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 OF 12 BUSINESS AND CONSUMER ASSOCIATIONS AS *AMICI CURIAE* IN SUPPORT OF RESPONDENT

ANDREW J. PINCUS
Counsel of Record
PAUL W. HUGHES
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF CONTENTS—continued

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES—continued

Page(s)

Statutes, Rules, and Regulations

TABLE OF AUTHORITIES—continued

Page(s)

Other Authorities

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

TABLE OF AUTHORITIES—continued

Page(s)

INTEREST OF *AMICI CURIAE*

Amici curiae are 12 associations representing the interests of businesses and individuals. They are united in the view that permitting U.S. law enforcement authorities to use a warrant to reach outside the United States and seize electronic information stored in another country—without complying with the legal requirements of the nation in which the information is stored—will eviscerate trust in cloud services providers, hamper U.S. companies' ability to compete in that market, and diminish critical privacy protections by opening the door to demands by other nations that highly confidential information belonging to U.S. individuals and companies stored in the United States be turned over to those governments without compliance with U.S. legal requirements.[1]

BSA | The Software Alliance is an association of the world's leading software and hardware technology companies. On behalf of its members, BSA promotes policies that foster innovation, growth, and a competitive marketplace for commercial software and related technologies.

The Center for Democracy & Technology (CDT) is a non-profit, public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitu-

---

[1] Pursuant to Rule 37.6, *amici* affirm that no counsel for a party authored this brief in whole or in part and that no person other than *amici*, their members, or their counsel made a monetary contribution to its preparation or submission. All parties have filed blanket consents to the filing of *amicus curiae* briefs.

tional and democratic values of free expression, privacy, and individual liberty.

The Chamber of Commerce of the United States of America is the world's largest business federation, representing 300,000 direct members and indirectly representing an underlying membership of more than three million U.S. businesses and professional organizations of every size and in every economic sector and geographic region of the country.

The National Association of Manufacturers (NAM) is the largest manufacturing association in the United States, representing small and large manufacturers in every industrial sector and in all 50 states. The NAM is the voice of the manufacturing community and the leading advocate for a policy agenda that helps manufacturers compete in the global economy and create jobs across the United States.

New America's Open Technology Institute (OTI) is New America's program dedicated to ensuring that all communities have equitable access to digital technology and its benefits, promoting universal access to communications technologies that are both open and secure. New America is a Washington, DC-based think tank and civic enterprise committed to renewing American politics, prosperity, and purpose in the Digital Age. OTI works to ensure that government access to electronic communications is subject to robust safeguards for cybersecurity and individual privacy.

ACT | The App Association is an international grassroots advocacy and education organization representing more than 5,000 small and mid-size app developers and information technology firms. ACT

advocates for an environment that inspires and rewards innovation while providing resources to help its members leverage their intellectual assets to raise capital, create jobs, and continue innovating.

Americans for Tax Reform (ATR) is a nonprofit organization that represents the interests of the American taxpayers at the federal, state, and local levels. Through its Digital Liberty project, ATR advocates on policies and proceedings relating to technology, telecommunications, privacy, and competition that affect taxpayers.

The Entertainment Software Association represents companies that publish computer and video games for video game consoles, handheld devices, personal computers and the Internet. Because its members are leading global innovators on the creation and delivery of interactive content, its advocacy focuses on intellectual property, technology, privacy, trade, immigration, and First Amendment protections.

FreedomWorks Foundation is a 501(c)(3) nonprofit and educational foundation dedicated to building, educating, and mobilizing the largest network of activists advocating the principles of smaller government, lower taxes, free markets, personal liberty, and rule of law.

The Information Technology and Innovation Foundation (ITIF) is an independent non-profit, nonpartisan think tank whose mission is to formulate, evaluate, and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress. ITIF's goal is to provide policymakers around the world with high-quality in-

formation, analysis, and recommendations they can trust.

National Taxpayers Union (NTU) is a nonpartisan citizen group founded in 1969 to work for simpler, less burdensome taxes, taxpayers' rights, limited government expenditures, prudent regulations, and economic liberty. NTU has advocated for numerous reforms to the administration of tax laws, including more clearly defined boundaries on government access to taxpayers' financial information. The organization has also encouraged robust entrepreneurial development of cloud-based information technology solutions in the private sector because of their "spillover potential" to help make public sector programs more nimble at managing information and delivering services in a cost-efficient manner.

Small Business & Entrepreneurship Council is a non-profit advocacy and education organization that works to protect small business and promote entrepreneurship. For nearly 25 years, the organization has worked to successfully advance a range of policies and initiatives to strengthen the ecosystem for startup activity and business growth.

INTRODUCTION AND SUMMARY OF ARGUMENT

The U.S. government is wrong in asserting that a warrant issued under 18 U.S.C. § 2703(a) may compel a person or entity within the United States to search and copy electronic data stored in another country, transmit the copy of the data to the United States, and deliver it to the government.

First, the government's position—if adopted by this Court—will significantly deter the use of remote data management technologies by businesses and

individuals, particularly their use of U.S. cloud services providers. That would undermine a significant contributor to U.S. economic growth.

The data that companies and individuals store with cloud services providers includes the most confidential information about their business operations and personal lives, respectively. If the price of using these services is losing the protections of the laws of the country in which the information is stored and permitting access by the U.S. government to information that it otherwise could obtain only by invoking the processes of the country in which the data is located, then businesses and individuals will be reluctant to store their information "in the cloud." That means that the benefits of cloud computing—cheaper and more flexible data services, enhanced security, and reduced equipment costs—will not be realized, and the adverse consequences for the U.S. economy will be substantial.

