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 TECHNOLOGY COMPANIES AS *AMICI CURIAE* IN SUPPORT OF RESPONDENT


CATHERINE M.A. CARROLL
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Ave. NW
Washington, DC 20006

*Counsel for Google LLC and Reddit, Inc.*

MARC J. ZWILLINGER
*Counsel of Record*
JEFFREY G. LANDIS
ZWILLGEN PLLC
1900 M Street, NW
Washington, DC 20036
(202) 296-3585
marc@zwillgen.com

*Counsel for Amazon.com, Inc., Apple Inc., Cisco Systems, Inc., Dropbox, Inc., eBay Inc., Facebook, Inc., HP Inc., Mozilla, Oath, salesforce.com, inc., SAP, and Verizon*


278197

## TABLE OF CONTENTS

*Table of Contents*

## TABLE OF CITED AUTHORITIES

*Page*

**CASES**

*Cited Authorities*

*Page*

**STATUTES**



**LEGISLATIVE AUTHORITIES**



**FOREIGN LAW**

*Page*



**OTHER AUTHORITIES**

*Page*

*Cited Authorities*

*Page*

## INTEREST OF AMICI CURIAE[1]

Amici are among the world's leading technology companies. Billions of people around the world rely daily on amici's search engines, email services, social networks, remote computing, cloud storage, and Internet infrastructure for their business and personal lives. Those customers entrust amici with some of their most important information, including the contents of their electronic communications. Given the sensitivity of that information, amici work continuously to secure their customers' privacy and have a strong interest in the legal standards governing law enforcement's ability to compel production of data about their customers.

To offer computing and electronic communications services as quickly and efficiently as possible, amici rely on worldwide networks of computer servers, including servers located outside the United States. Amici therefore have a particular interest in whether U.S. law enforcement may compel service providers to search, seize, and produce the contents of electronic communications stored on servers outside the United States using warrants issued under the auspices of the Stored Communications Act (SCA), 18 U.S.C. §§ 2703(a), (c).[2]

---

1. No counsel for a party authored this brief in whole or in part, and no entity or person, other than amici curiae, their members, and their counsel, made a monetary contribution intended to fund the preparation or submission of this brief. This brief is submitted pursuant to blanket consent letters from all parties on file with this Court.

2. Some of the amici may not be subject to the same statutory provisions at issue in this case, or in the same manner. But they are

***Amazon.com, Inc.*** is one of the world's largest and best known online retailers and cloud service providers. Amazon seeks to be the Earth's most customer-centric company, where customers can discover anything they might want to buy online at the lowest possible prices. Amazon's cloud computing business, Amazon Web Services, is trusted by more than a million active customers around the world—including the fastest growing startups, largest enterprises, and leading government agencies—to power their IT infrastructure, make them more agile, and lower costs.

***Apple Inc.*** is committed to bringing the best user experience and highly secure hardware, software and servers to its customers around the globe. In addition to selling the iPhone, iPad, Mac computer, and iPod, Apple also offers its users iCloud—a cloud service for storing photos, contacts, calendars, documents, device backups and more, keeping everything up to date and available to customers on whatever device they are using. To offer these services Apple relies on a worldwide network of computer servers to provide its users with fast, efficient services. Because some of those servers are located outside the United States and are operated by foreign subsidiaries, Apple's foreign subsidiaries control data stored abroad and may be subject to foreign laws regarding data transfer. Apple is committed to transparency and strives to provide straightforward disclosures about these laws, and the circumstances under which it is compelled to comply with legal process.

---

nonetheless concerned that the position taken by the government here could also be asserted under other laws, which could raise similar concerns to the concerns discussed in this brief.

***Cisco Systems, Inc.*** is the worldwide leader in providing infrastructure for the Internet. It also offers various services managed from data centers operated by Cisco which allow its customers to use, among other things, remote data centers, wireless internet services, internet security services, and collaboration tools which drive efficiency in their business. It relies on servers both inside and outside the United States, and is subject to, and must comply with, various foreign laws regarding data transfer. The confidence of customers in Cisco's ability to operate within the requirements of those laws is important to its business.

***Dropbox, Inc.*** provides file storage, synchronization, and collaboration services. With over 500 million users, people around the world use Dropbox to work the way they want, on any device, wherever they go. When users put their files in Dropbox, they can rest assured that their data is secure and their own.

***eBay Inc.*** is a global commerce leader including the Marketplace, StubHub and Classifieds platforms. Collectively, eBay connects millions of buyers and sellers around the world, empowering people and creating opportunity through Connected Commerce. eBay is one of the world's largest and most vibrant marketplaces for discovering great value and unique selection, with more than 1 billion listings globally.

***Facebook, Inc.*** provides a free Internet-based social-media service that gives more than two billion people the power to build communities and bring the world closer together. To provide a service that enables access and communication for people across the world, Facebook may

store and distribute some content and data in systems located outside the United States. Facebook is committed to protecting the privacy of the people who use its services. Facebook has robust privacy settings that allow people to control the audience of the information they choose to share. Facebook has also developed a privacy check-up tool to ensure that people's privacy settings reflect their desired level of privacy. Facebook regularly produces a Government Requests Report reflecting its responses to government requests for data.

