NO. 17-2

In the
Supreme Court of the United States

UNITED STATES OF AMERICA,
Petitioner,
v.
MICROSOFT CORPORATION,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Second Circuit

BRIEF FOR *AMICUS CURIAE* INTERNATIONAL BUSINESS MACHINES CORPORATION IN SUPPORT OF RESPONDENT

MICHELLE H. BROWDY
DANIELA COMBE
ANDREW H. TANNENBAUM
GEORGE KOTLARZ
IBM CORPORATION
One North Castle Drive
Armonk, NY 10504
(914) 765-4343

PAUL D. CLEMENT
Counsel of Record
GEORGE W. HICKS, JR.
DAMON C. ANDREWS
KIRKLAND & ELLIS LLP
655 Fifteenth Street, NW
Washington, DC 20005
(202) 879-5000
paul.clement@kirkland.com

Counsel for Amicus Curiae

January 18, 2018

CORPORATE DISCLOSURE STATEMENT

Amicus curiae states that it has no parent corporation and that no publicly held company owns more than 10% of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provision

Statutes

Rule

Other Authorities

STATEMENT OF INTEREST[1]

The exponential growth of data is the phenomenon of our time, fueling a rapidly evolving data economy with new technologies that are changing the way we live and work. This case involves one such transformative technology for businesses worldwide—cloud data storage. It provides a prime example of how technology often moves faster than the law.

The government in this case seeks to leverage emerging cloud technology to obtain an individual cloud user's emails stored abroad. The potential interests at stake, however, extend beyond individual cloud consumers. In particular, commercial enterprises increasingly rely upon the cloud to store their most important data, the lifeblood of their businesses. They do so while navigating a fluid and complex landscape of technological, economic, security, privacy, and legal concerns, often across international borders. For multiple reasons, the result the government seeks here would be even more problematic in this enterprise context. The government itself has recognized that the enterprise cloud involves unique considerations requiring careful application of distinct rules regarding government

---

[1] Pursuant to Supreme Court Rule 37.6, *amicus curiae* states that no counsel for any party authored this brief in whole or in part, and no entity or person, aside from *amicus curiae*, its members, and its counsel, made any monetary contribution toward the preparation or submission of this brief. Pursuant to Supreme Court Rule 37.3, counsel of record for all parties have consented to this filing via blanket consents filed with the Clerk's Office on November 9, 2017.

access to data.[2] This Court should always be hesitant to project United States law abroad and to bend existing jurisprudence to accommodate novel concerns better addressed by the political branches. Both concerns counsel caution here. The Court should avoid inadvertently crafting a rule regarding the government's ability to compel disclosure of cloud data that could have unintended consequences on enterprises in the United States and around the world.

The advent of cloud computing and cloud data storage has effected a paradigm shift in how society interacts and how companies conduct business. By allowing access to content from anywhere in the world with an Internet connection, the cloud provides users with an unprecedented degree of mobility. The benefits of the cloud—including scalability, workload migration, resiliency, and cost savings—are plentiful for both consumers and businesses alike. *See* Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law In the Cloud*, 73 Md. L. Rev. 313, 324-329 (2013); *see also* Kevin Werbach, *The Network Utility*, 60 Duke L.J. 1761, 1815-23 (2011); *see generally* Joe Weinman, *Cloudonomics: The Business Value of Cloud Computing* (2012).

International Business Machines Corporation (IBM) has a long history of leading enterprises through technological shifts, as an inventor and driver of transformative technologies for over a century.

---

[2] *See* U.S. Dep't of Justice, *Seeking Enterprise Customer Data Held by Cloud Service Providers* (Dec. 2017), http://bit.ly/2mEaf LF ("*DOJ Guidelines*") (advising prosecutors to seek data directly from enterprises rather than from their cloud providers).

IBM is a pioneer and globally recognized leader in cloud-computing technology, cloud services, cloud data storage, and global information technology services. Through its innovative cloud offerings, IBM offers a diverse suite of cloud-based services, including infrastructure, data storage, data management, analytics, security, and information technology consulting. In the past two years alone, IBM has received numerous awards for its cloud-based services, including 2016 North American Cloud Company of the Year,[3] an inaugural 2017 Cloud Excellence Award,[4] and 2017 Best Managed Security Service.[5] The U.S. Army has entrusted IBM with providing critical, cloud-based operational services, software support, and cognitive computing,[6] as well as with building and managing a secure cloud data center in the United States.[7] IBM's cloud services are used to teach math to elementary school students,[8]

---

[3] Press Release, Frost & Sullivan, Frost & Sullivan Awards Gala Draws in Top Industry Leaders for Prestigious Recognition (Jan. 12, 2017), http://bit.ly/2mBcoHV.

[4] Press Release, Incisive Media, Computing, Cloud Excellence Awards 2017, http://bit.ly/2DBcK9T (last visited Jan. 18, 2018).

