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 Second Circuit Court of Appeals

BRIEF OF INTERNETLAB LAW AND TECHNOLOGY CENTER AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENT

AMY NEUHARDT
Counsel of Record
JESSICA PHILLIPS
ISRA BHATTY
BIBEANE METSCH
BOIES SCHILLER FLEXNER LLP
1401 New York Avenue, NW
Washington, D.C. 20005
(202) 237-2727
aneuhardt@bsfllp.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF APPENDICES

TABLE OF AUTHORITIES

Statutes

Foreign Statutes

Page(s)

Rules

Treaties

Other Authorities

QUESTION PRESENTED

Whether a United States provider of email services must comply with a probable-cause-based warrant issued under 18 U.S.C. § 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad.

INTEREST OF AMICUS CURIAE[1]

InternetLab Law and Technology Center ("InternetLab") is an independent research center located in Brazil that aims to foster academic debate on issues involving law and technology, and in particular, on internet policy. It was founded in the wake of the 2014 enactment of Brazil's landmark internet legal framework, the Marco Civil da Internet, Lei No. [Law No.] 12.965, de 23 Abril de 2014, Col. Leis Rep. Fed. Brasil ("Marco Civil," or "MCI"), which recognized a strong individual right to privacy in electronic communications and provided means for law enforcement to access and obtain internet users' data and communications.

At the time that this milestone law was enacted, it was apparent to the founders of InternetLab that there was a lack of understanding and dialogue between advocates of civil liberties, the private technology industry, and the world of law enforcement. InternetLab's mission has been to mediate the debate and build bridges of dialogue between these different sectors.

InternetLab generates and disseminates information on these subjects and collaborates with a network of scholars, researchers, students, entrepreneurs, and both private and public institutions.

---

[1] Pursuant to Supreme Court Rule 37.3(a), InternetLab certifies that all parties have consented to the filing of this brief. Pursuant to Rule 37.6, InternetLab certifies that no counsel for a party authored this brief in whole or in part, and no persons other than InternetLab or its counsel made a monetary contribution to its preparation or submission.

It has participated in more than ten public hearings in the Brazilian National Congress with respect to these issues and has contributed to the work of the Brazilian Federal Supreme Court, Federal Prosecutors Office, Ministry of Justice, Public Defender's Office, and the Court of Justice of the State of São Paulo. InternetLab has spoken regarding these issues at events in more than fifteen countries and has been cited more than two hundred times by national and international media.

InternetLab's interest in this case is two-fold. First, InternetLab has devoted substantial time and effort to furthering the study of and discussion regarding global cross-border law enforcement access to user data and communications, including mutual legal assistance treaties ("MLATs").[2] These treaties have the force of law and, at least in the case of those entered into by the United States, generally were consented to by both the executive

---

[2] *See, e.g.*, Dennys Antonialli & Jacqueline de Souza Abreu, *State Surveillance of Communications in Brazil and the Protection of Fundamental Rights*, Necessary & Proportionate, *available at* https://necessaryandproportionate.org/country-reports/brazil (last visited Jan. 17, 2018); *see also* InternetLab, *Videos of the International Conference On Fundamental Rights and Criminal Procedure in the Digital Age* (Aug. 15, 2017), http://www.internetlab.org.br/en/privacy-and-surveillance/videos-of-the-i-international-congress-of-fundamental-rights-and-criminal-process-in-the-digital-age/; InternetLab, *Reforma do MLAT entre privacidade e eficiência*: *Greg Nojeim, Center for Democracy and Technology*, YouTube (Aug. 2, 2017), https://www.youtube.com/watch?v=0AwSGbGXgr0.

and legislative branches of government.[3] In the case of warrants issued pursuant to Section 2703 of the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq*. ("SCA"), that seek data located in a country with which the United States has entered an MLAT, the existence of those MLATs covering the same data must be considered in determining the extraterritorial application of warrants seeking production of data abroad.

MLATs also are a continually developing area of the law that with proper reform driven by legislative and executive policymakers in the United States and abroad, can resolve many of the concerns raised by the United States and *amici curiae* in this case.