***Google LLC*** is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of web-based products and services, including Search, Gmail, Maps, YouTube, and Blogger, that are used daily around the world. For example, there are more than a billion monthly active users of Gmail around the world. To use these and other services, users give Google information, including queries for Search, photographs for Photos, documents in Drive, emails in Gmail, videos for YouTube, and location information. To store this data, Google relies on servers located around the world and, like Microsoft, has received and brought legal challenges to search warrants issued under section 2703 of the SCA that purport to compel Google to search for, seize, and produce to the government the contents of customers' electronic communications that are stored on servers outside of the United States.

***HP Inc.*** engineers experiences that amaze through its portfolio of PCs, mobile devices, work stations, printers, 3D printers for industrial manufacturing, solutions and services. HP offers its products and services on a global

basis. A growing part of HP's business is its Device-as-a-Service offering for medium and large enterprises, where enterprises pay HP to manage their computing devices and/or solutions.

***Mozilla*** is a global, mission-driven organization that works with a worldwide community to create opensource products such as the Firefox browser. Mozilla's guiding principles recognize that individuals' security and privacy on the Internet are fundamental and not optional. Mozilla has therefore adopted data-privacy principles that emphasize transparency, user control, limited data collection, and multi-layered security control and practices.

***Oath,*** a subsidiary of Verizon, including its popular brand Yahoo! Mail, is a values-led company committed to building brands people love. As a global leader in digital and mobile, Oath reaches over one billion people around the world with a dynamic house of 50+ media and technology brands, including, in addition to Yahoo, well-known brands like Aol, HuffPost, TechCrunch, and Tumblr. Oath offers electronic communications and remote computing services to its customers around the world using a global network of servers to provide fast, efficient, reliable services. Because some of these servers are located outside the United States and operated by foreign subsidiaries, Oath and its foreign subsidiaries are subject to various foreign laws regarding data transfer. At the same time, Oath may also be subject to requests by U.S. law enforcement for data stored on servers abroad. Oath must balance complying with both foreign and domestic laws, as well as providing service to its customers, and doing so transparently in a way that enables users to understand how Oath handles their personal information.

***Reddit, Inc.*** operates the reddit.com platform, which is a collection of thousands of online communities attracting over 300 million monthly unique visitors that create, read, join, discuss and vote on conversations across a myriad of topics. Reddit is based in San Francisco, California.

***salesforce.com, inc.*** is a leading provider of enterprise cloud computing services headquartered in San Francisco, California. Salesforce has offices and data centers located internationally to service its customers.

***SAP*** is a leading technology company focused on developing innovative software and computer-based business solutions. It conducts significant research and development and invests heavily in commercializing innovative technologies.

***Verizon*** is a global leader delivering innovative communications and technology solutions. As a world-wide provider, Verizon offers integrated business solutions to consumer, business and government customers in more than 150 countries. The cloud is a key component of many of the managed services and platforms we sell to customers outside the United States and, as a result, many of these overseas customers' data is stored outside the United States. Verizon has long taken the view that the U.S. government cannot unilaterally require a U.S. company to produce data entrusted to it by a non-U.S. customer for storage outside the U.S.; and, Verizon has not received a U.S. warrant for our overseas business customers' data stored overseas. Still, the specter of receiving such a warrant is alarming to our current and potential customers who are concerned about a foreign country's law enforcement having access to their records; due to the risk and uncertainty, some

overseas customers are opting to obtain services from in-country providers. At the same time, the risk of receiving a U.S. warrant for data stored overseas is concerning to Verizon because it could put us in the position of facing inconsistent obligations, considering the data transfer laws in many of the countries in which we do business would prohibit our compliance with a U.S. warrant.

## SUMMARY OF ARGUMENT

This case presents a question not yet addressed by Congress—whether U.S. law enforcement can utilize a search warrant to gain access to the contents of a foreign user's email messages, stored by a U.S. electronic communications service provider in an Irish data center. Amici believe the answer is "No" for the following reasons: (1) section 2703 has no extraterritorial reach given that Congress did not contemplate U.S. providers storing data outside the U.S. when the law was enacted in 1986; (2) enforcing the warrant under these circumstances would violate the presumption against extraterritoriality outlined by this Court in *Morrison v. National Australia Bank Ltd.,* 561 U.S. 247 (2010); (3) enforcing the warrant risks a clash between U.S. interests and the interests of other nations; and (4) Congress is actively considering how to reconcile the competing interests involved in cross-border data searches and is, in any event, better suited to weigh the competing interests of law enforcement, foreign nations, and U.S.-based providers.

This Court, like the Second Circuit before it, must try to determine how the law applies to data stored overseas notwithstanding that rules for compulsory access by the government to such data cannot be found anywhere in

section 2703. The reason for this gap is simple: Congress did not consider that question when it enacted the SCA in 1986 because it could not foresee today's globally interconnected electronic world. Therefore, Congress never sought to address section 2703's extraterritorial application, and answers to the complicated policy questions raised by this case appear nowhere in section 2703. And, to be sure, these issues are weighty, implicating: sovereign interests of other countries that are concerned with protecting the security of their residents, the public-safety interests of the U.S. government, and the interests of providers of electronic communications services, who are responsible for building and maintaining the networks through which they provide those services.

