14-2985

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 14-2985

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

MICROSOFT CORPORATION,

Appellant,

—v.—

UNITED STATES OF AMERICA,

Appellee.

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

PETITION FOR REHEARING AND REHEARING *EN BANC*

PREET BHARARA,
United States Attorney for the Southern District of New York,
Attorney for the United States of America.
One St. Andrew's Plaza
New York, New York 10007
(212) 637-2200

TIMOTHY HOWARD,
MARGARET GARNETT,
Assistant United States Attorneys,
Of Counsel.

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

United States Court of Appeals

FOR THE SECOND CIRCUIT

Docket No. 14-2985

MICROSOFT CORPORATION,

Appellant,

—v.—

UNITED STATES OF AMERICA,

Appellee.

PETITION OF THE UNITED STATES OF AMERICA FOR REHEARING AND REHEARING *EN BANC*

Preliminary Statement

On July 14, 2016, this Court issued an opinion in this matter (Carney, C.J., and Bolden, D.J., by designation; Lynch, C.J., concurring) vacating an order holding Microsoft Corporation ("Microsoft") in contempt, and remanding the case to quash a search warrant (the "Warrant"), issued pursuant to Section 2703 of the Stored Communications Act ("SCA"), that required Microsoft to disclose the contents of an email account to the Government. The majority opinion ("Opinion"), written by Judge Carney and joined by Judge Bolden, reached the unprecedented conclusion

that Section 2703 does not authorize courts to issue and enforce warrants to U.S.-based Internet service providers for the disclosure of customer email content that is stored on foreign servers but entirely within the control of the U.S.-based company. Judge Lynch concurred in a separate opinion, although he disagreed with much of the majority's reasoning.

The Opinion rests almost entirely on the erroneous conclusion that the enforcement of the disclosure obligation in the Warrant would be an impermissible extraterritorial application of Section 2703. In contravention of *RJR Nabisco Inc.* v. *European Community*, 136 S. Ct. 2090 (2016), which clarified that the extraterritoriality inquiry proceeds on a provision-by-provision basis, the Opinion conducts almost no analysis of Section 2703 itself. Instead the Opinion relies on the title of the overall statute in which the SCA appears and provisions of the SCA other than Section 2703 in reaching its conclusion that the "focus" of Section 2703 is "privacy." The Opinion further concludes that the physical location of this nebulous privacy interest is in Dublin, Ireland, even though the email account-holder —the ostensible beneficiary of the privacy interest— does not choose the storage location, cannot prevent Microsoft from moving the email content into the United States or indeed anywhere it chooses, and has no means to determine where Microsoft, in its own business interests, has chosen to store the data.

This case plainly involves a "question[ ] of exceptional importance," Fed. R. App. P. 35(b)(1)(B), because it is significantly limiting an essential investiga-

tive tool used thousands of times a year, harming important criminal investigations around the country, and causing confusion and chaos among providers as they struggle to determine how to comply. The Opinion breaks with over two decades of settled SCA enforcement and compliance, in holding that a U.S.-based company can refuse to use U.S.-based facilities and employees to comply with a court-authorized disclosure warrant, issued upon a showing of probable cause, merely because the company chooses in its sole discretion to store the electronic data sought by the warrant on its own overseas servers. The Opinion's impact is not limited to cases in which targets are, or claim to be, located overseas and in which it is potentially feasible for the United States to obtain content data from authorities in the country where it is stored. Unlike Microsoft, some major providers cannot easily determine where customer data is physically stored, and some store different parts of customer content data in different countries. Major U.S.-based providers like Google and Yahoo! store a customer's email content across an ever-changing mix of facilities around the world. To the extent content is stored abroad by the provider at the moment the warrant is served, the Opinion has now placed it beyond the reach of a Section 2703 warrant, even when the account owner resides in the United States and the crime under investigation is entirely domestic. At least in the case of Google, the information is also currently beyond the reach of a Mutual Legal Assistance Treaty request or any foreign law enforcement authority, because *only* Google's U.S.-based employees can access customer email accounts, regardless of where they are stored;