Beyond that, the government's position would subject cloud computing providers to conflicting legal obligations. While a company would be required under U.S. law to export data from foreign nations and produce it to U.S. authorities, that same conduct will often violate foreign law. In particular, the European Union's General Data Protection Regulation Article 48 specifically forbids export of electronic data from Europe, absent authorization through the legal processes of the country in which the data is stored. The canon against interpreting U.S. statutes to have extraterritorial application is designed to preclude just such collisions between national laws.

The government's position, moreover, would encourage some foreign nations to employ similarly intrusive warrants. Those nations will target electronic

data belonging to U.S. individuals and businesses that is stored in the United States. If the U.S. government can use U.S. process unilaterally to require the disclosure of data stored in Ireland, then the Russian government can invoke that precedent to assert that Russian process can require the disclosure of data stored in the United States. The dangers to American privacy, security, and sovereignty are obvious.

Second, there is no basis in law for the extraordinary result urged by the United States. Affording extraterritorial reach to U.S. warrants violates fundamental principles of international comity and the plain language of 18 U.S.C. § 2703(a). The statute offers no indication that it applies extraterritorially, but the government's interpretation results in an obvious extraterritorial impact: empowering the U.S. government to require companies to reach into a foreign nation and retrieve data stored there without complying with the legal requirements of the nation in which the data is stored.

Indeed, it is elementary that the United States government cannot serve a search warrant on the U.S. headquarters of an international hotel company, demanding that the company deliver to the government photocopies of papers in a room in its hotel in Zurich without obtaining the assistance of Swiss courts. There is no basis to conclude that Congress intended a different result in the context of digital data.

Third, the statute at issue here was enacted in 1986—long before the advent of the modern Internet and cloud computing. Mutual Legal Assistance Treaties and international agreements provide for robust international law cooperation in obtaining access to

electronic information stored in other countries. To the extent that the United States maintains that this new technology demands new law enforcement tools, that is an argument properly addressed to Congress—not to this Court.

ARGUMENT

I. Permitting U.S. Law Enforcement To Use Warrants To Obtain Data Stored On Non-U.S. Servers Would Seriously Harm U.S. Economic And Security Interests.

A. Cloud computing produces substantial economic benefits for the U.S. economy.

Cloud computing has revolutionized the way individuals and businesses handle information in electronic form, allowing them to cheaply, easily, and safely store data on servers that can be accessed worldwide. U.S.-based companies have been at the forefront of this revolution.

1. "Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley* v. *California*, 134 S. Ct. 2473, 2491 (2014). These technologies permit the user to conduct a wide range of data storage or processing operations that until recently were performed on the user's desktop computer or local server. The physical hardware that performs those tasks is owned by the data services provider and accessed via the Internet; the information (email contents, contents of stored documents, etc.) remains the property of the user. Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, 16 J. Tech. L. & Pol'y 229, 232 (2011).

This revolution in computing is the result of dramatic reductions in the cost of storing digital data. In 1984—that is, two years prior to the Electronic Communication Privacy Act—it cost $85,000 to store a single gigabyte of data. Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 391 (2014). By 2011, that price had dropped to approximately five cents. *Ibid*. In 2016, it had fallen yet farther to two cents per gigabyte. Tom Coughlin, *The Costs of Storage*, Forbes (July 24, 2016), https://goo.gl/UXFZnE. Today, commercially available storage devices can hold "16 petabytes of data, roughly equal to 16 billion thick books." Quentin Hardy, *As a Data Deluge Grows, Companies Rethink Storage*, N.Y. Times (Mar. 14, 2016), https://goo.gl/HgB1Nc.

In *Riley*, the Court recognized that individuals now use electronic media to store virtually all of their personal information and records—"[t]he sum of an individual's private life." *Riley*, 134 S. Ct. at 2489-2490. The "immense storage capacity" of modern cell phones emphasized in *Riley* (*id.* at 2489) is dwarfed by the essentially limitless storage accessible through cloud computing. Individuals can store in the cloud *all* of their email messages, *all* of their photographs and videos, and *all* of their personal financial and health data. Thus, a government search of the information stored by an individual using cloud technology "would typically expose to the government far *more* than the most exhaustive search of a house"—not just "many sensitive records previously found in the home," but also "a broad array of private information never found in a home in any form." *Id.* at 2491.

Not only do cloud computing services provide immense storage capabilities for users, but they also provide new services never previously available. For example, the Xbox Live multiplayer gaming system—an online video game environment that serves tens of millions of customers—relies on cloud computing and remote data storage. Mario Aguilar, *How Xbox Live's Cloud Computing Could Make Games That Last Forever*, Gizmodo (Oct. 15, 2013), https://goo.gl/oFkyLr.

2. Businesses also increasingly rely on cloud computing to store a wide variety of essential business records. These include proprietary technology, financial data, intellectual property, business plans, manufacturing processes, acquisition plans and negotiating strategy, customer data, and privileged and confidential legal advice regarding pending lawsuits and other sensitive matters. Cloud computing is "one of the most significant technical advances for global business in this decade—as important as PCs were to the 1970s." Nancy J. King & V.T. Raja, *What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data*, 50 Am. Bus. L.J. 413, 418 (2013) (quotation omitted).

Cloud computing offers a number of advantages to businesses that use it.

First, "[r]ather than keeping and processing large amounts of data in-house, which is costly and inefficient," users can utilize cloud computing to "distribute that job efficiently among a global network of millions of computers, pooling and renting huge amounts of computing power for collective use." Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J.

Nat'l Security L. & Pol'y 247, 295 (2016). Customers can rapidly harness those servers' collective computing power when needed ("scaling up"), then rapidly release that power when the desired task is completed ("scaling down"). Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313, 325 (2013).

