14-2985-cv

United States Court of Appeals
for the
Second Circuit

In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation,

---

MICROSOFT CORPORATION,

Appellant,

– v. –

UNITED STATES OF AMERICA,

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF *AMICI CURIAE* AT&T CORP., RACKSPACE US, INC., COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION, i2COALITION, and APPLICATION DEVELOPERS ALLIANCE IN SUPPORT OF APPELLANT MICROSOFT CORPORATION

ALAN C. RAUL
KWAKU A. AKOWUAH
SIDLEY AUSTIN LLP
Attorneys for Amici Curiae
1501 K Street, NW
Washington, DC 20005
(202) 736-8000

RULE 26.1 DISCLOSURE STATEMENTS

AT&T Corp. is a wholly owned subsidiary of AT&T Inc., a publicly traded company. AT&T is one of world's largest communications companies. No entity owns more than 10% of AT&T Inc. stock.

Rackspace US, Inc. is a wholly owned subsidiary of Rackspace Hosting Inc., a publicly traded company. Rackspace is the number one managed cloud company. Its technical expertise and Fanatical Support® allow companies to tap the power of the cloud without the pain of hiring experts in dozens of complex technologies. Rackspace is also the leader in hybrid cloud, giving each customer the best fit for its unique needs—whether on single- or multi-tenant servers, or a combination of those platforms. Rackspace is the founder of OpenStack®, the open-source operating system for the cloud. Based in San Antonio, Rackspace serves more than 300,000 business customers from data centers on four continents. No entity owns more than 10% of Rackspace Hosting Inc. stock.

The Computer & Communications Industry Association (CCIA) represents more than twenty large, medium-sized, and small companies in the high technology products and services sectors, including computer hardware and software, electronic commerce, telecommunications, and Internet products and services—companies that collectively generate more than $465 billion in annual revenues. It is not owned in whole or in part by any entity.

The i2Coalition is a trade association of companies from the Internet infrastructure industry with key demographics in web hosting, data centers and Cloud infrastructure providers. It is not owned in whole or in part by any entity.

Application Developers Alliance is a non-profit global membership alliance organization that supports developers as creators, innovators, and entrepreneurs and promotes continued industry growth. It is not owned in whole or in part by any entity.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

STATUTES

LEGISLATIVE HISTORY

SCHOLARLY AUTHORITY

OTHER AUTHORITIES

INTERESTS OF THE *AMICI*[1]

Amici strongly believe it is imperative for this Court to confirm that our nation respects the data protection laws of other nations and invites reciprocal respect for our own. This is critical for businesses, for citizens, for our foreign relations, and ultimately for the future of the Internet, digital technology and consumer apps. As providers of communications and information services in many countries, *amici* (and, as applicable, their members) have direct experience with the ways national data protection laws can diverge, and recognize the importance that individuals, businesses, and governments around the world place on data protection and privacy laws. *Amici* urge the Court to adopt a construction of the Stored Communications Act that helps to reconcile these differences, and that promotes reciprocal respect for data privacy protections around the globe.

INTRODUCTION

The district court's decision is troubling because it rejects the premise that U.S. law should respect the data protection laws of foreign countries whose regulatory interests are directly implicated, dismissing those foreign interests as

---

[1] In accordance with Federal Rule of Appellate Procedure 29(c)(5) and Local Rule 29.1(b), *amici* state the following: (A) no party's counsel authored this brief in whole or in part; (B) no party or party's counsel contributed money that was intended to fund preparing or submitting the brief; and (C) no person, other than *amici* or their counsel, contributed money that was intended to fund preparing or submitting this brief. All parties have consented to this filing.

being "incidental at best." SA30. This disregard for the interplay between national laws threatens to universalize access to the private communications of American individuals and businesses. If foreign governments were to respond in kind, they could, for example, order a foreign Microsoft subsidiary to obtain and disclose to foreign authorities any private customer information in the United States that the foreign subsidiary is technically able to access from abroad, applying only foreign legal standards to the question. Such treatment would plainly undermine Congress's effort to "ensure the continued vitality of the Fourth Amendment," *see* H.R. Rep. No. 99-647, at 19 (1986), by enacting the Stored Communications Act ("SCA") and other privacy laws.