Second, InternetLab has an interest in furthering dialogue regarding the legal standards that govern access to information held in Brazil or oth-

---

[3] *See* T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, Federal Judicial Center, (2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf ("MLATs are legally binding negotiated commitments. . . . An MLAT is negotiated by the U.S. Department of Justice in cooperation with the U.S. Department of State. The Secretary of State formally submits the proposed MLAT, typically together with a report detailing the function and purposes of the MLAT's key provisions, to the President of the United States for transmittal to the U.S. Senate. Following the advice and consent of the Senate, the President signs the treaty and directs the Secretary of State to take the actions necessary for the treaty to enter into force. Once signatory countries have complied with entry-into-force provisions, the MLAT becomes binding under international law.").

erwise on behalf of Brazilians and Brazilian entities. Certain *amici curiae* already have provided the Court with information regarding the extraterritorial legal and practical impact of the position taken by the United States with respect to seeking data located in Ireland.[4] But the conflicts raised by the warrant to Microsoft here are not unique to Ireland.

Because of the large number of Brazilian citizens served by United States service providers, and Brazil's aggressive enforcement of judicial orders directing United States internet service providers to produce private communications located outside of Brazil, a scenario analogous to that presented to the Court in this case may well arise in the near future that will directly highlight the intersection of the laws of the United States and Brazil rather than those of the United States and Ireland. To fully understand the extraterritorial application of warrants such as those issued to Microsoft in the present case, it is useful for this Court to understand the interaction of the laws of the United States and Brazil with respect to these issues.

---

[4] *See* Brief for Ireland as *Amicus Curiae* in Support of Neither Party, *United States v. Microsoft*, (2017) (No. 17-2); Brief for the Government of the United Kingdom of Great Britain and Northern Ireland as *Amicus Curiae* in Support of Neither Party, *United States v. Microsoft*, (2017) (No. 17-2); Brief for the European Commission on Behalf of the European Union as *Amicus Curiae* in Support of Neither Party, *United States v. Microsoft*, (2017) (No. 17-2).

SUMMARY OF ARGUMENT

This case concerns whether Section 2703(b)(1)(A) of the SCA, which permits a state or federal government entity to force a provider of electronic communications to produce private customer communications—without notice to the customer—upon issuance of a valid warrant, has an extraterritorial application when those private communications are located abroad.

I. Section 2703(b)(1)(A) of the SCA should be found to have an extraterritorial application where the communications sought by a warrant issued pursuant to that provision are located in a country with which the United States has entered an MLAT. Those treaties, including the U.S.-Ireland MLAT specifically at issue in this case and the U.S.-Brazil MLAT potentially at issue in future cases, set forth mechanisms for obtaining evidence located in the other country such as the customer communications sought from Microsoft here. The existence of these treaties demonstrates official recognition by the United States of the extraterritorial application of any effort by the United States to seize items held in those countries. That official recognition should not be disregarded when considering the extraterritorial application of warrants such as the one used in this case, despite the concerns expressed by the United States regarding the efficacy of the MLAT process.

II. Section 2703(b)(1)(A) of the SCA also should be found to have an extraterritorial application where the communications sought by the warrant are the subject of dual jurisdiction with another country whose laws conflict with those of the

United States with respect to the relevant communications. Such conflict is not limited to those identified by other *amici curiae* with respect to the specific warrant here. Brazil is one of the largest consumers of internet services in the world, and is a prolific user of United States technology services. The experiences of those service providers in Brazil in recent years have revealed a concrete conflict between Brazilian law and the SCA with respect to law enforcements requests for private electronic communications. Regardless of whether production of such communications physically occurs within the United States, the act of complying with a warrant for such data can put a United States service provider directly in conflict with foreign law. This Court should find that when compliance with a warrant issued under Section 2703(b)(1)(A) of the SCA potentially subjects the recipient of the warrant to sanctions under foreign law, the warrant has extraterritorial application.