[5] Carmina Lees, *IBM Wins 'Best Managed Security Service' at 2017 SC Europe Awards*, IBM: SecurityIntelligence (June 8, 2017), https://ibm.co/2pHnsag.

[6] *Army Re-Ups With IBM For $135 Million In Cloud Services*, Cloud Strategy (Sept. 7, 2017), http://bit.ly/2D9ekP9.

[7] Stephanie Condon, *US Army turns to IBM to build, manage private cloud data center*, ZDNet: Between the Lines (Jan. 18, 2017), http://zd.net/2FC5drQ.

[8] Nick Morrison, *Will AI Be The Next Big Thing In the Classroom?*, Forbes (Sept. 13, 2017), http://bit.ly/2DCjZhF.

predict weather patterns and natural disasters,[9] reduce healthcare costs through always-available access to patient information,[10] and for countless other purposes. Accordingly, IBM is at the forefront of cloud technology across an array of industries that rely upon the cloud.

As its name suggests, IBM's business is truly international. IBM has nearly sixty cloud data centers spread throughout nineteen countries on six continents. These data centers anchor IBM's cloud-based services, which IBM provides primarily for enterprise clients. Unlike individual consumers—who typically deploy cloud-based systems for personal uses (such as e-mail and social media), and who typically access a particular cloud-based system from one connected device at a time—enterprises usually are large-scale and commercial in nature, and rely on cloud-based systems to support key functions of their business operations, which are run across networks of computers and devices from multiple locations. The information stored by enterprises cuts to the core of their businesses and may include sensitive customer and employee information, sales data, trade secrets, and documents subject to legal privilege. IBM's relationships with enterprise clients, moreover, are governed by arms-length contracts, with roles and responsibilities clearly assigned and understood by

---

[9] Mike Murphy, *IBM is going to change how we forecast the weather with Watson*, Quartz (Oct. 29, 2015), http://bit.ly/2r5AT5y.

[10] Lance Ulanoff, *IBM's Watson Health Cloud is on a mission to reduce healthcare costs*, Mashable (Apr. 13, 2015), http://on.mash.to/2r8DM5E.

the sophisticated parties. European enterprises, for example, typically contract for cloud services with a local IBM country subsidiary, thus subjecting their relationships to a host of local laws and, where applicable, European Union (EU) laws.

Given the nature and importance of enterprises' cloud data, it follows that enterprises have an acute sensitivity to data security and data privacy. IBM understands this first-hand by working proactively with enterprises to protect them from a number of cyber threats, such as the theft of sensitive data and attacks aimed at disrupting business operations. IBM also is keenly aware that enterprises are sensitive to government overreach, particularly in the wake of disclosures relating to the U.S. government's foreign intelligence surveillance programs. To that end, IBM has been an advocate for requiring governments to use proper legal channels to access cloud data, including through an open letter to clients reaffirming IBM's understanding of the importance of business data to enterprise clients and IBM's commitment to privacy and security of cloud data.[11] Moreover, IBM's cloud infrastructure enables enterprise clients to choose where their data are physically stored, and clients often make that selection deliberately based on, among other factors, concerns about security and privacy, including government access to their data.

At the same time, IBM also has been proactive in working *with* governments to develop standards and

---

[11] Robert C. Weber, *A Letter to Our Clients About Government Access to Data*, IBM: THINK Blog (Mar. 14, 2014), https://ibm.co/2rjyl0c; *see also Data Responsibility @ IBM*, IBM: THINKPolicy (Oct. 10, 2017), https://ibm.co/2gsQMvq.

protocols to assure customers that their cloud data are secure. Last year, IBM was among the first companies to sign on to the EU Data Protection Code of Conduct for Cloud Service Providers, which seeks to increase trust and transparency in the cloud industry, and which resulted from a collaborative effort between industry participants and the European Commission.[12]

Not only does IBM know first-hand the benefits for enterprises of cloud services, IBM also knows that competition for enterprise clients is fierce and international. A rule allowing the government to obtain cloud data stored abroad by a U.S.-based company will significantly disadvantage U.S. cloud services providers when it comes to competing for enterprise clients, who may prefer to use cloud services from a company with no presence in the United States. This concern is not a hypothetical; it was on full display following disclosures about the U.S. government's surveillance programs,[13] and it continues to be a topic of significant concern for enterprise customers today.

Compared to individual cloud consumers, enterprise clients generally are more sophisticated,

---

[12] *IBM software, cloud services now adhere to EU Cloud Code of Conduct*, Int'l Ass'n of Privacy Professionals: Daily Dashboard (June 15, 2017), http://bit.ly/2DgIAeh.