These practical policy considerations highlight the district court's key legal error—its misapplication of the presumption against extraterritoriality. That presumption makes clear that it is for Congress to decide whether federal statutes apply extraterritorially, and thereby precludes the district court's conclusion that the SCA silently authorized U.S. courts to regulate access to private customer communications that are stored anywhere in the world by any company that has a U.S. presence. The presumption instead counsels that the SCA applies only to customer accounts that can be fairly characterized as having a substantial nexus to the United States, and thus as within the statute's domestic focus. *Amici* ask this Court to reject the district court's sweeping extraterritorial application of the SCA

and adopt a more balanced approach, in line with Second Circuit precedent on the presumption against extraterritoriality and with congressional intent.

SUMMARY OF ARGUMENT

Amici strongly agree with Microsoft and with the Verizon *amici* that the district court's overbroad construction of the SCA is bad for American foreign relations (because it intrudes on the sovereignty of U.S. trading partners), bad for American business (because it threatens relationships with foreign consumers), bad for American citizens (because it invites reciprocal intrusions into U.S.-located data from foreign states that do not have any legitimate regulatory interest in the data and that may have far less protective data protection regimes), and bad for the future of the Internet, digital technology and consumer applications (because it invites countries to wall off and segment information so that it cannot be reached by U.S. law enforcement).

Amici also recognize that there are countervailing interests at play. A rigid rule that places all information stored in the United States (however temporarily or incidentally) within the reach of U.S. law enforcement and exempts all data outside the United States (no matter how strong the connection to this country) would also have undesirable effects. Under that sort of rule, information that is in all relevant senses closely tied to the United States, and that law enforcement officials have a legitimate need to reach, could become unreachable in an instant. That could occur

because the information is moved to a place outside the territorial jurisdiction of any state (*e.g.*, on the high seas) or to a place that is unlikely to cooperate with any U.S. law enforcement effort (*e.g.*, Iran).

By the same token, a rigid territorial rule could subject information that is in all relevant senses foreign to compelled disclosure under U.S. data protection laws merely because it is temporarily or incidentally stored on U.S.-based servers, perhaps for technical processing reasons. And a rigid geographical rule could simply prove unworkable. In the modern world, information moves fast and moves often. Information associated with a particular account could be stored one place in one moment (*e.g.*, when the government submits its warrant application), at a second place at the next (*e.g.*, when the magistrate judge approves the application), and in a third place at another relevant moment in time (*e.g.*, when the government serves the warrant). A rule keyed solely to geography could therefore prove unduly difficult to apply in a whole range of circumstances.

These realities can be addressed by requiring a district court to view geography as a predominant but not exclusive factor when considering an SCA warrant application, and to ask also whether the customer or subscriber account at issue can be fairly characterized as having a substantial nexus to the United States. Such a test would be consistent with this Court's recent observation that "evaluation of the presumption's application to a particular case" requires "inquiry

into whether the domestic contacts are sufficient to avoid triggering the presumption at all," and whether the "particular combination of conduct in the United States" is sufficient to make the case "domestic." *Mastafa v. Chevron Corp.*, 770 F.3d 170, 182, 190-91 (2d Cir. 2014).

Specifically, the Court should instruct district courts to apply the following framework when considering whether an SCA application involves a permissible regulation of a "domestic" provider-customer relationship, or rather an impermissible regulation of a "foreign" relationship.

Data Stored in the United States: A warrant will provide adequate legal process. However, the provider or account-holder, as appropriate, should be permitted to demonstrate that the information has such an incidental connection to the United States that it should be best understood as foreign in nature, and the district court should be required to consider such information in deciding whether to require compliance with the warrant.