Second, cloud computing providers' greater scale enables them to direct vastly greater resources into protecting against hacks and other unlawful intrusions than could a business, university, or government attempting to manage its own computer systems in-house. Luke Graham, *Ransomware Can Cost Firms Over $700,000; Cloud Computing May Provide the Protection They Need*, CNBC (Aug. 4, 2017), https://goo.gl/TTMb7Q. Moreover, Internet-based computing provides businesses with disaster recovery services on a much more cost-efficient basis. See Lee Badger et al., Nat'l Inst. of Standards & Tech., U.S. Dep't of Commerce, *Cloud Computing Synopsis and Recommendations* § 5-4 (2012), https://goo.gl/-KNlaJM.

Third, allowing users to access their information from any location in the world that has Internet access also creates seamless data portability—the user can create a document on a home laptop, edit it on a tablet, review it on a desktop computer at work, then share it with colleagues around the world. See Elijah Yip & Martin E. Hsia, *Confidentiality in the Cloud: The Ethics of Using Cloud Services in the Practice of Law*, 31 Computer & Internet Law. 2 (2014), https://goo.gl/D7WqX3.

For these reasons, cloud computing services have become an essential part of the business ecosystem. The average company uses over a *thousand* distinct

cloud services. Ajmal Kohgadai, *12 Must-Know Statistics on Cloud Usage in the Enterprise*, Skyhigh, https://goo.gl/2RJkzc (last visited Jan. 18, 2017). Just a few examples: Apple's iCloud, Microsoft Office 365, Dropbox, Gmail, and WestlawNext are all commonly used cloud services. Moreover, the largest cloud hosting provider, Amazon Web Services, is used by companies like "Comcast, Novartis, Pfizer, Bristol-Myers Squibb, Dow Jones, and even government entities like the CDC, the FDA, and NASA." Wei Chen Lin, Comment, *Where Are Your Papers?: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud, and Encryption*, 65 DePaul L. Rev. 1093, 1115 (2016). Put simply, "[c]loud services now support nearly every aspect of daily life, from mobile banking and online commerce to high-tech manufacturing and the Internet of Things." Letter from Act | The App Association et al. to Senators Orrin Hatch & Chris Coons, at 1 (July 27, 2017), https://goo.gl/SygvVz.

The widespread use of cloud computing enables significant productivity savings. McKinsey estimates that by 2025 those savings will range between $500 and $700 billion annually. James Manyika et al., *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy*, McKinsey Glob. Inst., McKinsey & Co. 65 (May 2013), https://goo.gl/d2EX5h. Cloud computing could have a total annual economic impact of $1.7 to $6.2 trillion by 2025. *Id.* at 61.

The value added by cloud computing has driven the extraordinary growth of the market for cloud computing services. The worldwide public cloud services market is expected to grow 18% in 2017 to a staggering $246.8 billion. Louis Columbus, *Roundup*

of Cloud Computing Forecasts, 2017, Forbes (Apr. 29, 2017), https://goo.gl/emhgTV. Cloud computing is the fastest-growing segment of the information technology market by a long shot, growing by 4.5 times the rate of IT spending since 2009. *Ibid.*

In sum, "[c]loud computing has taken the technology industry by storm," and "[t]echnology providers that fail to compete and win in tomorrow's cloud computing market risk missing out on this important source of future growth." Mark Brinda & Michael Heric, *The Changing Faces of the Cloud*, Bain & Co. 1 (2017), https://goo.gl/dx1A4C.

3. The United States has long been the world leader in cloud computing technology and stands to reap the greatest benefits from its adoption. See Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. Pa. L. Rev. 1623, 1624 (2013).

"U.S. companies are very well-positioned to continue in leadership positions within the cloud computing market," with factors like "a very innovative and competitive domestic market, high levels of expertise and talent, name recognition and first-mover advantages" contributing to continued market dominance. Jorge Pardo et al., *2016 Top Markets Report – Cloud Computing*, U.S. Int'l Trade Admin. 7 (Apr. 2016), https://goo.gl/UHee97. As a result, the United States substantially exports these services, and cloud computing generated "a trade surplus of approximately $18 billion in 2015." *2017 Top Markets Report: Cloud Computing Sector Snapshot*, U.S. Int'l Trade Admin. 1 (2017), https://goo.gl/19t5Dn. "[L]eadership today, however, guarantees neither that U.S. cloud vendors will succeed in every global market they enter, nor that they will remain on top." Pardo et al., *supra*, at 7.

4. For cloud computing to operate effectively and efficiently, customers often must choose where, physically, their information is housed. Corporate customers may "decide for any number of reasons that they want to control the migration of data based on location," including "on the basis of governing regulation, due to customer contractual requirements, due to concern about foreign governments or because they have target certifications in mind for data centers." Ed Moyle, *Storing Data in the Cloud: Addressing Data Location Security Issues*, TechTarget (Aug. 6, 2013), https://goo.gl/51kBtK.

For these reasons, many prominent cloud services providers allow business and government customers to choose where their data will be exclusively stored. See, *e.g.*, *Data Privacy*, Amazon Web Servs., https://goo.gl/YR7818 (last visited Jan. 18, 2018); *Frequently Asked Questions*, Google Cloud Platform, https://goo.gl/0JfVEN (last visited Jan. 18, 2018); *IBM Cloud Object Storage: FAQ*, IBM, https://goo.gl/xVNj3S (last visited Jan. 18, 2018); *Where Your Data Is Located*, Microsoft, https://goo.gl/CEKQHm (last visited Jan. 17, 2018).

B. The government's expansive interpretation of Section 2703 would cause businesses and individuals to shun U.S. cloud services providers.

Permitting the U.S. government to use Section 2703 warrants to obtain records stored abroad—including records that have no realistic connection to the United States—will hamstring U.S. cloud computing businesses and decrease the use of cloud computing services worldwide. That result would harm American businesses and the American economy.