indeed, Google cannot reliably identify the particular foreign countries where a customer's email content may be stored. Thus, critical evidence of crimes now rests entirely outside the reach of any law enforcement anywhere in the world, and the randomness of where within an intricate web of servers the requested content resides at a particular moment determines its accessibility to law enforcement. Not surprisingly, the Opinion has substantially impaired law enforcement's ability to use a vital tool to investigate and prosecute all types of serious crime—including terrorism, public corruption, cyber-crime, securities fraud, child sexual exploitation, and major narcotics trafficking—and has thus contravened the express will of Congress that disclosure of electronic communications, with the protections of the warrant requirement, be available to aid in criminal investigations. The appeal should be reheard.[1]

Statement of the Case

A. Microsoft's Customer Email Storage Practices

Microsoft is a U.S.-based provider of email services, available to the public without charge. Op. 7. Microsoft stores the contents of a customer's e-mails, in addition to non-content account information, on a network of computer servers. Those servers are housed in roughly 100 datacenters that Microsoft and its subsidiaries op-

---

[1] The Solicitor General has authorized this petition for rehearing and rehearing *en banc*.

erate in, among other places, the United States, Ireland, and approximately 38 other countries. Op. 7-9. Microsoft asserts that it typically stores email content at datacenters located near the physical location identified by the user as his own when subscribing to the service. Op. 8. Once a user provides his purported location, Microsoft typically migrates all the user's content data to the closest Microsoft-owned datacenter, and, where that process results in storage on a server outside the United States, Microsoft maintains only limited non-content information about the account on servers in the United States. Op. 8-9. Microsoft makes no effort to verify the location provided by the customer, and nothing in the Microsoft customer agreement gives the customer any control, or right to control, where Microsoft stores his email content or when Microsoft moves that content into or out of the United States. Microsoft asserts that, following migration, the only way to access and repatriate user data stored in overseas datacenters is for a Microsoft employee to log into a database management program and access the relevant foreign datacenter. Op. 9. Under current Microsoft practices for responding to requests from U.S. law enforcement agencies, that employee is located in Redmond, Washington.

B. Section 2703

Congress enacted Section 2703 in 1986 as part of the Electronic Communications Privacy Act, and substantially revised Section 2703 in 2001 via the PATRIOT Act. *See* Pub. L. 99-508 § 201; Pub. L. 107-56 §§ 209, 210, 212, 220. Section 2703 regulates the pro-

cesses that the Government can use to require providers of electronic communications services to disclose communications. Most relevant here, Section 2703(a) provides that the Government may require a service provider to disclose the content of email communications in electronic storage no longer than 180 days only when the government obtains "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction," 18 U.S.C. 2703(a), which expressly includes "federal courts with jurisdiction over the offense being investigated," 18 U.S.C. 2711(3).

C. Proceedings Below

On December 4, 2013, Magistrate Judge James C. Francis IV in the Southern District of New York, based on a finding of probable cause, issued the Warrant pursuant to Section 2703 to require Microsoft to disclose the contents of an email account and to authorize the Government to search the disclosed material for evidence of international drug trafficking. Op. 9. Microsoft subsequently determined that the content data related to the target email account was stored in its Dublin, Ireland datacenter. Op. 11. Microsoft disclosed all responsive non-content information that was stored on servers located within the United States, but moved to quash the Warrant with respect to email content stored in Dublin. Op. 11.