Data Stored Outside the United States: A warrant will provide adequate legal process only if the sworn warrant application recites that the data at issue belongs to a United States citizen or resident; that the content was generated under a U.S.-based service or transaction; or identifies some other substantial connection to the U.S. beyond the mere presence of the holder of the data in the U.S. If that recitation is missing or insufficient, the district court should determine that it lacks

statutory authority to issue or enforce a warrant for the information.[2] Where the recitation is adequate, the district court should then consider whether case-specific comity considerations—including, where applicable, MLAT procedures allowing access to the account in a manner consistent with foreign law—counsel against issuance or enforcement of a U.S. warrant. *Cf. Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court*, 482 U.S. 522, 544 n.28 (1987); *Ings v. Ferguson*, 282 F.2d 149, 152-53 (2d Cir. 1960).

Consistent with the presumption against extraterritoriality, this test would respect Congress's presumed intent to regulate only domestic matters, while also significantly balancing legitimate policy concerns, providing a workable test for law enforcement and providers, and granting district courts a degree of flexibility in responding to compelled disclosure requests as technological advances continue to test and stretch the SCA.

Amici also respectfully urge the Court to conclude that the so-called *Bank of Nova Scotia* doctrine—which supports law enforcement access to a company's own business records that are stored abroad—has no application here. Before the

[2] Because the SCA confers immunity with respect to any claims relating to a disclosure made pursuant to a warrant or another specified form of legal process, providers would be entitled to rely on a judicial officer's decision to issue a warrant based on a"substantial nexus" determination, just as providers are entitled to rely on a magistrate's probable cause determination. *See* 18 U.S.C. §§ 2703(e), 2707(e).

district court, the government was not able to identify a single case in which *Bank of Nova Scotia* has been invoked to justify law enforcement access to the contents of communications stored by providers.

ARGUMENT

I. The SCA Authorizes Compelled Disclosure Only of Data That Can Be Fairly Characterized as Having a Substantial U.S. Nexus.

Like Microsoft, *amici*'s position is rooted in "the 'presumption that United States law governs domestically but does not rule the world,'" *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013) (quoting *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 454 (2007)). This presumption precludes the district court's view that the SCA silently authorizes U.S. officials to reach any and all information abroad that companies with a U.S. presence can reach from within the United States. Indeed, the presumption exists largely to "'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*, 133 S. Ct. at 1664. But as Microsoft correctly has observed, the decision below has created just the kind of international friction that courts are obliged to avoid. *See* Brief for Appellant at 13–14, 59–60.

To be sure, the district court first appeared to accept—correctly—that the SCA does not contain the "clear indication of extraterritoriality" necessary to overcome the presumption. *See Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247,

265 (2010). Nothing in the text of the SCA suggests that the authority to compel disclosure of information pursuant to a warrant extends to extraterritorial applications. Nor do these provisions indicate how a court should proceed if foreign data protection laws impose different or additional requirements with respect to disclosure, even though "[t]he 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.'" *Id.* at 269 (quoting *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 256 (1991)).

Having successfully cleared the first step of the analysis, the district court erred at the second, which requires a court to ask "how the presumption affects the particular statutory provision in view of the 'focus of congressional concern,'" *Loginovskaya v. Batratchenko*, 764 F.3d 266, 271 (2d Cir. 2014) (quoting *Morrison*, 561 U.S. at 266), and "involves an evaluation of the territorial events or relationships that were the focus" of the statute. *Mastafa*, 770 F.3d at 184 (quotation marks and alterations omitted). This second step is pivotal because "it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States." *Morrison*, 561 U.S. at 266. When a case involves contacts with both the United States and foreign territory, a court must "delineate the types of contacts within the United States that would render an application of

the statute domestic rather than extraterritorial." *Liu Meng-Lin v. Siemens AG*, 763 F.3d 175, 179 (2d Cir. 2014).[3] And it must do so by considering the statute's regulatory "focus," as illustrated by its text and the "context" in which the statute operates. *Morrison*, 561 U.S. at 265, 266.