American consumers now "are more anxious about the security of their personal data and are more aware that greater and greater volumes of data are being collected about them." Lee Rainie & Shiva Maniam, *Americans Feel the Tensions Between Privacy and Security Concerns*, Pew Research Center (Feb. 19, 2016), https://goo.gl/zfetT5. Customers therefore shop for "companies who provide data security and withstand government surveillance." Margot E. Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DePaul L. Rev. 413, 435 (2017).

Foreign businesses and consumers contemplating the use of U.S.-based cloud computing providers have similar concerns. One survey showed that an "overwhelming number" of foreign companies "indicated that security and data privacy were their top concerns." Danielle Kehl et al., *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*, New Am.'s Open Tech. Inst. 8 (July 2014), https://goo.gl/VUuBJi. However, uncertainty about the U.S. legal framework governing the scope of U.S. warrants is "causing foreign governments, businesses, and individuals to question whether they can trust American products and technologies." Letter from Apple et al. to Senator Orrin Hatch et al. 1 (Aug. 1, 2017), https://goo.gl/eX3KY3. These "trust-related issues have increasingly caused hesitations amongst those considering purchasing of cloud services from U.S. vendors." Pardo et al., *supra*, at 7.

The government's position in this case has attracted the attention of foreign nations and consumers, who have signaled that they will not use U.S.-based providers if Section 2703(a) Stored Communications Act ("SCA") warrants can be used to obtain

data stored abroad. "Germany has been outright with its discontent with American data companies and has already refused to use Microsoft or any other U.S. data company for its data services, unless the SCA warrant is overturned." Ned Schultheis, Note, *Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry*, 9 Brook. J. Corp. Fin. & Com. L. 661, 688 (2015).

The use of such warrants will thus inevitably "undermine consumers' trust in the cloud and threaten the very foundation of the huge and growing cloud computing industry." Ashley Baker, *The Supreme Court Should Exercise Judicial Restraint in Microsoft Data Case*, The Hill (Oct. 22, 2017), https://goo.gl/KTH7SL.

Moreover, other nations are invoking privacy statutes, which were put in place to vindicate legitimate privacy rights, to advocate "data protectionism," designed to "keep foreign competitors out of domestic markets." Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, Info. Tech. & Innovation Found. (May 1, 2017), https://goo.gl/9xzTmL. European officials have asserted that they will launch a "massive information campaign" to inform consumers of their privacy rights under European law, noting that it has "become a factor in competition between companies." Lukáš Hendrych, *Jourová: I Will Launch a Massive Information Campaign on Data Protection*, Euractiv (May 5, 2017), https://goo.gl/b2XsBv.

In Europe specifically, there have been "calls for data localization requirements," which would require that data owned by a nation's individuals and companies be stored with local companies within the na-

tion's borders, "procurement preferences for European providers, and even a 'Schengen area for data'—a system that keeps as much data in Europe as possible." Daniel Castro & Alan McQuinn, *Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness*, Info. Tech. & Innovation Found. 4 (June 2015), https://goo.gl/bauuar. The government's interpretation of Section 2703(a) will fuel these efforts of other nations to promote their own companies at the expense of U.S.-based cloud providers.

The potential economic loss is staggering. That much is proven by the fallout from earlier disclosures about U.S. surveillance activities. "Since news reports emerged of the tech companies' involvement in U.S. government surveillance, estimates of losses in the U.S. cloud computing industry range from $21.5 billion to $180 billion." Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 Iowa L. Rev. 1441, 1481 (2015). More broadly, "[o]ne estimate of lost profits is in the billions of dollars for U.S. tech companies post-Snowden in the EU" alone. Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 Geo. L.J. 115, 166 (2017) (quotation omitted). Upholding the U.S. government's demands for copies of data stored abroad will injure U.S. competitiveness in the market.

And, as discussed above, many cloud computing providers have contracts with corporate and government customers that dictate where the customer's data will be stored. See pages 13-14, *supra*. Requiring cloud providers to transfer these customers' data to the United States may also force them to breach their contractual agreements.

In sum, this Court's approval of the government's attempt to use Section 2703 warrants to obtain data stored abroad would inflict very significant harm on U.S. companies and the cloud computing industry.

C. The government's position would impose conflicting legal obligations on cloud services providers.

In the government's view, a U.S. court could order any cloud provider within its jurisdiction to retrieve, copy, and produce in the United States data stored on servers outside the U.S. that are under the provider's control. But this position will inevitably impose conflicting legal requirements on cloud providers.

Other nations have enacted (and continue to enact) privacy laws that limit technology companies' ability to export locally-stored data. See Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. Nat'l Security L. & Pol'y 473, 477 (2016). Because those laws typically do not permit the export of data based on a U.S.-based search warrant, obligating cloud providers to comply with U.S. process in such circumstances would frequently create a conflict with foreign privacy laws. *Ibid.*

Starting in May 2018, the controlling data privacy regulation in Ireland will be the European Union's General Data Protection Regulation ("GDPR"). See Regulation (EU) 2016/479 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC

(General Data Protection Regulation), 2016 O.J. (L 119) 1.

The GDPR will permit cloud providers to export data from the EU only in specifically enumerated circumstances, and the existence of a foreign court order explicitly is not included. GDPR arts. 45-49.[2] Instead, Article 48 of the GDPR states that foreign court orders to export personal information from the EU can be recognized only "if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State." *Id.* at art. 48.