[13] *See, e.g.*, Aarti Shahani, *A Year After Snowden, U.S. Tech Losing Trust Overseas*, NPR (June 5, 2014), http://n.pr/2FFA2vD; Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. Times (Mar. 21, 2014), http://nyti.ms/2Ddvhw; Rob Lever, *Snowden Revelations Costly for US Tech Firms, Study Says*, Phys.Org (June 9, 2015), http://bit.ly/2r9uSoz.

have more riding on the confidentiality and security of their data (and their customers' data), and face potential liability for breaches of confidentiality and privacy. As stewards of their clients' most vital information, enterprise cloud services providers like IBM share their clients' concerns and work closely with them to safeguard and advance their clients' interests.

* * *

The case before the Court involves the government's effort to obtain *an individual's* cloud data stored abroad. The government's arguments in support of that effort are even more problematic, and the potential consequences even more troubling, in the enterprise context. Indeed, the government itself recognizes that different concerns apply in the enterprise context. *See DOJ Guidelines*, n.2, *supra*. IBM respectfully submits this *amicus curiae* brief to emphasize the need for caution and concern for the enterprise context when fashioning a rule for this case involving an individual's data.

SUMMARY OF ARGUMENT

The Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §2510 *et seq*., and the Stored Communications Act (SCA), 18 U.S.C. §§2701-2712, are, almost uniformly, considered to be outdated and in dire need of a congressional update. Until Congress acts, however, the text of the statute as written is the text that governs. Critically, Section 2703(a) of the SCA—the provision detailing the process that the U.S. government must follow to obtain the contents of electronic data, including an enterprise's cloud data—pertains to "warrants," not "subpoenas." The Court of

Appeals for the Second Circuit correctly recognized this textual difference and paid due respect to Congress' deliberate choice of words. And the distinction is an important one: Warrants are inherently territorial and cannot be used to effect a Fourth Amendment "search" of premises, including of cloud data storage facilities, located outside the United States.

Moreover, the possibility that the final act of "disclosing" the requested cloud data and information (i.e., physically handing over the data to government authorities) might occur in the United States does not excise the substantial *non*domestic conduct that necessarily precedes that final act. Before turning over data to the government on U.S. soil, a cloud services provider first must access the data *abroad*, collect the data *abroad*, and transfer the data to the United States from *abroad*. Execution of a Section 2703(a) warrant, therefore, imposes substantial extraterritorial obligations and does not merely involve the *domestic* application of Section 2703.

IBM urges the Court to recognize that while this case involves an individual cloud user, the Court's decision may well have a significant impact on enterprises, even though individuals and enterprises are frequently situated differently vis-à-vis their respective service providers. Whereas individuals do not typically control how or where their cloud data are maintained by a services provider, enterprises frequently contract for a menu of specific conditions relating to data storage and maintenance, including the data's physical location. The differences are even more pronounced in the context of non-U.S.

enterprises (and U.S.-based enterprises operating abroad), which are subject to a host of foreign laws with which they must comply and that may conflict with U.S. law.

The government has ample tools at its disposal, aside from the SCA, to obtain the same data that it seeks here. While many of these tools, such as mutual legal assistance treaties (MLATs), may be imperfect and also in need of a refresh from Congress, they are not unworkable. And while IBM acknowledges the need to update the SCA to reflect contemporary technological developments, such as the cloud, that is a problem for Congress, not this Court, to rectify.

The judgment of the Second Circuit should be affirmed.

ARGUMENT

I. The SCA Does Not Apply Extraterritorially.

A. Section 2703(a) Concerns Warrants, Not Subpoenas.

Congress employed the term "warrant"—not "subpoena"—to describe the necessary process for obtaining stored electronic communications under Section 2703(a) of the SCA. *See* 18 U.S.C. §2703(a) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a *warrant* issued using the procedures described in the Federal Rules of Criminal Procedure." (emphasis added)). By contrast, in the two subsections immediately after Section 2703(a), Congress described

three types of "subpoenas"—administrative subpoenas, grand jury subpoenas, and trial subpoenas—as the necessary process for law enforcement to obtain other types of communications under the SCA. *Id.* §2703(b), (c). In yet another subsection of Section 2703, Congress used "warrant" and "subpoena" side-by-side as disjunctive alternatives to one another. *See id.* §2703(e) ("No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, *warrant, subpoena*, statutory authorization, or certification under this chapter." (emphasis added)).

Congress' difference in word choice throughout adjacent and proximate subsections of Section 2703 is significant, and presumably was intended to impute different meanings to the different words. After all, "Congress' choice of words is presumed to be deliberate." *Univ. of Tex. Sw. Med. Ctr. v. Nassar*, 133 S. Ct. 2517, 2529 (2013). And where Congress "has chosen different language in proximate subsections of the same statute, courts are obligated to give that choice effect." *United States v. Barial*, 31 F.3d 216, 218 (4th Cir. 1994); *see also Russello v. United States*, 464 U.S. 16, 23 (1983). Moreover, "when Congress employs a term of art"—such as "warrant"—"it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken." *FAA v. Cooper*, 566 U.S. 284, 292 (2012) (quoting *Molzof v. United States*, 502 U.S. 301, 307 (1992))). Lower courts have recognized this distinction in the specific context of the

warrant–subpoena dichotomy. *See 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 and we find that Congress intended them to be treated as warrants.").