The SCA establishes rules governing access to, and disclosure of, electronic information that providers hold in a "subscriber or customer" account. Section 2702 of title 18 ("Voluntary disclosure of customer communications or records") generally provides that a provider "shall not knowingly divulge" such information. Section 2703 of the same title ("Required disclosure of customer communications or records") sets out certain exceptions to that prohibition. And other provisions of section 2703, along with sections 2704 and 2705, regulate the circumstances in which the "subscriber or customer" must be informed that a relevant disclosure has been made from his or her account. *See also* H.R. Rep. No. 99-647, at 17–18 (expressing concern that "[u]nder existing law, the interception of these services [*e.g.*, e-mail] or disclosure of the contents of messages over these services are probably not regulated or restricted").

[3] Indeed, *Morrison* itself held that because the "focus" of the Exchange Act is on regulating domestic transactions, a suit alleging that a false statement made in Florida caused a plaintiff to trade on a foreign exchange constitutes an impermissibly extraterritorial application of the statute, notwithstanding the clear (but in this sense irrelevant) allegation that the defendant's core misconduct occurred in this country. 561 U.S. at 266-70.

This statutory focus, taken together with the absence of any indication of congressional intent to regulate extraterritorially, strongly indicates that the SCA's compulsory disclosure provisions, *see* 18 U.S.C. § 2703, should be construed to regulate *domestic* customer accounts, and so to regulate the circumstances in which law enforcement officials can intrude on those *domestic* accounts by demanding disclosure from those accounts of information that providers otherwise would be obligated to hold private. *See id.* § 2702.

This understanding of the statute's regulatory focus should also inform how courts identify the specific "domestic" customer-provider relationships that are properly regulated by the SCA's compelled disclosure provisions. While *amici* agree with Microsoft that the location of storage will generally provide a compelling indication of whether a particular customer account is "domestic" for SCA purposes, they also believe that other considerations may also be relevant because, as two hypothetical examples below illustrate, data created or held as part of a customer account can in some circumstances be most accurately viewed as "domestic" when it is located abroad, and "foreign" when it is located here.

We first invite the Court to consider a person who lives and works in New York and contracts with a cloud service provider so he or she will have ready access to his or her personal or business information from any number of locations. If the provider has servers both in the United States and in other countries (as many

do), that information might at times shift between servers inside and outside the United States. It is also possible that, at times, copies of certain information will be stored on servers in multiple countries. Given the strong and substantial nexus that the customer account in this example would have with the United States, it would be consistent with the presumption against extraterritoriality to treat the information in that account as subject to compelled disclosure under the SCA even when located abroad (subject, always, to the district court's further consideration of whether case-specific international comity interests counsel against issuance or enforcement of a warrant).

On the other hand, information held in an account that does not have a substantial nexus to the United States may sometimes be incidentally stored or accessible in this country. For example, an Indonesian company that does not operate in the United States could contract for cloud storage services with a provider that has affiliates in both Indonesia and the United States and agrees to store the Indonesian company's information outside the United States, with the caveat that this foreign-stored data might be incidentally transferred to the U.S. affiliate for technical processing or other limited purposes. Because the customer account would have only a transitory connection to the United States, *amici* submit that the incidental presence of the foreign company's information, standing alone, would not justify applying the SCA's disclosure requirements to that information.