Similar to U.S. data protection laws that require the use of *domestic* U.S. legal process for the disclosure of stored data, Article 48 of the GDPR generally prevents cloud providers operating in Europe from complying with court orders like the one at issue here. Indeed, the GDPR explains that Article 48 targets the "judgments of courts * * * in third countries requiring" cloud providers "to transfer or disclose personal data * * * not based on an international agreement, such as a mutual legal assistance treaty." Recital 115, GDPR. Thus, cloud providers who comply with a U.S. court order to transfer data from Europe to the United States may violate the GDPR by

---

[2] See Art. 48 ("Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."). See also Art. 45-47, 49 (enumerating circumstances where data export is permitted).

doing so without the authority of an international agreement, such as the Mutual Legal Assistance Treaty that is in place between the United States and the EU. See Agreement on Mutual Legal Assistance Between the European Union and the United States of America, T.I.A.S. 10-201.1 (June 25, 2003).[3]

The GDPR imposes severe penalties for violations. In the past, national data protection authorities in Europe have routinely levied penalties against American technology companies for perceived data protection violations.[4] The GDPR implements far more draconian fines than previously available, empowering European regulators to extract up to 4% of an American technology company's total worldwide annual revenue for violations of the regulation.

---

[3] As the *amicus* brief filed by the European Commission in this case explains (at pages 15-16), a transfer of information pursuant to a U.S. warrant could be permissible under Article 49 of the GDPR. But that is a fact-specific determination, with Article 49's scope interpreted "strictly" (European Commission Am. Br. 16). Given Article 49's standards, the finding of a violation is likely for the sorts of disclosures most often required by U.S. warrants, such as a broad requirement to disclose to U.S. law enforcement officers all of the emails in a customer's account.

Moreover, the GDPR requires that the subject of personal information be notified if that information is transferred to a third country pursuant to Article 49. See GDPR, art. 15(2); *id*. art. 49(1) ("controller shall * * * inform the data subject of the transfer and on the compelling legitimate interests pursued"). That mandatory requirement conflicts with the confidentiality obligations imposed by U.S. law. See 18 U.S.C. §§ 2703, 2705.

[4] See, *e.g.*, Natasha Lomas, *Facebook Fined €1.2M for Privacy Violations in Spain*, TechCrunch (Sept. 11, 2017) https://goo.gl/csvgPC; Natasha Lomas, *Facebook Faces Fines Of $268K Per Day For Tracking Non-Users In Belgium*, TechCrunch (Nov. 11, 2015), https://goo.gl/LXXhFi.

GDPR art. 83(5). And it also authorizes private lawsuits. GDPR art. 82.

If the Court accepts the government's position that U.S. law enforcement can use Section 2703(a) warrants to force cloud providers to violate foreign privacy laws, such as the GDPR, the immediate consequence will be the imposition of conflicting legal requirements in some circumstances. A company in Microsoft's position may be left to choose between being held in contempt of a U.S. court—or being fined by the European Union of an amount up to 4% of its annual revenue.

The very purpose of the canon presuming that U.S. laws do not apply extraterritorially is to avoid just such conflicts. See pages 25-30, *infra*.

D. Endorsing the government's interpretation of Section 2703 will open the door to foreign nations' assertion of the same sweeping authority, undermining privacy and security of U.S. individuals and businesses.

The harms that the government's position would inflict are not merely economic. A ruling in favor of the government by this Court will lead foreign countries to adopt the same position—which would broaden the conflict in national laws and threaten the privacy and security of U.S. citizens and businesses.

Long before the European Union enacted GDPR Article 48, the United States adopted laws forbidding providers of stored communications systems from disclosing content data without *U.S.* legal process. See 18 U.S.C. § 2702(a). A foreign government's order does not excuse the provider from these obliga-

tions. Thus, pursuant to U.S. law, a foreign court may not compel a U.S. cloud computing provider present in the foreign country to disclose data stored on a U.S. server—the same principle embodied in the GDPR.

But a ruling by this Court in favor of the government here would encourage foreign governments to claim the same power. That is, "[t]he approach taken by the United States is likely to become a model for others." Daskal, 8 J. Nat'l Security L. & Pol'y at 474-475. That would seriously harm U.S. interests.

First, the assertion of this unilateral authority by other nations would place cloud providers in the impossible position of choosing between violating Section 2702(a) or a foreign government's orders.

This concern is not hypothetical. Brazil, for example, has long demanded that U.S. cloud providers operating there disclose communications stored in the United States. See Marco Civil (Law 12965/2014), art. 11, par. 2 (applying Brazilian law to Internet Service Providers operating abroad if they provide services to the Brazilian public).

When Microsoft recently refused such a request because compliance would violate Section 2702(a), the Brazilian authorities fined Microsoft and arrested one of its local executives on criminal charges. See *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests*: *Hearing Before the H. Comm. on the Judiciary*, 114th Cong. (Feb. 25, 2016) (Written Testimony of Brad Smith, President and Chief Legal Officer, Microsoft Corp.), https://goo.gl/8bp5sV (hereinafter *International Conflicts of Law*). Describing the situation in

recent Congressional testimony, Microsoft's Chief Legal Officer urged Congress to "[i]magine the kind of meeting that I have had to have with a Brazilian employee who is being prosecuted. And imagine trying to talk about the fact that we cannot, in fact, take the steps that would bring the prosecution to an end in Brazil, because it would require that we commit a felony in the United States." *Ibid.*

This incident in Brazil is hardly unique. For instance, a Belgian court recently rejected Skype's appeal of a fine imposed because Skype failed to comply with a court order to provide user messages. See Rachel Kaser, *A Belgian Court Fined Microsoft's Skype $36,000*, Bus. Insider (Nov. 16, 2017), https://goo.gl/R9NzLH. Before that, a Belgian court fined Yahoo! for failing to comply with a unilateral Belgian order to turn over emails stored in the United States. See Center for Democracy & Technology, *Yahoo! Protects User Privacy — and Gets Fined?* (July 11, 2009), https://goo.gl/26R7ge.

Second, the assertion of this authority by foreign governments—including those nations with interests adverse to our own—threatens the privacy and security of U.S. individuals and companies.