III. The parties and *amici curiae* have identified policy issues related to the merits and efficacy of using a warrant procedure such as that set forth in the SCA to obtain data located abroad. This Court need not address those policy questions to determine the narrow question of whether the warrant issued to Microsoft here has extraterritorial application. Rather, these policy issues are best resolved through reform of the current MLAT system, not through the judiciary or through attempts to rehabilitate the SCA and similar laws in other countries. Many currently proposed reforms to the MLAT system would resolve specific problems identified by the parties here, and would do so with the benefit of consultation and agreement between in-

ternational governments, as well as executive and legislative approval of such policy measures.

ARGUMENT

I. WHERE A WARRANT ISSUED PURSUANT TO SECTION 2703(B)(1)(A) OF THE SCA SEEKS ELECTRONIC COMMUNICATIONS LOCATED IN A COUNTRY WITH WHICH THE UNITED STATES HAS ENTERED AN MLAT, THE WARRANT HAS EXTRATERRITORIAL APPLICATION

The United States argues that the warrant issued to Microsoft here necessarily has domestic application because the conduct of gathering and releasing the private communications at issue could physically be accomplished by persons who never leave the United States. *See, e.g.*, Pet. Br. at 25. In support of this argument, the United States engages in a lengthy discussion of whether extraterritorial application should be judged by reference to the entirety of the SCA or to only Section 2703. *Id.* at 18-25.

InternetLab takes no position regarding the proper parsing of the SCA when considered in isolation. It suggests, however, that the SCA cannot be considered in isolation. Rather, the question whether the warrant at issue in this case has extraterritorial application can be answered only with reference to *all* directly applicable United States law, including MLATs specific to evidence located in the country in question.

In this case, the U.S.-Ireland MLAT—signed by the United States and ratified by the United States Senate after enactment of the Stored Communica-

tions Act in 1986[5]—specifically provides that "The Parties shall provide mutual assistance . . . in connection with the investigation, prosecution, and prevention of offenses, and in proceedings related to criminal matters." Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Ireland, Jan. 18, 2001, T.I.A.S. No. 13137 [hereinafter U.S.-Ireland MLAT] art. 1(1).[6] The treaty further includes spe-

---

[5] Examples of other MLATs entered into by the United States after the enactment of the SCA include MLATs with Argentina, Mexico, Thailand, Spain, South Korea, the Philippines, and the United Kingdom. *See* Treaty Between the Government of the United States of America and the Government of the Republic of Argentina on Mutual Legal Assistance in Criminal Matters, Dec. 4, 1990, S. Treaty Doc. No. 102-18 (1991); Treaty on Cooperation Between The United States of America and the United Mexican States, Dec. 9, 1987, S. Treaty Doc. No. 100-13; Treaty Between Thailand and the United States of America on Mutual Assistance in Criminal Matters, Mar. 19, 1986, S. Treaty Doc. No. 100-18; Treaty with Spain on Mutual Legal Assistance in Criminal Matters, November 20, 1990, S. Treaty Doc. No. 102-21 (1990); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-S. Kor., Nov. 23, 1993, S. Treaty Doc. No. 104-1 (1995); Treaty Between the Government of the Republic of the Philippines and the United States of America on Mutual Legal Assistance in Criminal Matters, Nov. 13, 1994, S. Treaty Doc. 104-18; Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Mutual Legal Assistance on Criminal Matters, Jan. 6, 1994, S. Treaty Doc. 104-2 (1995).

[6] The United States and Brazil are also parties to a MLAT that, like the U.S.-Ireland MLAT, was entered into by the United States and ratified by the United States Senate after enactment of the SCA. *See* Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Brazil, Oct. 14, 1997, S. Treaty Doc. No. 105-42 [hereinafter U.S.-Brazil MLAT]. Under the U.S.-

cific provisions for "search, seizure and delivery of any item to the Requesting Party if the request includes the information justifying such action under the laws of the Requested Party and it is carried out in accordance with the laws of that Party." *Id.* art. 14(1). That is, both Ireland and the United States have agreed to assist each other in criminal matters with respect to the search and seizure of "any item" so long as the search is legal under the Requesting Party's law, following the procedures set forth in the MLAT, and respecting the Requested Party's law. *Id.* Although the United States here questions the efficacy of the U.S.-Ireland MLAT for obtaining evidence in a timely manner,[7] there is no serious dispute that the U.S.-Ireland MLAT could have been used to obtain the communications sought. *Id.*[8]

Brazil MLAT, both countries are obligated to provide mutual assistance "in connection with the investigation, prosecution, and prevention of offenses, and in proceedings related to criminal matters," *id*. art. 1 (1), including "providing documents, records, and items," *id*. art. 1(2)(b).