In a sense, the challenge of identifying the "domestic" communications that Congress intended to regulate through the SCA resembles the issue that courts have traditionally faced in deciding how and when to apply U.S. domestic statutes to oceangoing ships. Because such vessels are constantly on the move and therefore regularly interact with different (and potentially conflicting) national legal rules, U.S. courts traditionally have declined to apply federal law with full force every time a foreign ship enters U.S. waters. *See, e.g.*, *Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 142 (1957); *McCulloch v. Sociedad Nacional de Marineros de Honduras*, 372 U.S. 10, 19-22 (1963). Absent clear guidance from Congress, courts have instead asked whether the ship has a fundamentally foreign character (in that context, by asking under what flag the ship flies), and if so have applied U.S. statutes sparingly to the ship itself, as well as its crew and cargo. For example, the Supreme Court declined to treat U.S. labor laws as controlling the validity of wage contracts that foreign sailors signed abroad, *Benz*, 353 U.S. at 142, or U.S. patent law as governing rights in shipboard technology that was installed abroad and incidentally transported into U.S. waters. *See Brown v. Duchesne*, 60 U.S. (19 How.) 183, 196-99 (1856); *see also Spector v. Norwegian Cruise Line, Ltd.*, 545 U.S. 119, 125 (2005) (indicating that Americans with Disabilities Act would not apply to "foreign-flag cruise ships," where "it requires removal of physical barriers").

The point is not that foreign ships are categorically immune from generally worded U.S. laws, *see, e.g.*, *Cunard S.S. Co. v. Mellon*, 262 U.S. 100 (1923) (Prohibition-era alcohol laws applied to foreign ships in U.S. waters), but rather that absent clear congressional direction, considerations of "international comity" have been understood to require leaving matters not principally affecting the United States "'to be dealt with by the authorities of the nation to which the vessel belonged.'" *Spector*, 545 U.S. at 130 (quoting *Wildenhus's Case*, 120 U.S. 1, 12 (1887)).

Electronic communications similarly may encounter multiple (and perhaps conflicting) legal systems as they travel. *See, e.g.*, Schwartz & Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. 877, 881–91 (2014) (noting differing conceptions of data privacy); Am. Bar Ass'n, *Resolution No. 103* (Feb. 6, 2012) (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"); *id.*, *Report* at 2–6 (describing different national approaches). As such, and for similar reasons, an approach that focuses solely on the potentially transient factor of storage location would be both over-inclusive and under-inclusive. To decide which electronic communications are best characterized as "domestic,"

therefore, courts should not look solely to its potentially transient location, but should instead ask other questions, pertinent to the context, that indicate whether the customer account at issue is best characterized as foreign or domestic. That analysis should look to ties like the citizenship or place of residence of the customer or subscriber, the places where the customer or subscriber typically accesses the account, the locus of the business relationship, and the places from which the provider typically services the account to determine whether the particular customer or subscriber account at issue has a substantial nexus to the United States.

Amici recognize that this framework would require courts to conduct a case-specific analysis of the contacts, if any, that link a specific customer account to this country. But this sort of case-by-case consideration is commonplace. *See, e.g.*, *Goodyear Dunlop Tires Operations, SA v. Brown*, 131 S. Ct. 2846, 2851 (2011) (U.S. courts may exercise "general jurisdiction" over foreign corporations only "when their affiliations with the State are so continuous and systematic as to render them essentially at home in the forum State") (quotation marks omitted). It would be highly appropriate here, moreover, because "[m]echanical or overbroad rules of thumb are of little value" in considering whether U.S. law should be used to compel the delivery of materials located overseas; "what is required is a careful balancing of the interests involved and a precise understanding of the facts and

circumstances of the particular case." *United States v. First Nat'l City Bank*, 396 F.2d 897, 901 (2d Cir. 1968). Similarly, as this Court has recently confirmed, determining whether conduct is "domestic," in terms of "the presumption's application to a particular case," requires consideration of the "particular combination of conduct in the United States," *Mastafa*, 770 F.3d at 182, 190-91, and judicial "delineation" of the specific contacts that would make a particular application of a statute domestic rather than extraterritorial. *Siemens*, 763 F.3d at 179. *Amici*'s proposed construction of the SCA is consistent with this domestic contacts inquiry, and with the statute's specific language and purposes.