The adverse consequences of such intrusions into U.S. sovereignty are obvious. Foreign nations could seek, under the cloak of an official investigation, to compel disclosure of confidential business or technical information stored in the United States in order to give companies in the foreign nation a competitive advantage. Non-democratic governments could seek information stored in the United States about the political activities of individuals and advocacy organizations.

There are no limits to the kinds of U.S.-stored data that foreign nations could seek to compel cloud providers to disclose if the principle advocated by the government here—that bare jurisdiction over a cloud computing provider is enough to compel disclosure over information stored abroad—were accepted. The disastrous effects to privacy and security of U.S. individuals and businesses are apparent.

II. Section 2703(a) Warrants Cannot Compel Production Of Electronic Information Stored Outside The United States.

The court of appeals properly concluded that a warrant issued pursuant to Section 2703(a) cannot compel Microsoft—or any other cloud computing services provider—to transfer into the United States and disclose to the government information stored outside the United States. The focus of the Stored Communications Act is, as its name indicates, the location where the data is stored, not the place of compelled disclosure. A conclusion to the contrary would undermine the longstanding principle—and the practical reality of the international legal system—that search warrants have no extraterritorial reach. In addition, the government's invocation of a supposed, broad subpoena authority directly contradicts its position before this Court in another case this Term.

A. The Stored Communications Act focuses on the location where the data is stored, not the place of its disclosure.

The government acknowledges that "the presumption against extraterritoriality applies to Section 2703 and is unrebutted." U.S. Br. 16. The government nonetheless contends that the focus of Section 2703 is the place of "disclosure"—where the tar-

get of a warrant "turns over" the relevant "materials" to "law enforcement personnel." U.S. Br. 17. Because, in the context of this case, the actual turnover occurs in the United States, the government asserts that there is no impermissibly-extraterritorial application of the statute. *Ibid.*

But it makes no sense to divorce the concept of "disclosure" from *what* is being disclosed. Section 2703(a) is not a general disclosure statute or broad discovery tool. Instead, it focuses narrowly on "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." 18 U.S.C. § 2703(a). The focus of the statute is inextricably tied, therefore, to the "contents" of a "communication" in a particular form of "electronic storage." Applying this statute to the disclosure of communication "contents" stored *outside* the United States necessarily requires an extraterritorial application of the statute—and thus the canon against such an interpretation is properly invoked to bar such applications.

Indeed, the consequence of the government's interpretation would be a tremendous expansion of the U.S. government's power to compel production of information located outside the nation's borders. Describing that as anything other than an extraterritorial application of the statute cannot be squared with reality.

That conclusion is bolstered by Section 2703(a)'s requirement that the government obtain a warrant pursuant to the Federal Rules of Criminal Procedure. The statute expressly states that service providers can be compelled to disclose the contents of

communications "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." The relevant rule—Rule 41—is limited, with exceptions not relevant here, to property located within the United States (Fed. R. Crim. P. 41(b)),[5] and it expressly defines "property" to include "information" (*id.* 41(a)(2)(A)).

Moreover, if, as the government suggests, the focus of Section 2703(a) were disclosure alone, that interpretation would lead to the absurd result that the Act would not prevent disclosure outside the United States of electronic communications stored in the United States. Section 2702, for example, prohibits service providers from disclosing communications stored within the United States. If, as the government contends, the statute applies only to the location of disclosure, then the SCA would not bar U.S. providers from disclosing U.S. data, so long as the disclosures are made abroad. Such a construction would render the statute hollow. Rather, it is the location of the stored electronic information—*in the United States*—that is the basis of protection; the place of disclosure is irrelevant.

B. The traditional territorial limitation on searches confirms that the Act focuses on where data is stored.

The government's request in this case is no different than serving a warrant on the U.S. headquarters of an international hotel company and directing the company to photocopy papers contained in a

---

[5] A 2002 amendment permits issuance of warrants for property located outside the United States in terrorism-related investigations. *Id.* 41(b)(3).

room in the company's hotel in Zurich and send those photocopies to the United States. Of course such a warrant would be impermissibly extraterritorial. It makes no difference to that analysis whether the data seized is a physical letter in a hotel room or digital data held in a data center.

1. The canon against extraterritorial application of federal statute, absent a clear sign of intent from Congress, is rooted in comity. It "reflects the 'presumption that United States law governs domestically but does not rule the world.'" *Kiobel* v. *Royal Dutch Petroleum Co.*, 569 U.S. 108, 115 (2013) (quoting *Microsoft Corp.* v. *AT&T Corp.*, 550 U.S. 437, 454 (2007)). The doctrine rests on the premise that foreign and international laws properly govern certain conduct—and extending U.S. law in those circumstances would risk intolerable legal conflicts. It thus "serves to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries." *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2100 (2016). It "helps the potentially conflicting laws of different nations work together in harmony—a harmony particularly needed in today's highly interdependent commercial world." *F. Hoffmann-La Roche Ltd.* v. *Empagran S.A.*, 542 U.S. 155, 164-165 (2004).

For the presumption against extraterritorial application of U.S. laws to have meaning, it must preclude the application of a statute where foreign and international regimes impose conflicting obligations on the entities regulated. The government's myopic focus on the place of "disclosure" ignores the practical realities that the canon, rooted in international comity, is designed to address.

Indeed, through Articles 48 and 49 of the European Union's General Data Protection Regulation, the European Union has chosen to foreclose many of the data transfers the U.S. government seeks permission to compel. See pages 17-20, *supra*. The government's efforts to obtain such data, in the face of these prohibitions, creates the very sort of international strife that the canon cautioning against extraterritorial application is meant to avoid. See, *e.g.*, Council of Europe Commissioner for Human Rights, *The Rule of Law on the Internet and in the Wider Digital World* 15 (2014), https://goo.gl/G9iRWj (specifically referencing this case and stating: "A state that uses its legislative and enforcement powers to capture or otherwise exercise control over personal data that are not held on its physical territory but on the territory of another state * * * is exercising its jurisdiction extraterritorially" and may not do so "without the consent of the second state").