The Court of Appeals below correctly recognized this distinction and accorded Congress' word choice the weight to which it is entitled. *See In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 214 (2d Cir. 2016) ("*Microsoft*") ("Warrants and subpoenas are, and have long been, distinct legal instruments. … The term 'subpoena,' therefore, stands separately in the statute, as in ordinary usage, from the term 'warrant.' We see no reasonable basis in the statute from which to infer that Congress used 'warrant' to mean 'subpoena.'" (footnote omitted)).

By contrast, the government's novel subpoena-in-practice view of Section 2703(a) warrants, *see* Pet.Br.15, would neuter such warrants of all but one facet of a traditional warrant. According to the government, the only trace of a traditional warrant that remains in a Section 2703(a) "*warrant*" is the requisite level of suspicion. *See id.* at 39. Congress distinct word choice, however, implies otherwise, as the Court of Appeals below properly recognized. *See Microsoft*, 829 F.3d at 214 ("Section 2703 does not use the terms [warrant and subpoena] interchangeably. Nor does it use the word 'hybrid' to describe an SCA warrant." (citation omitted)).

B. The "Disclosure" of Cloud Data Stored Abroad Involves More Than "Domestic Application" of the SCA.

Warrants, including those under Section 2703(a), have long been understood to apply domestically only. *See Microsoft*, 829 F.3d at 212-13; *cf. Sekhar v. United States*, 133 S. Ct. 2720, 2724 (2013) ("[I]f a word is obviously transplanted from another legal source, whether the common law or other legislation, it brings the old soil with it."). Section 2703(a)'s reference to the Federal Rules of Criminal Procedure reinforces the territorial nature of Section 2703(a) warrants, as the Rules authorize a magistrate judge "to issue a warrant to search for and seize a person or property *located within the district*." Fed. R. Crim. P. 41(b)(1) (emphasis added). Moreover, no provision in the SCA rebuts 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 Austrl. Bank Ltd.*, 561 U.S. 247, 255 (2010). The government concedes this point. *See* Pet.Br.16 ("Microsoft is correct that the presumption against extraterritoriality applies to Section 2703 and is unrebutted[.]"). Thus, whether a Section 2703(a) warrant may reach extraterritorial conduct turns solely on the question whether the government's request for cloud data "involves a domestic application of" the SCA. *See RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2101 (2016).

The answer is emphatically "no," as demonstrated by walking through the necessary steps for the government to obtain data stored in a cloud server

abroad. There does not appear to be any disagreement that cloud data stored abroad, while potentially *accessible* from anywhere in the world that has an Internet connection, are physically *stored* in a non-U.S. location. *See* Brief for *Amici Curiae* Computer and Data Science Experts at 11, *Microsoft*, No. 14-2985 (2d Cir. Dec. 15, 2014) ("Data has an identifiable physical location—'the cloud' relates to remote data access, not a new way to store data."), http://bit.ly/2rfkbk; *id.* at 16 ("Although data such as emails are more easily accessed by authorized parties, they still need to be stored on physical storage media[.]"); *see* Pet.Br.14, 27 (noting that Microsoft must "transfer" data "into or out of" a country). But that is where the agreement ends.

The government asserts that there is no Fourth Amendment "search" of a user's cloud data—and therefore no traditional warrant is required—because law enforcement officers do not "physically enter private premises" to execute a Section 2703 warrant. Pet.Br.14-15; *see also id.* at 35 ("Section 2703 … does not expressly authorize law enforcement officers to enter private premises against the wishes of a provider"). But that approach ignores the necessary preliminary steps that must occur before any "disclosure" of data to the government. *See id.* at 13 ("The focus of Section 2703 is on domestic conduct: the disclosure of electronic records to the government in the United States."); *id.* at 28 ("[A]ny invasion of a user's privacy occurs only when Microsoft discloses the communications to a third party ….").