Traditional tools of statutory interpretation compel only one result—affirming the Second Circuit's decision. The Government does not dispute that nothing in section 2703's text authorizes extraterritorial action. And the record in this matter is undisputed that the content subject to the warrant is located in, and would be seized from, Microsoft's Dublin datacenter. Thus, application of the warrant in the normal course would be considered an extraterritorial action because it would require a seizure of data from abroad at the Government's behest. The theory that the Government espouses—that the only factor that matters in determining whether section 2703 is being applied domestically or extraterritorially is the location of the disclosure to law enforcement—is unsupported by the law.

The rationale for the presumption against extraterritoriality is that only Congress is equipped to decide whether to risk conflict between U.S. interests

and the interests of other nations by extending U.S. law beyond our borders. By presuming that U.S. law does not apply overseas without clear evidence of congressional intent, the presumption protects against unintended clashes with other nations. The fact that the Government's interpretation might lead to just such unintended clashes affirms that the application of section 2703 here is not purely domestic.

This case raises difficult policy questions. But difficult policy questions must be answered by Congress in the first instance, not by the courts. Indeed, Congress is presently considering legislation designed to address this very issue. In the interim, however, the Court should adhere to the territorially limited terms of section 2703 and leave to Congress the job of deciding whether and how to extend the reach of warrants authorized by that section beyond the Nation's borders. Such an outcome may be unsatisfying as compared to a more thoughtful resolution that Congress could ultimately devise, but it is the only defensible result under existing law. Accordingly, the Court should affirm the Second Circuit's decision.

## ARGUMENT

### I. Congress Did Not Contemplate The Difficult Questions Posed By Modern Technology, Including U.S. Companies Storing Data Abroad, When It Passed the SCA.

The interconnected world we live in was not foreseen, let alone accounted for, by Congress when it drafted and enacted section 2703 more than 30 years ago. Today, the Internet and Internet-connected devices figure

prominently in nearly all aspects of our everyday lives. We communicate with friends and family located in the next room or on another continent nearly instantaneously using email, FaceTime, WhatsApp, and iMessage. We consume breaking news, store pictures of our family, and keep track of our food intake and exercise regimes using web browsers on our computers or mobile apps on our smartphones. We eschew paper maps in favor of the Global Positioning Systems built into our handheld devices. We use smart-refrigerators to tell us when to buy milk and smart-thermostats to turn up the heat automatically before we get too cold.

These daily interactions with Internet technology are essential parts of our lives. In short, "[u]se of the Internet is vital for a wide range of routine activities in today's world—finding and applying for work, obtaining government services, engaging in commerce, communicating with friends and family, and gathering information on just about anything, to take but a few examples." *United States v. LaCoste*, 821 F.3d 1187, 1191 (9th Cir. 2016); *see also United States v. Sofsky*, 287 F.3d 122, 126 (2d Cir. 2002) ("[c]omputers and Internet access have become virtually indispensable in the modern world. . . .") (citation omitted).

The Internet's ubiquity is not limited to the United States. In 2015, two-thirds of the world's adults used the Internet.[3] Even in developing countries, a median of 54 percent of the population used the Internet at least

3. Pew Research Center, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies* 4 (Feb. 2016).

occasionally.[4] As of 2013, 70 percent of Gmail users and 84 percent of Facebook users resided outside the United States.[5] There are now more Facebook users in India alone than in the United States.[6]

This current technological landscape sits in stark contrast to the background against which the SCA was enacted. Public access to the Internet did not arrive until three years after the SCA's enactment.[7] Web browsing functionality did not arrive until 1991.[8] And private companies did not host the "Internet backbone" until 1995.[9] When the SCA was enacted, there was no web-based email, and limited storage.[10] In fact, there was barely any online storage capacity at all—when email was

4. *Id.* at 3.

5. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act,* 162 U. Penn. L. Rev. 373, 406-407 (2014).

6. Dimitra DeFotis, *India Facebook Users Surpass U.S.: Is It Demonetization, Apple?*, Barron's (July 14, 2017), https://www.barrons.com/articles/india-facebook-users-surpass-u-s-is-it-apple-demonetization-1499982716.

7. *See* Yvonne Lee, *Compuserve, MCI Mail Introduce Gateways To Internet Network*, InfoWorld (Sept. 25, 1989) (discussing availability of first public gateways to the Internet).

8. Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1572 (2004).