It is not surprising that foreign nations have legislated to protect the privacy of electronic information stored within their borders. These laws reflect the centuries-old principle that "warrants" have only domestic application. See, *e.g.*, *United States* v. *Verdugo-Urquidez*, 494 U.S. 259, 279 (1990) (Stevens, J., concurring in the judgment) ("American magistrates have no power to authorize" searches of non-citizens' homes in foreign jurisdictions); *United States* v. *Odeh*, 552 F.3d 157, 169-170 (2d Cir. 2008).

And there is no doubting that the government's construction of Section 2703(a) would cause conflict and controversy with foreign nations. This "potential for international controversy" plainly "militates against" extending the law abroad "without clear di-

rection from Congress." *RJR Nabisco*, 136 S. Ct. at 2107.

2. International agreements confirm that conclusion.

The U.S. government itself has recognized the need to respect the laws of other nations when it seeks evidence located within their borders. That is why the United States has entered into Mutual Legal Assistance Treaties (MLATs) providing means for obtaining another country's assistance in gaining access to data stored in that country—including evidence relevant to criminal and related matters. See, *e.g.,* Treaty Between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, T.I.A.S. 13137 (Jan. 18, 2001).

Even more significantly, the Convention on Cybercrime (2001), to which the United States is a party, confirms the international norm that a nation seeking information stored within another country's territory must obtain the assistance of that country in order to seize that information. The treaty commits parties, including the United States, to respect each other's laws and processes when seeking data across borders—establishing mechanisms for requesting the assistance of the country in which the servers containing the desired information are located.

It provides for general mutual assistance where there is no applicable international agreement (Article 27), specifically addresses assistance in preserving and obtaining access to stored data (Articles 29 and 31), and requires each signatory nation to designate a point of contact "available on a twenty-four

hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance" with regard to, among other things, "the preservation of data" and "the collection of evidence" (Article 35).

Particularly relevant in this case is the fact that the Convention on Cybercrime specifically does *not* authorize the use of domestic warrants to obtain electronic data stored extraterritorially. Article 32, which addresses "[t]rans-border access to stored computer data," states that one nation may obtain such data without the consent of the other nation only if the data is publicly available or the requesting nation "obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the [requesting nation] through that computer system." Public availability and voluntary consent were the only circumstances "in which all agreed that unilateral action [by the requesting nation] is permissible." *Explanatory Report to the Convention on Cybercrime* ¶ 293 (2001), https://goo.gl/9HxfkS.

The government seizes on Article 18.1(a) of this Convention, arguing it authorizes the sort of turnover ordered here. But that provision describes an order to a "person" to submit certain information within "that person's possession or control." Art. 18.1(a). Article 18.1(b), by contrast, applies to a "service provider," and it requires production of much more limited information: "a service provider offering its services in the territory of the Party" may be compelled to provide "subscriber information relating to such services in that service provider's possession or control." Article 18.3 defines "subscriber information" as information "other than traffic or content

data" that can be used to identify a subscriber's location or identity.

Article 18, accordingly, cannot be understood as authorizing countries to compel service providers to supply anything beyond "subscriber information" that it maintains outside the United States. Subscriber information is potentially analogous to third-party address data, and the provision makes clear that the underlying contents of the electronically stored data is not subject to production.

Indeed, the Council of Europe is considering adopting a protocol to the Convention that would expand its reach beyond subscriber information. See Council of Europe, *Cybercrime: Towards a Protocol on Evidence in the Cloud* (June 8, 2017), https://goo.gl/ji756p. See also *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era*: *Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 7 (2017) (statement of Richard W. Downing, Acting Deputy Assistant Attorney General) (acknowledging discussions regarding addition to Convention), https://goo.gl/X4WKwq [hereinafter *Data Stored Abroad*]. The fact that such a protocol is being considered confirms that the current Article 18 does not authorize countries to compel cross-border disclosure of anything other than subscriber information.

In sum, the international and foreign laws governing disclosure of the stored electronic communications at issue in this case provide strong confirmation that the government's interpretation of Section 2703(a) would have impermissible extraterritorial effect.

C. The government's analogy to subpoena authority is undermined by its position in *Carpenter*.

The government contends that Section 2703(a) must be construed in light of what it deems common law authority allowing subpoenas to reach business records a company maintains abroad. U.S. Br. 32-41. The linchpin of this argument is the government's assertion that stored electronic data—including the *content* of user emails—is a Microsoft business record and thus properly subject to the traditional subpoena power. *E.g.*, *id.* at 37. See also *id.* at 33 (describing subpoena authority to "requir[e] a company doing business in the United States to produce records," even if "the company must retrieve those records from outside the country").

This contention is directly contrary to the government's position in *Carpenter* v. *United States*, No. 16-402. There, the government contends that cell tower location data is a business record of the cell service provider and therefore unprotected by the Fourth Amendment. To narrow the scope of that position, the government in *Carpenter* expressly distinguished this material from email "contents," which, "like those of a sealed letter in the mail, may remain private." U.S. *Carpenter* Br. 12. The government argued that the business record is limited to "information conveyed to the provider" and does not include "information conveyed to others that the provider merely carries, transports, or stores." *Id.* at 36.

Having argued, correctly, in *Carpenter* that the contents of an email do not constitute business records of the service provider, the government cannot argue otherwise here. Moreover, that conclusion flows directly from the third-party doctrine, which

holds that only information conveyed to the transportation or storage provider (like addresses)—and not the contents of the communication itself—qualify as business records. See *Ex parte Jackson*, 96 U.S. 727, 733 (1878); *Walter* v. *United States*, 447 U.S. 649, 654 (1980).