7 Pet. Br. at 44-45.

8 In its submission as *amicus curiae*, Ireland reiterated that it "considers that the procedures provided for in [the U.S.-Ireland MLAT] represent the appropriate means to address requests such as those which are the object of the warrant in this case" and noted that "Ireland remains ready to consider, as expeditiously as possible, a request under that Treaty, if and when it be made." Brief for Ireland as *Amicus Curiae* in Support of Neither Party, *United States v. Microsoft*, (2017), (No. 17-2), at 3.

InternetLab does not argue here that as a matter of current United States law, use of the U.S.-Ireland MLAT is mandatory in this matter or that use of the existing U.S.-Brazil MLAT is mandatory in cases presenting warrants between those two countries. Rather, InternetLab argues that the very existence of these MLATs—signed and ratified after the enactment of the SCA—demonstrates official recognition by the United States of the extraterritorial application of any effort by the United States to obtain evidence held in one of those countries.[9]

Giving weight to the existence of a directly applicable MLAT in this case is consistent with this Court's jurisprudence on determining the extraterritoriality of statutes. For example, in *Morrison v. National Australia Bank, Ltd.*, 561 U.S. 247 (2010), which addressed the extraterritorial application of Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act"), the Court looked not only to that statute, but also to the language of the Securities Act of 1933 ("Securities Act"). *Id.* at 268-69. The Court explained that "[t]he same focus on domestic transactions" evident in the Securities Act provided further evidence of the focus on domestic transactions in the Exchange Act. *Id.* at 268. Although the Court noted in its comparison that the Securities

---

[9] InternetLab also submits that the decision of the United States to enter into MLATs with more than sixty countries reflects official recognition by the United States of the extraterritorial impact of efforts to obtain evidence in any foreign country.

Act was "enacted by the same Congress as the Exchange Act, and formed part of the same comprehensive regulation of securities trading," *id.*, the fact that the U.S.-Ireland MLAT was not ratified by the same Congress as the one that passed the SCA is of no moment here. The President that signed the U.S.-Ireland MLAT and the Senate that ratified it are presumed to be aware of the existence of the SCA at the time they did so. *See, e.g., Mississippi ex rel. Hood v. AU Optronics Corp.*, 134 S. Ct. 736, 742 (2014) ("[W]e presume that Congress is aware of existing law when it passes legislation.") (internal quotation marks omitted). They nonetheless recognized in a treaty with the force of United States law that efforts by the United States to seize items held in another country have extraterritorial application.[10]

This Court's decision in *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa*, 482 U.S. 522 (1987), also is directly on point. There, the Court considered the interaction between United States Federal Rules of Civil Procedure and the Hague Convention on the Taking of Evidence Abroad in

---

[10] Similarly, in *RJR Nabisco, Inc. v. European Community,* 136 S. Ct. 2090 (2016), the Court compared the statute providing a private right of action under RICO to Section 4 of the Clayton Act. In making that comparison, the Court found RICO's failure to include the specific language from the Clayton Act defining "person" to include foreign entities to be strong evidence that Congress did not intend RICO to include foreign injuries. *Id.* at 2109-10.