II. The District Court's Holding Rests On Significant Additional Errors of Law.

Giving undue weight to Microsoft's ability to secure the information sought by acting in the United Stats, the courts below each held that applying the SCA's compulsory disclosure provisions to information stored outside the United States cannot involve an extraterritorial application of U.S. law. Those conclusions ignore that allowing U.S. authorities to access any and all communications that a U.S. affiliate of a provider has the technical capacity to reach would plainly affect the legitimate interests of foreign nations in setting data protection rules for their own citizens and businesses, just as it would obviously affect U.S. prerogatives if another country authorized its police to seize and scan any private email in the United States that could be moved abroad through a provider's network. *Cf. F.*

Hoffman-LaRoche v. Empagran, S.A., 542 U.S. 155, 165 (2004) ("No one denies that America's antitrust laws, when applied to foreign conduct, can interfere with a foreign nation's ability independently to regulate its own commercial affairs.").

The rationales that the courts below cited in support of their conclusions were flawed in significant ways. The magistrate judge first held that the government's demand did not involve an extraterritorial application because it does not criminalize conduct abroad, does not require deployment of U.S. personnel, does not require physical presence of service provider personnel abroad, and requires actions only within the United States. SA21–22. That view of the presumption is unduly cramped and literalistic; it must be rejected because it conflicts directly with the many Supreme Court's precedents finding the application of a statute to be impermissibly extraterritorial even though all actions necessary to implement the statute could have been undertaken by people acting wholly within the United States. *See, e.g.*, *Sale v. Haitian Cntrs. Council, Inc.*, 509 U.S. 155, 173-74 (1993) (Attorney General need not apply statutory protections for asylum seekers to persons interdicted on the high seas); *Smith v. United States*, 507 U.S. 197, 203–04 (1993) (Federal Tort Claims Act does not authorize suits against the United States for allegedly negligent conduct in Antarctica); *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949) (American workers not entitled to overtime pay for work performed overseas under federal government contracts). Indeed,

that description cannot even account for *Morrison*, which did not involve any of the elements that the magistrate judge seemed to view as prerequisites for applying the presumption.

The district court relied on an equally flawed rationale, citing the so-called "*Bank of Nova Scotia*" cases as its principal basis for holding that the warrant in this case does not involve an extraterritorial application of U.S. law.[4] These cases hold that a party subject to U.S. jurisdiction may be subpoenaed to deliver copies of its *own* records to assist a grand jury or other law enforcement investigation, even if those records are located outside the United States. *See, e.g.*, *United States v. Bank of Nova Scotia*, 691 F.2d 1384, 1388 (11th Cir. 1982) (subpoena for bank transaction records); *In re Marc Rich & Co.*, 707 F.2d 663 (2d Cir. 1983) (subpoena for commodity trader's records of crude oil transactions); *First Nat'l City Bank*, 396 F.2d at 901 (bank transactions).

[4] The district court also described a Restatement provision as "dispositive." SA 30. But that provision offers no guide to whether any specific statute should be construed as authorizing extraterritorial applications. It states simply that "*when authorized by statute or rule of court*," a court or agency may order production of documents or other information from abroad. Restatement (Third) of Foreign Relations Law § 442(1)(a); *see also id.* cmt. b ("Whether an agency's authority to require disclosure includes authority to demand production of documents or information located abroad is a matter of interpretation of the governing statutes . . . . *General authorization to issue disclosure orders should not necessarily be construed as implying such authority*.") (emphasis added). The Restatement thus correctly indicates that the first-order question is one of congressional intent—one that must be analyzed by applying the presumption against extraterritoriality and other principles of statutory construction.