Judge Francis denied the motion to quash the Warrant. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014). Judge

Francis noted that he had previously found probable cause for the requested search and, inasmuch as a Section 2703 warrant is served on a service provider rather than on a law enforcement officer, it "is executed like a subpoena in that it . . . does not involve government agents entering the premises of the [Internet Service Provider] to search its servers and seize the e-mail account in question." *Id.* at 471. Accordingly, Judge Francis determined that Congress intended that Section 2703's warrant provision impose similar obligations to a subpoena to "produce information in [the provider's] possession, custody, or control regardless of the location of that information." *Id.* at 472 (citing *Marc Rich & Co.* v. *United States*, 707 F.2d 663, 667 (2d Cir. 1983)). Judge Francis concluded that Microsoft was obligated to disclose the content information for the target email account, regardless of where it was stored. In the course of his analysis, Judge Francis treated the place where the government would receive and review the disclosed content (the United States), and not the place of storage (Ireland), as the relevant location. *See id.*

Microsoft appealed the decision to then-Chief District Judge Loretta A. Preska, who adopted Judge Francis' reasoning and affirmed. Op. 12.

D. The Opinion

The Panel reversed, vacated the contempt order, and remanded for the District Court to quash the Warrant, holding that enforcing the Warrant would constitute an impermissible extraterritorial application of the statute.

First, relying largely on *RJR Nabisco, Inc.* v. *European Community*, 136 S. Ct. 2090 (2016), and *Morrison* v. *National Australia Bank Ltd.*, 561 U.S. 247 (2010), the Court held, "with relative ease" and in line with the Government's position at oral argument, that Section 2703 does not apply extraterritorially. *See* Op. 21-32 & n.19. The Court rejected the District Court's finding (and the Government's argument) that the warrant provision in Section 2703 was equivalent to compelled disclosure pursuant to subpoena, because Section 2703 has a separate explicit "subpoena" provision for disclosure of non-content subscriber information and because Section 2703 makes specific reference to the procedures for traditional search warrants outlined in Federal Rule of Criminal Procedure 41. Op. 28-29. Although Section 2703 warrants first require disclosure by service providers in order for government agents to perform the authorized search, the Court asserted that such disclosure to the Government was akin to private parties sometimes being required to assist with searches or seizures pursuant to traditional search warrants. Op. 29. Further, the Court distinguished compelled disclosure of overseas records by subpoena under *Marc Rich* from SCA warrant disclosures, based both on the differences between subpoenas and search warrants, and on the fact that, unlike the financial institution in *Marc Rich*, the data was not Microsoft's own data, but rather data for which its customer had a protectable privacy interest and for which Microsoft acted as a caretaker. Op. 30-31.

After concluding that the SCA does not apply extraterritorially, the Court held that requiring Microsoft to disclose email content stored overseas, but

accessed here in the United States, pursuant to a Section 2703 warrant was a prohibited extraterritorial application of the statute. Op. 32-37. It did so by concluding that the "focus" of the SCA was the *privacy* of stored communications, and not *disclosure* to the government, based on the title of the overall statute that created the SCA (the "Electronic Communications Privacy Act"), and the statutory structure, which permits certain disclosures under Section 2703 as exceptions to broader prohibitions in other SCA sections against unauthorized access and disclosures of data stored by internet service providers. Op. 34-37. Given its conclusion that the SCA's focus is on protecting the privacy of stored data, the Court had "little trouble concluding" that because the data at issue was stored in Dublin, the invasion of the customer's privacy interest would occur there, where it would be "seized" by Microsoft as a compelled agent of the government, and thus the execution of the Warrant was an unlawful extraterritorial application of the SCA. Op. 39. The Court explicitly rejected the District Court's conclusion that the SCA only places obligations on the provider to act domestically to retrieve the data and act within the United States (which Microsoft conceded it would do here), because the Court found that the requested data lay within the jurisdiction of a foreign sovereign, and because the District Court's reasoning overlooked the SCA's formal recognition of the service provider as merely the caretaker of the content data that is entrusted to it by its customers. Op. 40.