9. *Id.*

10. Hotmail was released in 1996, and Yahoo Mail debuted in 1997. *See* Teddy Wayne, *A Eulogy for the Long, Intimate Email*, N.Y. Times (July 11, 2015), https://www.nytimes.com/2015/07/12/style/a-eulogy-for-the-long-intimate-email.html.

retrieved by a user it would be deleted from the server to make room for more email.[11]

Geographically, the Internet of 1986 was narrowly confined and barely crept outside the United States. Most relevant here, "communication over computer networks" in 1986 "occurred mostly in the United States."[12] It was not until 1988 that other countries began connecting to the U.S.-based Internet infrastructure.[13] The "World Wide Web" was not invented until 1991.[14] As the court below observed, "a globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future" when Congress passed section 2703. Pet. App. 14a.

In light of the mostly domestic Internet, Congress could not have contemplated that U.S. electronic communication providers would have the ability to store data belonging to hundreds of millions of foreign users on servers half-a-world away, and then be able to retrieve that data for U.S. law enforcement upon request. Indeed, the modern notion of "cloud computing" was at least a decade,

---

11. *See* Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 Am. U. L. Rev. 267, 272 (2013) (noting that around the time of the SCA's passage "permanent storage of emails was not feasible" and "communications were stored at the [personal computer] level and could only be accessed through that point.").

12. Kerr, 162 U. Penn. L. Rev. at 404-405.

13. *See* David C. Mowery & Timothy Simcoe, *Is the Internet a U.S. Invention?*, 31 Res. Pol'y 1369, 1376 (2002).

14. *See id*. at 1377-1378.

if not two, away when the SCA was passed in 1986.[15]

Not surprisingly given the foregoing sea change in technology, nearly everyone recognizes that the SCA is vastly outdated. Courts already acknowledged as much fifteen years ago. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002) (noting that because the statute "was written prior to the advent of the Internet and the World Wide Web" the "existing statutory framework is ill-suited to address modern forms of communication . . . ."). The insufficiency of the SCA has only gotten worse as technology has continued to march on, seemingly at an ever increasing pace.

One way in which section 2703 is outdated is in its territorial scope. The SCA does not address whether and to what extent U.S. law enforcement can gain access to the contents of communications stored extraterritorially. As a result of that silence, section 2703 contains no indication of what Congress would have intended with respect to the many complicated policy questions that are raised by extraterritorial warrant enforcement, such as how to accommodate the competing interests of foreign nations. As one commentator succinctly stated, section 2703 "simply was not written with the territoriality problem in mind." Kerr, 162 U. Penn. L. Rev. at 410.

Congress is currently looking at this issue. In July 2017, a bipartisan group of Senators introduced the

15. *See* Keith D. Foote, *A Brief History of Cloud Computing,* Dataversity (June 22, 2017), http://www.dataversity.net/brief-history-cloud-computing/.

International Communications Privacy Act ("ICPA").[16] That bill recognizes the "many interests that must be recognized when law enforcement agencies seek information from providers," such as the "legitimate needs of law enforcement agencies in the United States" to obtain data and the "legitimate interests of governments to protect the human rights, civil liberties and privacy of their nationals and residents." *Id.* §§ 2(3), 2(3)(A), 2(3)(C). The bill sets out a framework to allow courts to balance these interests, including the interests of consumers and the companies who serve them.

Amici favor a nuanced framework similar to what ICPA provides. But they also recognize that Congress could instead adopt some alternative framework that contemplates different considerations. What is beyond dispute, however, is that no such debate preceded the enactment of the SCA in 1986. As a result, the SCA's warrant provision contains no mechanism for accommodating both the legitimate needs of law enforcement to conduct cross-border investigations and the fundamental responsibility of other nations to safeguard their people.

## II. The Second Circuit Reached the Conclusion Dictated by the SCA as Currently Written.

Faced with an ill-fitting statute, the Second Circuit reached the only conclusion possible under the law as it exists today—that the Government lacked authority to compel Microsoft to retrieve data stored in a foreign country belonging to a self-proclaimed foreign user, and

16. S. 1671, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/senate-bill/1671/text.

provide it to U.S. law enforcement. In so holding, the Second Circuit faithfully applied the presumption against extraterritoriality as set forth in this Court's two-step test outlined in *Morrison*.

The Government concedes that the warrant provisions of the SCA do not contemplate or permit extraterritorial application. *See* Gov't Br. 16 ("Microsoft is correct that the presumption against extraterritoriality applies to Section 2703 and is unrebutted . . . ."). As to the second step of the *Morrison* analysis, the Second Circuit found that because "the content subject to the warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States." Pet. App. 44a. This was the only justifiable result. There is no dispute that the electronic communications subject to the warrant were stored exclusively in Ireland when the warrant was served by law enforcement in the United States. *See id.* at 21a.

To the extent that electronic data like that at issue here can be said to have a definitive location, warrant jurisprudence requires that data must be within the jurisdiction of the court issuing the warrant. A person within the jurisdiction cannot be conscripted to go outside the jurisdiction to retrieve the data. Amici have employees, offices, and users all over the world. A warrant ordering one of amici's American employees to fly to Ireland to retrieve data about a foreign user from a server located in Ireland, and bring that data back to U.S. law enforcement, would plainly be an extraterritorial application of the statute. The fact that amici have the technological

capability to retrieve the same information about the same foreign user from the same foreign country and hand it over to U.S. law enforcement without an employee (or law enforcement) physically entering the foreign country should not lead to a different conclusion. *Cf. United States v. Jones*, 565 U.S. 400, 406 n.3 (2012) (Fourth Amendment no more permits the government to track the movements of a vehicle by placing a GPS device on its undercarriage, than it permits the government to track the vehicle by concealing a constable in the vehicle's trunk).