Civil or Commercial Matters (the "Hague Convention"). As with Section 2703(b)(1)(A) of the SCA and the U.S.-Ireland MLAT in this case, in *Aérospatiale* both laws were applicable to the particular request for foreign discovery. Although the Court declined to hold that the Hague Convention is mandatory when seeking discovery from a foreign litigant to civil litigation in the United States, it acknowledged the international impact of such discovery requests and directed United States courts to pay heed to the concerns that necessarily arise from such impact. *See Aérospatiale*, 482 U.S. at 546 ("American courts should . . . take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of the nationality or the location of its operations, and for any sovereign interest expressed by a foreign state.").[11] The recognition by the *Aérospatiale* Court of the extraterritorial nature of United States civil discovery requests for documents abroad should have even more force here. The foreign defendants in *Aérospatiale* that ultimately were required to comply with discovery requests propounded under the United States Federal Rules of Civil Procedure were parties to the litigation and also plainly subject to the jurisdiction of the United States courts. *Id.* at 539-40 ("We conclude accordingly that the Hague Convention did not deprive the District

---

[11] Another *amicus curiae* has provided the Court with an analysis of the effectiveness of the guidance given by the *Aérospatiale* Court. *See* Brief for E-Discovery Institute et al. as *Amici Curiae* in Support of Neither Party, *United States v. Microsoft*, (2017), (No. 17-2) at 17.

Court of the jurisdiction it otherwise possessed to order a foreign national party before it to produce evidence physically located within a signatory nation."); *id.* at 540 ("[T]he Hague Convention does not divest the District Court of jurisdiction to order discovery under the Federal Rules of Civil Procedure. . . ."). They also were required to produce only their own documents located abroad. *Id.* at 525-26, 547.

Here, the warrant does not seek Microsoft's own communications, unlike the records at issue in *Morrison* or in *In re Marc Rich & Co. v. United States*, 707 F.2d 663 (2d Cir. 1983), *cert. denied*, 463 U.S. 1215 (1983). Rather, it requires Microsoft to produce the private communications of a third-party customer.[12] Because the United States chose to proceed under 18 U.S.C. § 2703(b)(1)(A), rather than under one of the provisions of 18 U.S.C. § 2703 that requires notice to the third-party customer,[13]

---

[12] The record is devoid of information regarding that customer's citizenship or residency. *See Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 209 (2d Cir. 2016) ("As to the citizenship of the customer whose e-mail content was sought, the record is silent."), *cert. granted sub nom. United States v. Microsoft Corp.*, 138 S. Ct. 356 (2017); *id.* at 220 ("The record is silent regarding the citizenship and location of the customer."); *id.* at 229 ("We do not know, on this record, whether the customer whose emails were sought by the government is or is not a United States citizen or resident.") (Lynch, J. concurring). Given this uncertainty about the subscriber's connections to the United States, it is unclear whether he or she can even be subject to the jurisdiction of United States courts.

[13] *See* 18 U.S.C. § 2703(b)(1)(B).

that customer—unlike the parties in *Aérospatiale, Morrison* or *Marc Rich*—is unable to assert directly his or her own privacy and jurisdictional interests. Consequently, the foreign sovereign's interest in asserting those rights on behalf of its residents and citizens is even greater than in *Aérospatiale*. The existence (and magnification) of the international impact recognized by this Court in *Aérospatiale* should itself be conclusive evidence of the extraterritorial application of 18 U.S.C. § 2703(b)(1)(A) in this case.

II. WHERE THE ELECTRONIC COMMUNICATIONS SOUGHT BY A WARRANT ISSUED PURSUANT TO SECTION 2703 (B)(1)(A) OF THE SCA ARE SUBJECT TO DUAL JURISDICTION WITH ANOTHER COUNTRY WHOSE LAWS CONFLICT WITH THOSE OF THE UNITED STATES WITH RESPECT TO THOSE COMMUNICATIONS, THE WARRANT HAS EXTRATERRITORIAL APPLICATION

Section 2703(b)(1)(A) of the SCA also should be found to have an extraterritorial application where the communications sought by the warrant are the subject of dual jurisdiction with another country whose laws conflict with those of the United States with respect to those communications. Other *amici curiae* have identified such conflicts specific to the warrant at issue in this case,[14] but potential for

---

[14] *See* Brief for Ireland as *Amicus Curiae* in Support of Neither Party, *United States v. Microsoft*, (2017) (No. 17-2) at 3; Brief for the European Commission as *Amicus Curiae* in Support of

such conflict is not limited to the specific circumstances of the warrant here.