Judge Lynch concurred in the judgment, writing separately in part to dispute Microsoft's arguments

that the case involved a government threat to individual privacy, as the Government here had complied with the most restrictive privacy-protecting requirements of Section 2703 and the Fourth Amendment by obtaining a warrant from a neutral magistrate based on a showing of probable cause. Conc. Op. 1-2. Judge Lynch emphasized that Microsoft was not arguing that "if the emails sought … were stored on a server" in the United States "there would be any constitutional obstacle to the government's acquiring them by the same means that it used in this case." Conc. Op. 3. Rather, "the sole issue" in the case was "whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing—in its own discretion—to store them on a server in another country." Conc. Op. 4. Judge Lynch also noted that the Government's characterization of the warrant in this case "as [a] domestic, rather than extraterritorial" application of the statute is "far from frivolous," and found "quite reasonable" the Government's argument that the "focus" of Section 2703 "is not on the place where the service provider stores the communications, but on the place where the service provider discloses the information to the government, as requested." Conc. Op. 10-12. Ultimately, however, Judge Lynch agreed with the majority's conclusion, based primarily on his view that Congress had never considered factual circumstances like these when it enacted the SCA, and that the strong presumption against extraterritoriality compelled such a conclusion. Conc. Op. 13-16.

ARGUMENT

The Panel Erroneously Concluded that Enforcement of the Warrant Was an Impermissible Extraterritorial Application

A. The "Focus" of Section 2703 is Disclosure, Which Occurs in the United States

The Government does not challenge the Panel's conclusion that the SCA, and Section 2703 in particular, does not apply extraterritorially. However, that does not end the inquiry. As the Supreme Court explained in *RJR*, if a statute does not have extraterritorial effect, the next question is to "determine whether the case involves a domestic application of the statute, and [courts] do this by looking to the statute's 'focus.'" 136 S. Ct. at 2101. "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad." *Id*. The "focus" inquiry is provision-specific, not on the statute as a whole, such that some provisions of a statute may apply extraterritorially even where other provisions of the same statute do not. *Id*. at 2101-11 (in RICO, certain aspects of 18 U.S.C. § 1962 apply extraterritorially but § 1964(c) does not); *see also Morrison*, 561 U.S. at 263-65.

Applying those principles here, the focus of Section 2703 is plainly disclosure, not privacy. Each of the first three subsections begins with "a governmental entity may require disclosure" or very similar language, and goes on to describe the specific circumstances in which

the Government may require a service provider to disclose electronic communications, including email content, and the procedures the Government must follow. Section 2703(e) also shields service providers from civil liability for disclosing information in response to process under Section 2703. Indeed, the clear purpose of Section 2703, as a whole, is to outline the circumstances in which a customer's privacy interest in the content of their emails must yield to the Government's interests in obtaining those emails through disclosure by the service provider. The Opinion acknowledges as much. *See* Op. 35 ("Section 2703 governs the circumstances in which information associated with stored communications may be disclosed to the government"). Moreover, Section 2703's title—"Requirements for governmental access," Pub. L. 99-508 (Oct. 21, 1986), amended to "Required disclosure of customer communications or records," Pub. L. 107-56 (Oct. 26, 2001)—further supports the view that the provision's "focus" is disclosure to the Government.[2]

The majority's conclusion that the "focus" of the SCA is "privacy" rests on several faulty premises, in addition to its failure to conduct the "focus" inquiry on

---

[2] The majority noted the *overall statute's* title—"The Electronic Communications Privacy Act"—as support for its conclusion that the "focus" is privacy. *See* Op. 34. But as set forth above, the "focus" inquiry of *Morrison* and *RJR* proceeds provision by provision, and accordingly the title of Section 2703 is far more relevant to ascertaining the section's focus than the title of the statute as a whole.

a provision-specific basis. First, the Opinion essentially ignores the fact (identified repeatedly by Judge Lynch, *see, e.g.,* Conc. Op. 2-3) that all the references to "privacy" in the SCA, *see, e.g.,* Op. 13-14, 33, must be viewed in the context of an understanding—since the nation's founding and certainly in 1986—that a warrant issued by a neutral magistrate based on a showing of probable cause is a recognized and constitutionally-prescribed means of overcoming *any* privacy interest. Indeed, no privacy interest (whether in email content stored by Microsoft, or in a personal diary stored in a bedroom) is protected against such a warrant. Thus any discussion of privacy in the SCA or its legislative history is occurring in the context of the widespread recognition that the limit of privacy is reached where the warrant begins. The majority acknowledges this only in passing, with seemingly no effect on its analysis. Op. 38.