But the district court's analogy fails because it wrongly assumes that content stored by a customer with a communications provider is equivalent in kind to a bank's records of its own transactions. Rather, the mere fact that private communications "might be kept on a server owned or maintained by the email provider . . . does not mean that the information in those emails belongs to the provider—just the opposite." *Brown v. Tellermate Holdings Ltd.*, No. 2:11–cv–1122, 2014 WL 2987051, at *8 (S.D. Ohio July 1, 2014) (addressing business information stored by a cloud provider). In fact, reflecting an understanding that a customer's communications are "analogous to items stored, under the customer's control, in a safety deposit box" and are "[u]nlike" the records of a bank, H.R. Rep. No. 99-647, at 23 n.41, the SCA directs that a provider "shall not knowingly divulge" the contents of private communications except in circumstances specifically delineated by the statute. *See* 18 U.S.C. § 2702. Notably, the district court did not give any reason for treating private customer communications in the same manner as a bank's own records of its transactions, other than to contend, erroneously, that Microsoft had waived any argument that they are different. *See* SA30. The district court so ruled even though the parties plainly had joined issue and were available, along with various *amici*, to provide additional briefing and argument.

This Court should not compound that mistake. "An issue is reviewable on appeal only if it was 'pressed or passed upon below.'" *United States v. Harrell*, 268 F.3d 141, 146 (2d Cir. 2001) (quoting *United States v. Williams*, 504 U.S. 36, 41 (1992)). The district court directly "passed upon" whether private customer communications may be treated like bank records in respect to compulsory disclosure to the government, *see* SA30, and Microsoft just as plainly "pressed" a different view to that court. *Id*. The Court should accordingly review the issue. Upon doing so, it should recognize that private customer communications are different in fundamental respects from banking or commodities trading records, that the text and legislative history of the SCA reflect that distinction, and that there is accordingly no sound reason to conclude that Congress intended the SCA's provisions applicable to the contents of communications stored by service providers to be read in light of the *Bank of Nova Scotia* business record cases.

It was particularly inappropriate for the district court to extend *Bank of Nova Scotia* to electronic communications stored outside the U.S. because of the stark conflict between the reasoning of the *Bank of Nova Scotia* cases and that of the Supreme Court decisions applying the presumption against extraterritoriality. The latter decisions emphasize that the courts should not read generally worded statutes in ways that might provoke international tensions, and should instead wait for Congress to take the lead in addressing any extraterritorial application. *See, e.g.*,

Kiobel, 133 S. Ct. at 1664; *Arabian Am. Oil Co.*, 499 U.S. at 248; *Benz*, 353 U.S. at 147.

Bank of Nova Scotia and its progeny adopt the opposite approach. They do not purport to rest on any clear statutory authorization, and some even go so far as to deny that any such enabling legislation could be necessary. *See Marc Rich & Co.*, 707 F.2d at 668-69. Unlike the district court here, moreover, these cases expressly recognize that "international friction has been provoked by enforcement of subpoenas" seeking foreign-located information, *Bank of Nova Scotia*, 691 F.2d at 1388, and acknowledge that such subpoenas may "impinge upon the political prerogatives of the government in the sensitive area of foreign relations." *Id.* That candid acknowledgement arguably understates the point: The Restatement (Third) of Foreign Relations reports that "[n]o aspect of the extension of the American legal system beyond the territorial frontier of the United States has given rise to so much friction as the requests for documents in investigation and litigation in the United States." Restatement (Third) of Foreign Relations Law § 442, reporters' note 1. And the government has conceded elsewhere that "foreign governments strongly object to [*Bank of Nova Scotia*] subpoenas, contending that they constitute an improper exercise of United States jurisdiction." Department of Justice, *Criminal Resource Manual* 279 (1997).

The *Bank of Nova Scotia* cases thus turn the presumption against extraterritoriality on its head. Rather than allow Congress to lead, thus avoiding "'foreign policy consequences not clearly intended by the political branches,'" *Kiobel*, 133 S. Ct. at 1664, these cases announce that courts will knowingly press into diplomatically sensitive fields, but "remain open to the legislative and executive branches of our government if matters such as this prove to have international repercussions." *Bank of Nova Scotia*, 691 F.2d at 1388.