A. Brazil, One Of The Largest Global Internet Markets, Has Aggressively Enforced Brazilian Law Against United States Internet Service Providers Confronted With Judicial Orders To Turn Over Private Electronic Communications Covered By The SCA

Brazil is one of the largest markets for internet use worldwide. A survey conducted in 2016 by the Brazilian Internet Steering Committee revealed that nearly 108 million Brazilians used the internet in 2016.[15] Moreover, Brazilian internet users' interaction with United States-based technology companies is particularly robust. American technology companies including Facebook, YouTube, Google, and Microsoft have millions of users in Brazil. As of July 2017, for example, Brazil had the third-largest number of Facebook users, second only to India and the United States,[16] and the second-

---

Neither Party, *United States v. Microsoft*, (2017) (No. 17-2) at 5.

[15] *See*, *e.g.,* Brazilian Internet Steering Committee, 2016 ICT Households Survey 164 ("Currently there are 107.9 million Internet users in Brazil.") (2017), http://cetic.br/media/docs/publicacoes/2/TIC_DOM_2016_LivroEletronico.pdf.

[16] Statista.com, *Facebook Users By Country* (extrapolated from data released by Facebook), https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/ (last visited Jan. 16, 2018).

largest number of YouTube users, second only to the United States.[17] In a December 2016 survey of 1801 Brazilians, 92% of respondents with a cell phone or smart phone stated that they used WhatsApp, 79% of respondents used Facebook, and 64% of respondents used YouTube.[18]

1. *Brazil Provides Specific Privacy Guarantees To Users Of The Internet*

As does the United States Constitution, common law and statutory law, the Brazilian Constitution recognizes a strong right to privacy. Constituição da República Federativa do Brasil de 1988 [Constitution of the Federative Republic of Brazil] art. 5(X), (XII). In addition, in 2014, Brazil enacted the Marco Civil, which "establishes the principles, guarantees, rights and obligations for the use of Internet in Brazil. . . . " MCI art. 1.[19] This law makes

---

[17] Statista.com, *Leading Countries Based On Number Of Monthly Active YouTube Users As Of 1st Quarter 2016 (In Millions)*, https://www.statista.com/statistics/280685/number-of-monthly-unique-youtube-users/ (last visited Jan. 16, 2018).

[18] Datafolha, *Hábitos de Uso de Aplicativos, População brasileira, 13 anos ou mais [App Use Habits, Brazilian Population, 13 Or Older]* 10 (Dec. 2016), http://media.folha.uol.com.br/datafolha/2017/01/27/da39a3ee5e6b4b0d3255bfef95601890afd80709.pdf; *see also* 2016 ICT SURVEY, at 217 (Chart 4: Activities Carried Out On The Internet In The Last Three Months, by Age Group (%) (2015)).

[19] Quotations are to the English language translation of the Marco Civil distributed to all participants of the Global Multistakeholder Meeting on the Future of Internet Governance. *See* Public Knowledge, *Marco Civil English Version* (May 27, 2014), https://www.publicknowledge.org/documents/marco-civil-english-version.

clear Brazil's recognition of the human right to privacy specifically with respect to internet use, including "protection of privacy" and "protection of personal data, pursuant to law." *Id*. art. 3(II), (III). Consistent with this recognition, Chapter II of the Marco Civil provides that "the access to the internet is essential to the exercise of citizenship, and the following rights are guaranteed to the users:

> II – inviolability and secrecy of the flow of user's communications through the Internet, except by court order, as provided by law;
>
> III – inviolability and secrecy of user's stored private communications, except upon a court order.
>
> …
>
> VII – non-disclosure to third parties of users' personal data, including connection records and records of access to internet applications, unless with express, free and informed consent or in accordance with the cases provided by law.

Id. art. 7(II), (III), (VII).