For a cloud service provider to have the ability to disclose data, it must first access that data, then

collect that data, and then transport that data. All of those steps indisputably occur (in whole or substantial part) *outside* of the United States. *See Microsoft*, 829 F.3d at 209 ("[N]o party disputes that the electronic data subject to this Warrant were in fact located in Ireland when the Warrant was served. None disputes that Microsoft would have to collect the data from Ireland to provide it to the government in the United States."). To access cloud data stored abroad, a U.S. cloud provider may be required to obtain authorization from the country, enterprise client, or non-U.S. subsidiary where the data are physically located due to infrastructure and security protocols, contractual obligations, and local data privacy laws. Any or all of these hurdles to access may put the gatekeeping entity in the awkward situation of being forced to choose between complying with a U.S. warrant or complying with local law, European law, or its contract with its client. And even once data are accessed and collected abroad, there still is the transport of that data *to* the United States—an inherently *non*domestic process required to carry out a Section 2703(a) warrant. This step, too, may cause friction with other sovereigns' laws that this Court seeks to avoid.[14] *See F. Hoffman-La Roche Ltd. v.*

[14] The EU directive on the protection of individuals with regard to the processing of personal data, for example, permits "transfer to a third country of personal data … only if … the third country in question ensures an adequate level of protection." Directive 95/46/EC, art. 25.1, 1995 O.J. (L 281) 38; *see also* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 Geo. L.J. 115, 117-18 (2017) (describing the so-called "transatlantic data war" based on the United States' and European Union's differing approaches to data privacy).

Empagran S.A., 542 U.S. 155, 164 (2004) ("[T]his Court ordinarily construes ambiguous statutes to avoid unreasonable interference with the sovereign authority of other nations.").

Under the government's theory, there is no Fourth Amendment "search" of cloud data because cloud services providers are not the entities actually "reviewing" the cloud data. *See* Pet.Br.31. But such a narrow view ignores the first half of the equation: The government could not obtain the cloud data to review if cloud services providers (for individuals and enterprises alike) were not accessing the data *abroad*, collecting the data *abroad*, and transporting it to the United States from *abroad*.

By analogy to a physical object that is the subject of a criminal investigation, under the government's view, the government could "compel" a cloud services provider, *see id.* at 12, 37, to go to Europe, enter a house (a cloud data storage facility), go into a bedroom (an enterprise client's data files), take from the bedroom a diary (the requested data), and return to the United States with the diary, and only *after* the diary is presented to the government in the United States would there be a search. *See id.* at 26 ("[T]he relevant invasion of privacy occurs in the United States, when Microsoft discloses the information to the government and the government reviews the information."). The government's refusal to acknowledge the substantial extraterritorial measures necessary to produce the diary in a domestic courtroom blinks reality and hardly makes such an international search a purely "domestic" application of the SCA. *See RJR Nabisco, Inc.*, 136 S. Ct. at 2101.

II. The Third-Party Doctrine Does Not Apply To Enterprise Client Relationships.

Absent a lawful warrant—which the government cannot obtain for cloud data stored outside the United States—the government's ability to access an enterprise's cloud data should not be governed by the traditional third-party doctrine, under which there is no reasonable expectation of Fourth Amendment privacy in information revealed to a third party. *See United States v. Miller*, 425 U.S. 435, 442-43 (1976); *see also Smith v. Maryland*, 442 U.S. 735, 744 (1979) ("When … petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the normal course of business … [he] assumed the risk that the company would reveal to the police the numbers he dialed.").

Society's expectations of privacy evolve and depend in part on the information shared. The Internet revolution and advent of cloud computing and cloud data storage have dramatically affected those expectations. *See* Steven M. Bellovin, et al., *It's Too Complicated: How the Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1, 2-11 (2016). Merely because data generated by an enterprise are stored in the cloud by a service provider does not diminish any expectation by the enterprise of privacy in its data. As the Court of Appeals for the Sixth Circuit aptly recognized, "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy." *United States v. Warshak*, 631 F.3d 266, 286-87 (6th Cir. 2010). And as Justice Sotomayor similarly

acknowledged, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *This approach is ill suited to the digital age*, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (emphasis added) (citation omitted); *cf. Riley v. California*, 134 S. Ct. 2473, 2493 (2014) (warrants are generally required before police may search a cell phone).

The third-party doctrine is particularly ill-suited in the context of an enterprise's cloud data, because enterprise clients own and maintain control over their cloud data.

A. An Enterprise's Cloud Data Belong to the Enterprise, Not the Cloud Services Provider.

An important focus of the third-party doctrine is on who owns the subject of the search at issue (here, data stored in the cloud). Critically, SCA warrants do not seek documents belonging to cloud service providers; rather, they seek documents for which the providers are mere "caretakers" on behalf of the owners, which are the enterprise clients. While cloud service companies may perform periodic maintenance on their servers, may provide various services, and host the cloud data, they typically have no legal ownership interest in the substance and contents of client data stored on their systems.