The Government argues that the only relevant factor in determining whether section 2703 is being applied domestically or extraterritorially is where the disclosure to law enforcement takes place, and here the place of disclosure would be in the United States. *See* Gov't Br. 25 (asserting that the focus of section 2703 is disclosure and a section 2703 warrant requires a provider "to disclose records to the U.S. government in the United States"); *Id.* at 26 (noting that even if section 2703 focuses on "user privacy," any "relevant invasion of privacy occurs in the United States, when Microsoft discloses information to the government and the government reviews that information").

The location where the data is disclosed by a Microsoft employee to law enforcement officials cannot be the sole determinant of whether section 2703 is being applied extraterritorially. As the Supreme Court noted in *Morrison*, "it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States," and "the presumption against extraterritorial application would be a craven watchdog indeed if it retreated to its kennel whenever *some*

domestic activity is involved in the case." 561 U.S. at 266-67 (emphasis in original). But that is the conclusion the Government urges the Court to reach—as long as some portion of the execution of the warrant (the disclosure to law enforcement) occurs within the U.S., any and all extraterritorial actions or impacts of enforcing the warrant are irrelevant. This ignores how warrants work. In other contexts, warrants are not deemed executed at the place where the seized materials are disclosed.

The Second Circuit rejected this myopic view that a "foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to 'collect' from servers located overseas and 'import' into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States." Pet. App. 47a. Of course they are affected. They are affected the same way U.S. interests would be affected if a foreign judge issued an order requiring a foreign service provider to collect data belonging to a U.S. citizen from a U.S. location and provide it to foreign law enforcement. When a foreign law enforcement agency demands that the private communications of another country's citizens be retrieved from that country and turned over to the foreign law enforcement agency it, at the very least, affects the foreign country's interest in protecting the security and privacy of its citizens.

The Government cannot avoid the SCA's limitation on foreign seizures by arguing that a warrant issued pursuant to section 2703 is not really a warrant at all, but a special hybrid "warrant-subpoena" that can compel production of a company's own business records stored

abroad. Here, and in many other instances, electronic communication service providers are merely custodians holding customers' private email communications in which those customers have a reasonable expectation of privacy, and thus those email communications cannot be obtained via subpoena. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (noting that the government cannot compel a commercial ISP to turn over the contents of a subscriber's emails with a subpoena: it must obtain a warrant based on probable cause). And because providers like amici perform many services beyond transmitting emails or photos, in many cases the materials they store are not even the provider's customers' records, but rather their customers' customers' records.[17] The *Bank of Nova Scotia* doctrine simply does not apply to such materials.

Congress's deliberate decision to use the term "warrant" cannot be ignored when identifying the territorial locus of the conduct that the statute seeks to regulate. "[T]he SCA plainly distinguishes between subpoenas and warrants, and there is no indication that Congress intended for SCA warrants to be treated as subpoenas." *In re 381 Search Warrants Directed to Facebook, Inc.,* 78 N.E.3d 141, 147 (N.Y. 2017). Indeed, to equate a "warrant" and a "subpoena" in the SCA—as the government seeks to do (Gov't Br. 14-15, 34-36)—"would be to ignore the plain language of the SCA in contravention of the rules of statutory interpretation." 78 N.E.3d at 147; *see also United States v. Bach*, 310 F.3d 1063, 1066 n.1 (8th

17. For example, many businesses use cloud computing providers to host their own customers' data. For those businesses, the data in the cloud is neither the service provider's business records nor the business records of the service provider's customer.

Cir. 2002) ("Congress called them warrants and we find that Congress intended them to be treated as warrants.").

A warrant has long been understood to carry inherent territorial limitations. As then-Judge Gorsuch observed, "[t]he principle animating the common law at the time of the Fourth Amendment's framing was clear: a warrant may travel only so far as the power of its issuing official." *United States v. Krueger*, 809 F.3d 1109, 1124 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Engleman v. Murray,* 546 F.3d 944, 948 (8th Cir. 2008) ("At the time the Bill of Rights was adopted, a warrant issued in one English county was not valid in another county unless a justice of the peace in that county 'backed' the warrant." (citing Blackstone, 4 Commentaries on the Laws of England 292 (1765-1779))). Those territorial limitations apply to the Nation's international borders, no less than its domestic borders.

## III. Enforcing This Warrant In These Circumstances Will Have Impact Outside the United States and is Therefore Extraterritorial.

In characterizing the application of the search warrant in this case as purely domestic, the Government essentially disregards the issues that lie at the heart of the decision in *Morrison.* One basis for the strong presumption against extraterritoriality is that where there is a material risk of a clash between U.S. interests and the interests of other nations, the U.S. law should not apply unless there is a clear manifestation of congressional intent. *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991) (observing that presumption against extraterritoriality "serves to protect against unintended clashes between our laws and those of other nations").