Second, the Opinion weighted heavily, unmoored from any precedent, the notion that Microsoft is the "caretaker" of customer's privacy interests. *See, e.g.*, Op. 31. This "caretaker" argument is not compelling where it is Microsoft who chooses the storage location and not the customer (indeed the customer does not even know where the content is stored), and both Microsoft and the Panel acknowledge that Microsoft would promptly disclose to the Government any customer email content that it chose to store in the United States. It cannot be true that the "focus" of the statutory provision is privacy, but the protection of that privacy interest rests entirely on the profit-driven deci-

sions of a private business, with no choice by or consultation with the owner of the account and the beneficiary of the privacy interest.

Third, the Panel ignored relevant legislative history of Section 2703. In its consideration of legislative history, the Opinion focuses exclusively on the enactment of the SCA in 1986. Op. 37-39. But in 2001, in response to the 9/11 attacks, Congress passed the USA PATRIOT Act, and four separate provisions of that Act revised Section 2703 to ensure that the SCA's disclosure provisions functioned effectively. *See* USA PATRIOT Act of 2001 §§ 209, 210, 212, 220, Pub. L. 107-56, 115 Stat. 272 (2001). That Act (and its amendments to Section 2703) focused on disclosure: its very first clause stated that its purpose was "to enhance law enforcement investigatory tools." Thus, if there was ever any doubt that the focus of Section 2703 is disclosure rather than privacy, the USA PATRIOT Act removes it. The Opinion, which leaves the warrant provisions of Section 2703 fundamentally broken, is inconsistent with that Act.

In short, the "focus" of Section 2703 is disclosure, and that disclosure happens in the United States, when Microsoft discloses the responsive material to the Government.[3] That understanding also comports

---

[3] Judge Lynch's concurring opinion does not directly address this second step of the *Morrison*/*RJR* inquiry, and never squarely identifies what, in his view, is the "focus" of Section 2703, nor whether the relevant conduct occurs in the United States or elsewhere. Rather, his concurrence seems based primarily on his

with the longstanding legal rule that a subpoenaed party subject to the jurisdiction of the district court is required to turn over materials in that party's control, even if the materials are located elsewhere. *See, e.g.*, *Marc Rich*, 707 F.2d at 670; *Hay Group, Inc.* v. *E.B.S. Acquisition Corp.*, 360 F.3d 404, 412 (3d Cir. 2004) (Alito, J.) ("'[p]roduction' refers to the delivery of documents, not their retrieval, and therefore 'the district in which the production . . . is to be made' is not the district in which the documents are housed but the district in which the subpoenaed party is required to turn them over").

Moreover, even if the relevant focus were "privacy," the conduct relevant to that focus would still occur in the United States, when Microsoft discloses the content information to the Government or when law enforcement agents search it. The account owner has no

---

view that Congress did not "demonstrate a clear intention to reach situations of this kind in enacting the Act," because situations of this kind did not exist, nor were they foreseeable, in 1986. Conc. Op. 15. But this cannot be the correct analysis. The applicability of federal statutes, with broadly defined terms like "electronic communications," cannot be held hostage to rapid changes in technology, particularly where, as here, Section 2703 warrants were used by the Government, and honored by Microsoft and other service providers without complaint, for the last two decades of rapid development of internet-based and mobile communications platforms, none of which were widely anticipated in 1986.