This arrangement is as intentional as it essential, as both the risks and consequences of a data breach

can be far greater for enterprises than for individual consumers. Whereas individuals primarily interact *socially* in the cloud, enterprises operate and compete *commercially* in the cloud, and enterprises' cloud data are often their lifeblood. That lifeblood is subject to a host of threats, including industrial espionage and hacking. The instances are plentiful. For example, last November, the Department of Justice charged three Chinese nationals with "conspir[ing] to hack into private corporate entities in order to maintain unauthorized access to, and steal sensitive internal documents and communications from, those entities' computers." Press Release, U.S. Dep't of Justice, U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage (Nov. 27, 2017), http://bit.ly/2BiQXBv. The costs associated with these hacks are significant. Accordingly, to ensure the highest level of protection, enterprise agreements reinforce that the enterprises retain ownership of their data, including, if appropriate, the ability to encrypt their data or otherwise restrict access with keys that only the enterprise controls. *See DOJ Guidelines* 2 ("Moreover, a provider will not always have access to all possible data. For example, the enterprise might encrypt data on its own systems before transmitting to their cloud provider.").

A recipient of a lawful subpoena generally must turn over his *own* records responsive to the subpoena. But that rule has limited (if any) application to enterprise data stored in the cloud, because cloud storage providers do not own enterprise clients' cloud data. Consistent with that notion, IBM has announced unequivocally that "such information

belongs to our clients." Weber, n.11, *supra* (emphasis added); *compare* Pet.Br.29 ("By contrast, where a private actor merely gathers information stored in its *own* files, it does not function as a government agent." (emphasis added)).

B. Enterprise Clients, Not Cloud Service Providers, Can Control Where Their Data Are Physically Located.

Not only do enterprise clients own their cloud data, they also generally maintain principal control over it (including its physical location). The government recently conceded as much. *See DOJ Guidelines* 2 ("While cloud services have changed the location of the servers storing enterprise data, in many cases *the enterprise maintains primary control over the data*." (emphasis added)). And notwithstanding a cloud service provider's right of *access* to a particular server (for example, to perform maintenance), more than access is necessary before a provider can be said to *control* an enterprise's data. *See Searock v. Stripling*, 736 F.2d 650, 653 (7th Cir. 1984) ("Control is defined not only as possession, but as the *legal right* to obtain the documents requested upon demand." (emphasis added)); *In re Grand Jury Subpoena*, 646 F.2d 963, 969 (5th Cir. 1981) ("That [an employee] had access to the records is irrelevant, for mere access is not possession, custody, or control.").

The government's arguments with respect to Microsoft's unilateral ability to dictate the location of an individual's cloud data therefore significantly cabin the outcome for which the government advocates. Accordingly, even if the government were to prevail, the Court should craft a narrow rule limited to the

particular facts of this case, which concern an individual with no control over where his or her data are physically stored—not an enterprise who may, and often does, contract *specifically* for data to be stored in a designated location.

Throughout its brief, the government emphasizes that Microsoft—not an e-mail account holder—is the unbridled decision-maker when it comes to where data are physically stored. *See, e.g.*, Pet.Br.27 ("Just as Microsoft was not restricted from migrating the specified account from the United States to Ireland in the first instance, it is not restricted from migrating the account back to the United States. It does not need authorization to do so[.]" (citation omitted)); *id.* at 31 ("Microsoft does not offend any reasonable expectation of privacy when it transfers material from a server in Dublin to its domestic offices—a transfer that Microsoft is free to perform at any time in the conduct of its business."). In the case of enterprise clients, however, that framework gets turned on its head, as enterprise clients may, and often do, determine where their data are stored, and can contract to have their cloud data stored on a server *not* in the United States. *See* Sebastian Krause, *IBM Gives Clients Control of their data in Europe with cloud, underscoring data responsibility*, IBM.com (Nov. 8, 2017), https://ibm.co/2ArS4PF. Thus, in contrast to Microsoft and the facts of this case, cloud services providers generally do not "decide" to store an enterprise client's cloud data wherever they choose, let alone decide "at any given moment." *See* Pet.Br.28.

To apply the third-party doctrine to data stored outside of the United States, which an enterprise

deliberately chooses to store outside the United States, and to which the enterprise and local (non-U.S. subsidiary) cloud services provider contractually agree, would disrupt the contractual relationships between the enterprise clients and cloud providers (which are typically more protective of the client than similar contractual relationships between individual consumers and cloud services providers). That level of protection, is due, at least in part, because of an enterprise client's separate legal obligation to protect its data and its customers' data.