Thus, another reasonable way to evaluate whether a purely domestic application is being proposed is to identify the existence and extent of foreign disruption caused by application of the statute. *See, e.g.*, Pet. App. 65a (Lynch, J., concurring) (noting that "concern[] about the diplomatic consequences of over extending the reach of American law enforcement officials" suggests a "more complex balancing exercise than identifying a single 'focus' of the legislation"). As Judge Lynch pointed out, given that "[t]he now-familiar idea of 'cloud' storage of personal electronic data by multinational companies was hardly foreseeable to Congress in 1986, and the related prospects for diplomatic strife and implications for American businesses operating on an international scale were surely not on the congressional radar screen when the Act was adopted," the Court "should not lightly assume that Congress chose to permit SCA warrants for communications stored abroad when there is no sign that it considered the consequences of doing so." *Id.* at 67a-68a (Lynch, J., concurring) (citing *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 116 (2013) ("The presumption against extraterritorial application helps ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches.")). The potential for conflicting interests between the United States and foreign nations is to be avoided under *Morrison* absent a clear expression of intent by Congress, which both parties agree is missing here. Regardless of whether any foreign implications were on the congressional radar screen in 1986, conflicting interests clearly exist today.

### A. The Government's Position Could Provoke Reciprocation from Foreign Governments.

Every nation founded on democratic principles has a strong and legitimate interest in ensuring that the security and privacy of the people it is charged with protecting are not improperly or unduly invaded.[18] Failure to accommodate that legitimate sovereign interest threatens to provoke dangerous reciprocation by foreign governments—at great potential cost to U.S. citizens and service providers.

Under current practices, service providers ordinarily refuse requests by foreign governments for the private communications of U.S. persons unless those requests proceed through diplomatic mechanisms such as the process established under the Mutual Legal Assistance Treaty ("MLAT") system.[19] Steering foreign requests

---

18. United Nations Declaration of Human Rights and the International Convention on Civil and Political Rights both recognize privacy as a fundamental human right. *See* Universal Declaration of Human Rights art. 12, G.A. Res. 217 (III) A, (Dec. 10, 1948); Int'l Covenant on Civil and Political Rights art. 17 G.A. Res. 2200A(XXI) (adopted Dec. 16, 1966, entry into force Mar. 23, 1976). Likewise, the European Union ("EU") has enshrined privacy as such in both the European Convention on Human Rights and the European Union Charter of Fundamental Rights. *See* European Convention for the Prot. of Human Rights and Fundamental Freedoms, art. 8, 213 U.N.T.S. 222 (Nov. 4, 1950); Charter of Fundamental Rights of the European Union, arts. 7-8, 2012 O.J. (C 326) 391 (Oct. 26, 2012).

19. For examples of provider guidelines for law enforcement discussing the need to use MLATs to obtain data, *see*, *e.g.*, https://support.google.com/transparencyreport/answer/7381738?hl=en;

to government-to-government diplomatic mechanisms, like the MLAT process, ensures that Americans' data is not disclosed absent compliance with the SCA and other statutory and constitutional safeguards. But the Government's position in this case puts significant pressure on this protective practice.

The potential for this pressure was acknowledged by multiple Second Circuit judges in this case. Judge Lynch's concurrence recognized that "[t]he attempt to apply U.S. law to conduct occurring abroad can cause tensions with those other countries, most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our borders." Pet. App. 55a-56a. Judge Jacobs' dissent on the Government's petition for en banc review, which was joined by three other judges, echoed these sentiments, explaining "I too would like to see Congress act, chiefly to consider certain ramifications, such as whether the United States might be vulnerable to reciprocal claims of access through local offices of American companies abroad." *Id.* at 123a. Law enforcement authorities have expressed similar concerns. *See* U.S. DOJ, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, A Report of the President's Working Group on Unlawful Conduct on the Internet* 21-22 (March 2000), *available at* https://www.hsdl.org/?view&did=3029. ("If law enforcement agents in the United States . . . remotely access a Canadian computer (from the United States),

---

https://www.facebook.com/safety/groups/law/guidelines/; https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf; https://www.tumblr.com/docs/en/law_enforcement.

might this constitute a criminal act under Canadian law notwithstanding the existence of the U.S. warrant? . . . [C]onsider how we would react to a foreign country's 'search' of our defense-related computer systems based upon a warrant from that country's courts.").[20]

### B. The Government's Position Could Undermine the MLAT Process.

The extraterritorial nature of this warrant is also illustrated by the fact that enforcing the warrant here could undermine existing international treaties. By participating in the MLAT process, the U.S. government has endorsed a specific set of procedures for resolving the complex web of jurisdictional questions and conflict of law issues presented by requests for foreign-stored data. MLATs provide a means by which one country can obtain another country's assistance in gaining access to data stored in that country. They do so in a way that seeks to strike a balance between one nation's law enforcement needs and another nation's autonomy to, among other things, promote its legal interests in areas like data privacy. MLATs, by definition, involve interests between sovereigns. *See* Black's Law Dictionary (10th ed. 2014)

---

20. The Government tries to downplay the risk of reciprocity by asserting that other countries already have laws that would allow them to reach into the U.S. to obtain a U.S. user's data, and suggesting that it is the U.S. that is the outlier by not acting similarly. *See* Gov't Br. 46-47. Notably, however, the Government does not identify any instance where any foreign government has sought to use a local form of legal process to obtain data about a U.S. citizen located in the U.S. without any involvement from the U.S. government. Nor does it say that the U.S. government would acquiesce in any attempt to do so.