privacy interest in his emails being stored in Microsoft's Dublin datacenter, as opposed to Microsoft's datacenters in the United States. Indeed, the undisputed record in this case makes clear that the customer has no say in choosing where Microsoft stores his email content, is not told where that email content is stored, and would have no recourse whatsoever—nor even any notice—if Microsoft decided, for its own private business interests and in its sole discretion, to move that email content into or out of the United States. There is no infringement of the customer's privacy interest in his email content based on where Microsoft, at any given moment, chooses to store that content. Rather, the privacy intrusion occurs only when Microsoft turns over the content to the Government, which occurs in the United States. The majority's conclusion that the intrusion instead occurs where Microsoft "accessed" or "seized" the email content, Op. 39, is plainly wrong, because Microsoft could "access" or "seize" the email content on its own volition at any time and move it into the United States, or to China or Russia, or anywhere it chose, and the content would remain under Microsoft's custody and control and the subscriber could not be heard to complain, unless and until the content were disclosed to the Government or another party. This point is amply demonstrated by the concession of both Microsoft and the majority that Microsoft would have to comply with the Warrant if it had chosen (without consulting the subscriber) to move the target email account into the United States, even mere moments before the Warrant was served.

B. The Opinion Contravenes the Will of Congress that Disclosure Be Permitted for Criminal Investigations

Contrary to the suggestion in the Opinion that law enforcement interests were merely peripheral to Congress' purpose in enacting and amending Section 2703, the entirety of Section 2703 is trained on the means by which the Government may require disclosure of electronic communications, whether by demonstrating to a neutral magistrate that there is probable cause to believe the communications contain evidence of a crime, or by proffering "specific and articulable facts showing that there are reasonable grounds to believe that the … information sought [is] relevant and material to an ongoing criminal investigation," 18 U.S.C. 2703(a), (d). In contravention of this clear intent, the Opinion allows U.S.-based service providers to frustrate important criminal investigations, whether purposefully or inadvertently, by adopting a business practice of storing email content overseas. In the best case, the Government may be able to obtain this information via the costly, cumbersome and time-consuming process of seeking legal assistance from foreign authorities pursuant to treaties, where available; but in many cases the Government will have no ability to use those means at all. This effect is already harming important criminal investigations, and it has potentially even farther-reaching consequences. Criminals, like most everyone else today, communicate electronically, and thus prosecutors routinely use Section 2703 warrants to require disclosure of information relevant to a

wide array of criminal investigations.[4] The numbers are substantial. For example, in the second half of 2015, Google alone received 3,716 warrants seeking data from a total of 9,412 accounts. *See* Google Transparency Report, *available at https://www.google.com/transparencyreport/userdatarequests/US/#criminal_legal_requests*. Major service providers like Google and Yahoo!, who store different

---

[4] Significant examples of the vital importance of this investigative technique, in this District alone, include *United States* v. *Clarke*, 13 Mj. 0683 (extensive bribery scheme in violation of the Foreign Corrupt Practices Act); *United States* v. *Ross William Ulbricht*, 14 Cr. 68 (KBF) (international narcotics trafficking on the Silk Road internet platform); *United States* v. *Mitsakos*, 16 Mj. 4997 (securities fraud); *United States* v. *Reza Zarrab*, 15 Cr. 867 (RMG) (large-scale evasion of the financial-sanction regime against Iran); *United States* v. *Samia*, 13 Cr. 521 (LTS) (murder for hire); *United States* v. *Le*, 15 Cr. 38 (AJN) (purchase of the dangerous poison ricin and aggravated identity theft); *United States* v. *Li Fangwei*, 14 Cr. 144 (RA) (international arms trafficking); *United States* v. *El-Hanafi*, 10 Cr. 162 (KMW) (material support to terrorist organizations); *United States* v. *Ashe*, 15 Cr. 706 (VSB) (bribery of United Nations officials); *United States* v. *Skelos*, 15 Cr. 317 (KMW) (bribery of New York state senate majority leader); *United States* v. *Seabrook*, 16 Cr. 467 (ALC) (bribery of the head of the NYC correction officer's union); *United States* v. *Pan*, 12 Cr. 153 (RJS) (election fraud).