Cloud providers serving clients that handle personal data of Europeans, if not already under a legal obligation to protect such clients' data, soon will be. The European Union General Data Protection Regulation (GDPR), set to take effect on May 25, 2018, introduces such legal obligations for cloud services providers. For example, Article 6.1(b) of the GDPR contemplates contractual agreements as a basis for processing cloud data, and provides that "[p]rocessing shall be lawful *only if* and to the extent that," among other reasons, "processing is *necessary* for the performance of a contract." Regulation (EU) 2016/679 2016 O.J. (L 119) 59 (emphases added). Presumably, processing cloud data to comply with a foreign government's search warrant would not be "necessary for the performance of a contract."[15] Similarly, Article 7(b) provides that consent for performance of a contract is invalid if "performance of a contract … is

---

[15] Indeed, IBM has assured its enterprise clients that it "will take appropriate steps to challenge [a U.S. government order to obtain client data stored outside the United States] through judicial action or other means." Weber, n.11, *supra.*

conditional to the processing of personal data that is not necessary for the performance of that contract." In other words, cloud service providers cannot condition a contract on extra-contractual processing, such as acquiescence to a Section 2703(a) warrant.

* * *

The government misses the mark, at least with respect to enterprise clients, by pinning the outcome of this case on the notion that cloud data are "within th[e] provider's control." Pet.Br.I. Not only is that not the relevant inquiry, but the nature of enterprise relationships typically places control securely in the hands of clients—not the (local non-U.S.) provider.[16] By limiting its arguments to a scenario where cloud data are purportedly within providers' control (such as with individuals' email accounts), *see id.* at 32-41, the government impliedly acknowledges that enterprise

---

[16] The third-party doctrine is perhaps even less justifiable in the context of enterprise cloud services providers. In the consumer cloud context, the government arguably has only two targets when seeking information: the cloud provider and the targeted individual. In the enterprise cloud context, however, the government also can look to the organizational entity using the service, if, for example, the targeted individual is an employee or customer of that entity. For example, if the government is investigating an individual who uses a bank that is an enterprise client, and keeps bank statements in the service provider's cloud, the government can seek this information from the bank, not the service provider. *See DOJ Guidelines* 2 ("[P]rosecutors should seek data directly from the enterprise, if practical, and if doing so will not compromise the investigation. Therefore, before seeking data from a provider, the prosecutor, working with agents, should determine whether the enterprise or the provider is the better source for the data being sought.").

arrangements, where companies maintain control over their data, are distinct.

III. There Are Alternative Legal Methods For Obtaining Cloud Data Stored Abroad And For Altering The Statutory Landscape.

IBM acknowledges the need for robust law enforcement tools when investigating crimes, and terrorism in particular, with a multinational dimension. But the U.S. government already possesses such tools, counseling against an unnatural overreading of the SCA. Moreover, the government's criticisms about the SCA are best addressed in the chambers of Congress, not in this Court.

A. The Government Has Tools at Its Disposal to Obtain Cloud Data Stored Abroad.

The U.S. government has several arrows in its quiver that would allow it to obtain the cloud data it seeks from Microsoft, and that were designed for this very situation.

First, the government can rely on mutual legal assistance treaties (MLATs), which are bilateral and multilateral treaties to assist law enforcement and facilitate the exchange of information in furtherance of criminal investigations. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 393-94 (2015). Although the United States is not a party to an MLAT with every foreign sovereign, the United States has entered into MLATs with more than fifty countries (including the Republic of Ireland). *See* Mutual Legal Assistance Treaties, MLAT Index, http://bit.ly/2EMVrBQ (last visited Jan. 18, 2018).

While the government characterizes the MLAT process as "slow and uncertain," Pet.Br.44-45, many MLATs include specific provisions that provide for treatment of "urgent cases," *see, e.g.*, MLAT, U.S.-Gr. Brit.-N. Ir., art. 4, §1, http://bit.ly/2FGnCE1, and for making and responding to requests via "expedited means of communication," *see* MLAT, U.S.-EU, art. 7, http://bit.ly/2rcOIzc. IBM recognizes that the MLAT process is not perfect, and the U.S. government is not alone in its frustration with respect to the length of time involved for completing the MLAT process. Indeed, other countries have expressed frustration with the *United States'* "[d]elays and difficulties in obtaining evidentiary records through the MLAT process." Press Release, U.S. Dep't of Justice, Attorney General Holder Announces President Obama's Budget Proposes $173 Million for Criminal Justice Reform (Mar. 4, 2014), http://bit.ly/2rcOLLo. But imperfections in an agreed-to process—which includes provisions that ensure compliance with foreign law[17]—do not justify the government's refusal to honor its commitment to other countries, especially when the MLAT process is subject to mutually agreed-upon revisions.

In any event, however, the government did not even attempt to use the MLAT process to obtain the email communications at issue in this case, and thus

---

[17] *See, e.g.*, MLAT, U.S.-Gr. Brit.-N. Ir., art. 14, §1 ("The Requested Party shall execute a request for the search, seizure and delivery of any article to the Requesting Party if the request includes the information justifying such action under the laws of the Requested Party and it is carried out in accordance with the laws of that Party.").

cannot complain that the process would have been ineffective. To the contrary, the Republic of Ireland (where the requested email communications are located on Microsoft's cloud server) submitted *amicus curiae* briefs both in the Court of Appeals below and this Court stating in no uncertain terms that "Ireland remains ready to consider, *as expeditiously as possible*, a request under that Treaty, if and when it be made." Brief for A*micus Curiae* Ireland, at 3 (emphasis added).