(defining "Treaty" in the context of international law as "[a]n agreement . . . between two countries or sovereigns"). Here, what the Government is asking the Court to do is to authorize an end-run around MLAT procedures in the precise circumstances they were designed to address, rendering such procedures unnecessary and superfluous.[21] If the interpretation of a statute makes international treaties unnecessary and superfluous, then the statute is being applied in an extraterritorial way.

That there are complex policy ramifications in resolving the extraterritoriality question in favor of Microsoft or in favor of the government does not mean, however, that the two readings of section 2703 stand on equal footing.[22] The presumption against extraterritoriality

21. *See* Restatement (Third) of Foreign Relations § 321, cmt. a (noting that the doctrine of *pacta sunt servanda*—the principle that international agreements are binding and must be performed in good faith—"lies at the core of the law of international agreements and is perhaps the most important principle of international law"); s*ee also United States v. Stuart*, 489 U.S. 353, 368 (1989) (treaties "should generally be 'construe[d] . . . liberally to give effect to the purpose which animates [them]'") (citation omitted); *Chew Heong v. United States*, 112 U.S. 536, 540 (1884) ("Treaties of every kind . . . are to receive a fair and liberal interpretation, according to the intention of the contracting parties, and are to be kept in the most scrupulous good faith . . . the court cannot be unmindful of the fact that the honor of the government and people of the United States is involved in every inquiry whether rights secured by [treaty] stipulations shall be recognized and protected.") (internal quotation marks and citation omitted).

22. According to the Government, one policy ramification of a ruling that section 2703 does not allow law enforcement to gain access to foreign users' electronic communications stored outside the U.S. is that it will make it harder for law enforcement

dictates how to construe a statutory provision that triggers extraterritoriality concerns that Congress did not address: select the reading that gives the statute only a domestic scope and leave to Congress the task of revising the statute to address whatever shortcomings result. *See, e.g., RJR Nabisco, Inc. v. Eur. Cmty.*, 136 S. Ct. 2090, 2100 (2016) (noting that "to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries" is the "most notabl[e]" reason for the presumption against extraterritoriality); *see also Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 261 (2010) (presumption "preserv[es] a stable background against which Congress can legislate with predictable effects").

## IV. Only Congress Can Decide How Section 2703 Should Apply Beyond U.S. Borders.

If the potential effects of allowing U.S. law enforcement to obtain data belonging to foreign users stored within foreign borders are to be properly weighed and balanced, Congress, not the courts, must do so. The job of the courts is "to apply faithfully the law Congress has written," not to "rewrite a constitutionally valid statutory text under

---

to obtain such communications because providers can choose to store them in a way that might stymie law enforcement. Gov't Br. 42-43. But there is nothing in the record in this case to suggest that Microsoft stored the relevant communications the way it did in order to stymie law enforcement. Rather, the record is that it was Microsoft's desire to reduce "network latency" that led it to store the communications near this user's reported location (which the Government does not claim was falsely designated). Gov't Br. 5. Nor do amici make decisions on how to store electronic communications based on a desire to thwart U.S. law enforcement.

the banner of speculation about what Congress might have done had it faced a question that, on everyone's account, it never faced." *Henson v. Santander Consumer USA*, 137 S. Ct. 1718, 1725 (2017); *see also Magwood v. Patterson,* 561 U.S. 320, 334 (2010) ("We cannot replace the actual text with speculation as to Congress' intent."). But rewriting section 2703 based on speculation regarding what Congress might have done in 1986 had it encountered U.S. providers storing foreign users' communications abroad is what the Government is asking the Court to do. That is not proper. Congress, not the courts, "has the prerogative to determine the exact right response—choosing the policy fix, among many conceivable ones, that will optimally serve the public interest." *Kimble v. Marvel Entm't, LLC*, 135 S. Ct. 2401, 2414 (2015).

Congress could, after debate and deliberation, pick any number of ways to address this issue. Congress ***could*** decide that the benefit of making it easier for U.S. law enforcement to obtain data stored abroad so greatly outweighs risks such as reciprocity or undermining the existing MLAT process, that it simply adds a provision to the SCA saying that its warrants apply extraterritorially. Congress ***could*** instead take a nuanced approach, and identify various requirements for a warrant seeking foreign-user data and/or factors courts should consider when evaluating requests for data stored abroad, such as the nature of the crime being investigated, the location of the user, and any reciprocal rules enacted by other nations. Or Congress ***could*** do something else entirely. The point is that these are decisions for Congress, not the courts.