pieces of information for a single customer account in various datacenters at the same time, and routinely move data around based on their own internal business practices, are now disclosing only those portions of customer accounts stored in the United States at the moment the warrant is served—even though, at least as to Google, the *only* employees who can access the entirety of a customer's account, including those portions momentarily stored overseas, are located in the United States. Yahoo! has informed the Government that it will not even preserve data located outside the United States in response to a Section 2703 request, thereby creating a risk that data will be moved or deleted before the United States can seek assistance from a foreign jurisdiction, much less actually serve a warrant and secure the data. In addition, some providers are apparently unable to tell the Government, in response to Section 2703 disclosure orders, where particular data is stored or whether it is stored outside the United States, further frustrating law enforcement's ability to access such data.

In clear violation of Congress' expectations when enacting and amending Section 2703, the Opinion has created a regime where electronic communication service providers—private, for-profit businesses answerable only to their shareholders—can thwart legitimate and important criminal and national security investigations, while providing no offsetting, principled privacy protections. As Judge Lynch explained, with respect to Microsoft's customers, "[i]t is only *foreign* customers, and those Americans who *say* that they reside abroad, who gain any enhanced protection from the

Court's holding." Conc. Op. 4. Even if the "focus" of Section 2703 is privacy, Congress cannot have intended to give *greater* privacy protections to foreign nationals and those Americans falsely claiming to reside abroad, while engaged in violations of U.S. criminal laws, than to American citizens at home—indeed, any suggestion to the contrary is absurd. Moreover, even as to those first two favored categories of users, their privacy protection is only as strong as Microsoft's desire to protect it—should Microsoft decide for business reasons, or any reason, or no reason, to store the relevant content in the United States, even Microsoft concedes that neither the subscriber nor Microsoft would have a basis to object to Microsoft disclosing the information pursuant to a validly obtained Section 2703 warrant.

Finally, advancing the clear law enforcement mission of Section 2703 does not run afoul of the extraterritoriality concerns identified by the Panel. Insofar as the presumption against extraterritoriality is meant "[m]ost notably … to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries," *RJR*, 136 S. Ct. at 2100, that concern is substantially muted here, where the entity availing itself of Section 2703 is the executive branch of the federal Government—the branch primarily charged with conducting the nation's foreign relations. The United States Government is well-suited to deciding, given the facts and circumstances of a given case, whether the possibility of international friction is outweighed by the law enforcement need to obtain the information. When the United States decides to seek a Section 2703 warrant for information that may be stored abroad, it takes into account the possibility of

"unintended clashes," *Kiobel* v. *Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013), and "unreasonable interference," *F. Hoffman-La Roche Ltd.* v. *Empagran S.A.*, 542 U.S. 155, 164 (2004), with other countries. Thus, unlike litigation between private parties, which presents a heightened risk of creating international tension that the federal government cannot easily control, *see, e.g.*, *RJR*, 136 S. Ct. at 2106, the same concerns are substantially less pronounced where, as here, the Government itself is a party to the proceedings.

CONCLUSION

The petition for panel rehearing or rehearing *en banc* should be granted

Dated: New York, New York
October 13, 2016

Respectfully submitted,

PREET BHARARA,
United States Attorney for the Southern District of New York,
Attorney for the United States of America.

TIMOTHY HOWARD,
MARGARET GARNETT,
Assistant United States Attorneys,
Of Counsel.

CERTIFICATE OF COMPLIANCE

The undersigned counsel hereby certifies that this brief exceeds the page limits set by Rules 35(b)(2) and 40(b) of the Federal Rules of Appellate Procedure, but is within the 21-page limit for which the Government is seeking permission in a motion being filed simultaneously with this petition.

PREET BHARARA,
United States Attorney for the Southern District of New York

By: MARGARET GARNETT,
Assistant United States Attorney

ADDENDUM