Significantly, the district court's application of the *Bank of Nova Scotia* cases was also inapt. Far from blessing the district court's conclusion that the only pertinent factor is whether the subpoena recipient has control over the requested information, *see* SA30, those cases recognize that because cross-border discovery demands can cause serious international friction, courts must conduct a case-specific comity analysis before deciding "whether to order compliance" with a *Bank of Nova Scotia* subpoena "or excuse it." *In re Grand Jury Subpoena Dated Aug. 9, 2000*, 218 F. Supp. 2d 544, 554 (S.D.N.Y. 2002); *see also First City Nat'l Bank*, 396 F.2d at 901-03 (describing necessary comity analysis). The Supreme Court has likewise identified a number of factors relevant to international comity where foreign discovery is sought from a party to a U.S. civil dispute, most notably including "whether the information originated in the United States," and "the availability of alternative means of securing the information." *See Aérospatiale*,

482 U.S. at 544 n.28; *see also* Restatement (Third) Foreign Relations Law § 442(1)(c).

Consistent with that guidance, this Court has declined to enforce a subpoena directed to Canadian banks for information located in Canada, reasoning that in the circumstances presented, "fundamental principles of international comity," required the requesting party to use Canadian procedures to obtain the information. *Ings*, 282 F.2d at 152; *see also United States v. First Nat'l Bank of Chi.*, 699 F.2d 341, 345-47 (7th Cir. 1983) (distinguishing *Bank of Nova Scotia* on its facts and declining on comity grounds to enforce IRS subpoena for bank records located at a Greek branch office). The district court dispensed with this comity analysis altogether, however, declining as a result to consider matters like whether the information in the e-mail account originated in the U.S., whether U.S. officials could alternatively have used the MLAT process to obtain the information in a manner consistent with Irish law, or whether—as a former Attorney General of Ireland attested below—the disclosure could violate Irish law if it did not occur pursuant to an order made by an Irish court. *See* A116.

For all of these reasons, the *Bank of Nova Scotia* cases—none of which involved the SCA or communication service providers—cannot justify the district court's construction of the SCA, which directly conflicts with the presumption against extraterritoriality and with the Supreme Court's directive that the

presumption must be applied "in all cases, preserving a stable background against which Congress can legislate with predictable effects." *Morrison*, 561 U.S. at 261.

CONCLUSION

Amici respectfully ask this Court to vacate the district court's contempt order and remand for the district court to consider whether the customer account addressed in the warrant application at issue bears a substantial nexus to the United States.

Dated: December 15, 2014

/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
kakowuah@sidley.com
Attorneys for Amici Curiae

Of Counsel:

Wayne Watts
Senior Executive Vice President and
General Counsel
AT&T Inc.
208 South Akard Street
Dallas, TX 75202
(214) 757-3300

Perry C. Robinson
Justin D. Freeman
Rackspace U.S. Inc.
1 Fanatical Place
City of Windcrest
San Antonio, TX 78218
(210) 312-4700

Bijan Madhani
Computer & Communications
Industry Association
900 17th Street NW, Suite 1100
Washington, D.C. 20006
(202) 783-0070

Timothy Sparapani
Vice President, Policy, Law &
Government Affairs
Application Developers Alliance
1025 F. Street NW, Suite 720
Washington, DC 20004
(202) 250-3008

David Snead
Co-founder and public policy chair
i2Coalition
P.O. Box 33115
Washington, D.C. 20033
(202) 558-2366

CERTIFICATE OF COMPLIANCE WITH FED. R. APP. 32(a)(7)(B)

1. This brief complies with the type-volume limitations of Federal Rules of Appellate Procedure 29(c) and 32(a)(7)(B) because this brief contains 5,373 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(&)(B)(iii).
2. This brief complies with the requirements of Federal Rule of Appellate Procedure 29(c), the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2007 in Times New Roman 14-point font.

Dated: December 15, 2014

/s/ Alan Charles Raul
Alan Charles Raul
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
(202) 736-8000