country that has an MLAT with the United States, the government ordinarily should be required to rely on MLAT procedures, rather than the SCA, to obtain information from a provider's computer systems. The reason is straightforward. MLAT are binding treaties of the United States, adopted by the President with Senate advice and consent for the precise purpose of addressing the comity concerns (and other logistical obstacles) that cross-border law enforcement investigations frequently present. *See generally*, S. Exec. Rep. 110-13, *Mutual Legal Assistance Treaties with the European Union*, 2-4 (Sept. 11, 2008) (describing the general operation and purposes of MLATs), *available at* http://www.foreign.senate.gov/imo/media/doc/executive_report_110-131.pdf. When the United States seeks to side-step its own mutually negotiated agreement in favor of unilateral action, it is fair for a court to wonder why, and as such, to adopt a rebuttable presumption that unilateral action under the SCA is inconsistent with international comity principles.

This rebuttable presumption would dovetail with the approach that many American providers have adopted for addressing analogous information requests from foreign law-enforcement officials. As explained, AT&T and other major American providers do not respond directly when foreign governments request information that is stored on servers in the United States, and instead refer the requestors to the MLAT process. *See supra* at 1. That policy serves

several interlocking purposes. First, it gives U.S. persons assurance that every disclosure made to law-enforcement authorities will be made consistent with U.S. legal standards, no matter whether the request comes from a domestic or foreign government. Second, the policy affords U.S. authorities an opportunity to intervene if the foreign request raises any issue of U.S. law or policy. And third, the policy helps providers avoid "conflicting commands" from multiple sovereigns, *First Nat'l City Bank*, 396 F.2d at 901, because the MLAT process brings the sovereigns together to discuss how the provider should address the law-enforcement request.

If sustained, the approach adopted by the magistrate judge could unsettle that salutary policy. The reason is simple: under that approach, the law of the foreign place where data is stored is irrelevant to whether the provider must disclose information to U.S. authorities. If courts in this country adopt that approach, it seems safe to predict that foreign officials will likewise seek to forgo the MLAT process and demand that U.S. providers allow access to U.S.-based servers when presented with orders that satisfy foreign law.[6]

The approach adopted by the magistrate judge also poses a serious risk of harm to American companies. As the Court is no doubt aware, the scale and reach of U.S. government surveillance has been a subject of considerable controversy, and substantial misunderstanding, in recent years. That controversy has prompted some to argue that foreign consumers should not entrust their information to U.S.-based firms because of a misimpression that the U.S. government has inordinate and undue access to the information that these companies possess. *See, e.g.*, Kashmir Hill, *How the NSA Revelations Are Hurting Businesses*, Forbes Magazine (Sept. 10, 2013), *available at* http://www.forbes.com/sites/kashmirhill/2013/09/10/how-the-nsa-revelations-are-hurting-businesses/; *Foreign Intelligence Surveillance Act (FISA) Reforms:*

[6] *See* Vodafone Law Enforcement Disclosure Report, *supra* at 4 n.4.

Hearing Before S. Select Comm. on Intelligence, 112th Cong. (Comm. Print 2014) (statement of Dean C. Garfield, President & CEO, Information Technology Industry Council), *available at* http://www.intelligence.senate.gov/140605/garfield.pdf. A decision like the one reached by the magistrate judge can only feed that unfortunate perception, because its bottom-line holding appears to be that under the SCA, U.S.-based providers alone may be compelled to give U.S. authorities access to information held anywhere in the world, without regard to applicable foreign law or whether the customer-provider relationship has any substantial nexus to the United States. This Court should not endorse that view, which risks placing U.S. providers at a significant competitive disadvantage in foreign markets.

CONCLUSION

For the foregoing reasons, this Court should conclude that the SCA does not authorize U.S. courts to issue warrants that operate extraterritorially to compel providers to disclose foreign information lacking a substantial nexus to the United States. Alternatively, if the Court concludes otherwise, it should require the magistrate judge to conduct an international comity analysis before deciding whether the warrant in this case should be enforced in respect to information stored in Ireland.

Dated: June 11, 2014

Respectfully submitted,

/s/ Alan Charles Raul
Alan Charles Raul
Kwaku A. Akowuah
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
(202) 736-8000
araul@sidley.com
Attorneys for AT&T Corp.

Charles W. Douglas*
SIDLEY AUSTIN LLP
One South Dearborn
Chicago, Illinois 60603
(312) 853-7000
cdouglas@sidley.com
* *Of Counsel*
Attorneys for AT&T Corp.