The United States also is a party to the Convention on Cybercrime (also known as the Budapest Convention), which specifically addresses mutual legal assistance in preserving and obtaining access to electronic data. *See* Kristen Eichensehr, *Data Extraterritoriality*, 95 Tex. L. Rev. *See Also* 145, 157-58 (2017). And similar to many MLATs to which the United States is a party, the Convention on Cybercrime recognizes that timely cooperation is an important factor in the fight against crime. Specifically, Article 35 of the Convention provides that "[e]ach Party shall designate a point of contact *available on* a *twenty-four hour, seven-day-week basis, in order to ensure the provision of immediate assistance* for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence." Council of Europe, Convention on Cybercrime, art. 35 (Nov. 23, 2001) (emphasis added), http://bit.ly/2B7JQv5.

Further, while certain exigent situations may call for lawfully authorized exceptions to current laws in

the interest of obtaining information as promptly as possible, the government has not argued that the data requested here are of that unique nature. Nor need there be a rigid framework that never takes into account the gravity of a particular situation. The European Union, through the soon-to-be-implemented GDPR, has acknowledged as much. The GDPR recognizes that its Member States would provide access to cloud data under exceptional circumstances relating to national security, such as terrorism. Recital 16 of the GDPR provides: "This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, *such as activities concerning national security*." 2016 O.J. (L 119) 59 (emphasis added).

B. The Government Is In The Wrong Forum.

Given the prevalence of multinational companies operating worldwide, the increasingly complex patchwork of data privacy laws—especially outdated ones—has made the legal landscape particularly thorny. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 416-417 (2014). It is for Congress to craft a solution to find a way out of the thicket, not the Court. In fact, after the Court of Appeals issued its decision below, and before the government petitioned for certiorari, the government requested that Congress update the SCA in view of the ruling below. Br. in Opp.1 n.1.

If the government is to obtain the relief that it seeks, it must do so through proposed legislation—such as the pending Law Enforcement Access to Data

Stored Abroad Act ("LEADS Act")—not by asking the Court to interpret the SCA in a way that contravenes the canons of statutory construction, shoehorns an outdated law into existing technology, and disrupts international comity. The LEADS Act, for example, is intended to "safeguard data stored abroad from improper government access," LEADS Act, S. 2871, 113th Cong. (2014), and, under its most recent proposal, would "authorize[ ] the use of search warrants extraterritorially only where the Government seeks to obtain the contents of electronic communications belonging to a United States person," *id.* §2(4).

It is Congress' job to weigh the countervailing interests at play between private parties' interest in protecting their information, on the one hand, and the government's need to access data in furtherance of law enforcement, on the other. Congress appears to have recognized the need to balance these interests and address these issues in an updated statutory framework, but has yet to act. *See id.* §§2(3), 2(4) (recognizing that "courts in the United States lack the power to issue warrants authorizing extraterritorial searches and seizures," but "also recogniz[ing] the legitimate needs of law enforcement agencies in the United States to obtain, though lawful process, electronic communications relevant to criminal investigations related to United States persons wherever that content may be stored"). But it is not the Court's job to step in and do Congress' job for it. *See* U.S. Const. art. I, §1 (vesting "*All* legislative Powers" in Congress (emphasis added)). Congress can address the particular concerns, needs, and technologies of different types of cloud providers,

whether consumer- or enterprise-facing. By contrast, it is this Court's job to apply the statute as written. *See Lewis v. City of Chi.*, 560 U.S. 205, 217 (2010) ("Our charge is to give effect to the law Congress enacted.").

IBM has supported, and will continue to support, efforts to arrive at an appropriate legislative solution that recognizes the competing interests and the modern, global technological era, and it stands ready to do so with respect to the important interests implicated in this case. *See* Weber, n.11, *supra* ("IBM is committed to being a responsible participant in th[e] discussion [about government access to data] and a strong advocate for our clients.").

CONCLUSION

For the foregoing reasons, this Court should affirm the judgment of the Second Circuit.

Respectfully submitted,

MICHELLE H. BROWDY
DANIELA COMBE
ANDREW H. TANNENBAUM
GEORGE KOTLARZ
IBM CORPORATION
One North Castle Drive
Armonk, NY 10504
(914) 765-4343

PAUL D. CLEMENT
Counsel of Record
GEORGE W. HICKS, JR.
DAMON C. ANDREWS
KIRKLAND & ELLIS LLP
655 Fifteenth Street, NW
Washington, DC 20005
(202) 879-5000
paul.clement@kirkland.com

Counsel for Amicus Curiae

January 18, 2018