While the SCA has given rise to many disagreements—in this case and elsewhere—there is broad consensus

about the need for Congress to step in to update the statute. Indeed, that seems to be the one point on which the members of the court below uniformly agreed. In her opinion concurring in the order denying rehearing en banc, Judge Carney noted that ECPA "is overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose." Pet. App. 108a. The other opinions filed in response to the government's petition for rehearing en banc, including those denying rehearing, likewise encouraged Congress to address this issue. *See id.* at 105a-119a.

That consensus is shared widely across relevant sectors. A June 2017 hearing before the Judiciary Committee in the House of Representatives, for example, featured testimony from representatives of state, federal, and international law enforcement; the technology sector; academia; and civil liberties groups. Although each witness advocated for different legislation, the one thing they seemed to agree on was the need for ***Congress*** to craft a solution.[23]

---

23. *See, e.g.*, *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era*, Hearing Before the H. Comm. on the Judiciary, 115th Cong. (June 15, 2017), *available at* https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era/. Testimony of Richard Salgado ("Congress has an opportunity to update ECPA for the Internet age, and to consider how the application of domestic U.S. surveillance laws affects the equities of foreign countries and the privacy rights of non-US persons."); Testimony of Andrew Keane Woods ("Congress is faced with a momentous task: to devise a set

Even the U.S. Department of Justice has joined the chorus of voices calling for Congress to act. During the June 2017 House hearing, for example, Acting Deputy Assistant Attorney General Richard W. Downing urged that "Congress should consider targeted amendments to the SCA that will provide for the legitimate needs of law enforcement" but also "address foreign countries' legitimate public safety needs" and "reduce the chance that providers will be caught in conflicting obligations between U.S. and foreign laws."[24] In doing so, he cautioned that any legislative solution "should avoid creating an incentive for other countries to create 'data localization' laws" which he said "are burdensome on U.S. providers, limit access to evidence needed to assure public safety, and have been called out by the U.S. Trade Representative as a key barrier to trade."[25]

If the SCA's warrant provisions are to accommodate the interconnected world brought about by the digital age, including addressing how to deal with foreign user data

---

of rules for law enforcement access to criminal evidence stored in the global cloud."); Testimony of Paddy McGuinness ("Congress now has the opportunity to set new global standards for cross-border data access, improve UK and US ability to protect each others' citizens and tackle global threats, through introducing and advancing this ground breaking legislation."); Testimony of Chris Calabrese ("We urge the committee to find solutions to this problem that update key components of the Electronic Communications Privacy Act (ECPA) and respect the privacy of individuals around the world while also meeting the legitimate needs of law enforcement.").

24. *Id.* Testimony of Richard Downing.

25. *Id.*

held by U.S. providers in foreign countries, Congress must act. As this Court recently reiterated:

> For us to run interference in . . . a delicate field of international relations there must be present the affirmative intention of the Congress clearly expressed. It alone has the facilities necessary to make fairly such an important policy decision where the possibilities of international discord are so evident and retaliative action so certain. The presumption against extraterritorial application helps ensure that that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches.

*Kiobel*, 569 U.S. at 115-16 (internal quotation marks and citation omitted).

Where no such affirmative intention exists, courts must not entertain "judicial-speculation-made-law—divining what Congress would have wanted if it had thought of the situation before the court." *Morrison*, 561 U.S. at 261. The proper role of the judiciary is instead "to give the statute the effect its language suggests, however modest that may be; not to extend it to admirable purposes it might be used to achieve." *Id.* at 270. As in *RJR Nabisco*, the proper question in this case is "not whether we think 'Congress would have wanted' a statute to apply to foreign conduct 'if it had thought of the situation before the court,' but whether Congress has affirmatively and unmistakably instructed that the statute will do so." *RJR Nabisco*, 136 S. Ct. at 2100 (citation omitted). The answer to that question is not in dispute—it has not.

In light of the efforts and attention expended so far on ICPA and other measures, there is every reason to believe that Congress is considering possible solutions here. Until it acts, however, this Court's path is clear: it must give section 2703 the territorial scope that aligns with the text of the statute and the domestically focused expectations of Congress in 1986, and allow Congress the opportunity to revise the SCA to better accommodate the more interconnected world that exists today.

## CONCLUSION

For the foregoing reasons, the court of appeals' judgment should be affirmed.

Respectfully submitted,

Catherine M.A. Carroll
Wilmer Cutler Pickering
Hale and Dorr LLP
1875 Pennsylvania Ave. NW
Washington, DC 20006

*Counsel for Google LLC and Reddit, Inc.*

Marc J. Zwillinger
*Counsel of Record*
Jeffrey G. Landis
Zwillgen PLLC
1900 M Street, NW
Washington, DC 20036
(202) 296-3585
marc@zwillgen.com

*Counsel for Amazon.com, Inc., Apple Inc., Cisco Systems, Inc., Dropbox, Inc., eBay Inc., Facebook, Inc., HP Inc., Mozilla, Oath, salesforce.com, inc., SAP, and Verizon*