III. The Government's Law Enforcement Concerns Do Not Justify Its Construction Of The Statute And Are Properly Addressed To Congress.

The government contends that its broad interpretation of Section 2703(a) furthers U.S. law enforcement interests. See U.S. Br. 44-45. But the government provides little evidence that MLATs and other forms of international cooperation are insufficient mechanisms for obtaining data stored abroad. While the government points to one MLAT request that apparently took two years (*ibid.*), MLATs have evolved to include expedited processing mechanisms. See, *e.g.,* Agreement on Mutual Legal Assistance Between the United States of America and the European Union, Article 4, § 7, T.I.A.S. 10-201.1 (June 25, 2003).

MLATs are also flexible, permitting the parties to assist each other through means other than those specified in the agreement. For example, the U.S.-Ireland MLAT at Articles 17 and 18 provides that a party may provide assistance "through the provisions of its national laws" and pursuant to "any bilateral arrangement, agreement, or practice which may be applicable" and "may also agree on such practical measures as may be necessary to facilitate the implementation of th[e] Treaty."

It is no surprise, therefore, that there are abundant examples of international legal cooperation working effectively and quickly during urgencies. For example, after the Charlie Hebdo attack, while the assailants were still at large, Microsoft responded to a proper FBI request within 45 minutes. *International Conflicts of Law*, *supra*.

But the Stored Communications Act—enacted in 1986, long before the advent of cloud computing or even broad use of the Internet—is anachronistic in a number of respects. The Act, for example, distinguishes between emails that are more or less than 180 days old, most likely because, in 1986, computer storage was much more expensive than it is today and providers usually did not hold email for more than six months. These older emails were treated as abandoned by the parties and akin to business records of the provider. *Ibid*.

That is not true today: email archives now function as a repository of the most sensitive forms of individual and corporate data. Many Americans, for example, maintain medical records, financial information, family photos, passwords, private correspondence, and a host of other sensitive information in their email archives. Businesses retain some of their most confidential records via email and cloud storage accounts. These systems are the modern-day locked filing cabinet and safe deposit box. Modernization of that Act, to recognize today's uses of modern technology, is essential.

In fact, the government itself acknowledges that the SCA is archaic. It has recognized "that some of the lines drawn by the SCA that may have made sense in the past have failed to keep up with the development of technology, and the ways in which indi-

viduals and companies use, and increasingly rely on, electronic and stored communications." Elana Tyrangiel, *Reforming the Electronic Communications Privacy Act*, U.S. Dep't of Justice 4 (Sept. 16, 2015), https://goo.gl/PCgu1x.

These shortcomings are not an invitation for this Court to legislate. The long-settled canon against giving federal statutes extraterritorial reach, absent a clear contrary indication from Congress, resolves this case. Whether the government should have the authority it requests is a question for Congress.

That is particularly true because the multiple, conflicting policy considerations implicated by that question are not appropriate for resolution by this Court. They have nothing to do with the extraterritoriality canon or other governing legal principles—unlike the conflict with other nations' laws, and intrusion into other nations' legitimate interests, resulting from the government's interpretation, which are just what the canon seeks to prevent.

Perhaps the nationality of an account holder—or the location of a suspected crime—should factor into the government's ability (or inability) to access electronic data stored abroad. Indeed, such limits are at issue in proposed bipartisan, bicameral legislation. See Press Release, Sen. Orrin Hatch, Hatch Urges Senators to Support International Communications Privacy Act (Aug. 1, 2017), https://goo.gl/DjDrKt.[6]

---

[6] The government points to the different ways in which companies other than respondent store data. See U.S. Br. 43-44. But those issues are not before the Court in this case, and they merely underscore the need for a legislative response, because Congress can develop a comprehensive approach that takes account of the different types of network architecture that may af-

Likewise, legislation may account for foreign laws. As Senator Hatch observed, "[e]xtending the reach of U.S. warrants without reasonable limits would * * * place service providers in the impossible position of having to choose which country's laws to violate—ours or the foreign jurisdiction's." *Ibid.* This Court, however, cannot make—and then implement—these nuanced policy judgments. Rather, "[t]his is a policy question for Congress." *Ibid.* See, *e.g.*, Pet. App. 68a (Lynch, J., concurring in the judgment) ("the policy concerns raised by the government are significant, and require the attention of Congress").

Both the Obama and the Trump administrations proposed legislation to address these concerns through new cross-border data access frameworks. See, *e.g.*, *Data Stored Abroad*, *supra*. The bilateral agreements envisioned in that legislation could be part of the solution to the problem of cross-border data demands.

Against this backdrop, the government is flatly wrong to assert that Microsoft's position is that Congress has "surrendered" "the raw power" for law enforcement to compel production of electronic contents stored abroad. U.S. Br. 47. Congress has not conferred that authority on law enforcement. It certainly may do so, but the Court should leave that issue for determination by Congress—particularly because the issue is one of statutory interpretation, not constitu-

---

fect the places in which a provider stores data. The Court should tailor its decision here to the facts before it, leaving Congress to develop more comprehensive standards and—in the absence of action by Congress—to future cases the question whether other network architectures might warrant a different outcome.

tional authority, and Congress "has ample power to amend the statute." *Holder* v. *Hall*, 512 U.S. 874, 957 (1994). Cf. *Carpenter* v. *United States*, *supra* (presenting question regarding the Fourth Amendment standard applicable to the seizure and search of cell site location information).

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted.

ANDREW J. PINCUS
Counsel of Record
PAUL W. HUGHES
Mayer Brown LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

Counsel for Amici Curiae

JANUARY 2018