2. *The Marco Civil, Like Section 2702 Of The SCA, Prohibits Disclosure Of Customers' Private Communications Absent Appropriate Legal Process*

To protect these guarantees of privacy, the Marco Civil provides, "The content of private communications may only be made available by court order, in the cases and in the manner established

by law, and in compliance with items II and III of art. 7." *Id.* art. 10 § 2. Violation of the prohibition against disclosure of protected electronic communications can result in severe penalties including a fine of up to 10% of the gross income of the company in the previous fiscal year and temporary or permanent suspension of activities within the country. *Id.* art. 12(II), (III).

Responsibility for ensuring protection of these guarantees is laid squarely upon internet service providers such as Microsoft:

> In any operation of collection, storage, retention and treating of personal data or communications data by connection providers and internet applications providers where, at least one of these acts takes place in the national territory, the Brazilian law must be mandatorily respected, including in regard [to] the rights to privacy, to protection of personal data, and to secrecy of private communications and logs.

Id., art. 11. This responsibility extends not only to data collected in Brazil, but also to "the content of the communications in which at least one of the terminals is placed in Brazil" ("Brazilian Data"). *Id.* art. 11, § 1.[20] A foreign company is subject to

---

[20] As one report on the then-new Marco Civil explained:

> Under the new provisions, log data and private communications may not be disclosed absent a Brazilian court order. According to the terms of the law, Brazilian law must be followed for this

these provisions—and the penalties set forth in the Marco Civil—if the company provides services in Brazil or has but a single employee in the country. *Id.* art. 11 § 2 ("Art. 11 applies even if the activities are carried out by a legal entity placed abroad, provided that it offers services to the Brazilian public or at least one member of the same economic group is established in Brazil.").

Consistent with the exception to liability for disclosure pursuant to court order, *see id.* art. 10 § 2; *id.* art. 7(II) and (III), the Marco Civil provides a mechanism for obtaining a judicial order for electronic records. Through this and the previously discussed provisions of the Marco Civil, a United States internet service provider with a single employee in Brazil can be issued a court order to produce customers' private communications under the Marco Civil—even if those communications are lo-

---

> data even if the data is stored abroad, if one of the following occurs in Brazil: a) collection, storage or processing of data; or b) one end of personal communications. This requirement is explained to apply where data or communications are collected in Brazil by virtue of one of the computers or devices being located in Brazil. Further, it applies even if the actions are performed by a legal entity domiciled abroad, if a public service is offered in Brazil or a member of the same corporate family owns property in Brazil.

Elizabeth Banker, *New Brazil "Bill of Rights" Takes Effect at End of June*, ZwillGen Blog, Law Across The Wire and Into the Cloud (June 17, 2014), https://blog.zwillgen.com/2014/06/17/going-brazil-just-world-cup/.

cated in the United States or were made by only United States citizens—so long as the communications are considered Brazilian Data (*i.e.*, communications made with one terminal located in Brazil).

These provisions of the Marco Civil are similar to the protections and obligations provided in Sections 2702 and 2703 of the SCA. Section 2702 prohibits persons or entities providing an electronic communication service to the public from divulging communications stored, carried or maintained by the service except under limited circumstances, including the methods set forth in Section 2703 for a warrant such as that at issue in this case. 18 U.S.C. §§ 2702, 2703.

B. The Practical Experiences Of United States Internet Service Providers Doing Business In Brazil Demonstrate How A Global Internet Service Provider Responding To Law Enforcement Requests Can Be Penalized Under Conflicting International Laws

The experiences of United States internet service providers with at least one employee in Brazil illustrate how the SCA can place international electronic service providers in the untenable position of choosing between compliance with United States law or a foreign country's law. Where the application of United States law creates such a conflict or potential conflict, that application of the law should be considered extraterritorial.

As discussed above, foreign internet service providers are subject to the Marco Civil if they provide services in Brazil or have a single employee based in Brazil. MCI art. 11 § 2. Such companies are

subject to warrants issued by Brazilian courts as well as to the penalties for unlawful disclosure set forth in Article 12 of the Marco Civil.

Where a United States-based company is subject to Brazilian law with respect to electronic communications, it also may be bound by the SCA. In such circumstances, law enforcement requests for communications covered by both laws can put the company in the position of conflicting obligations in each jurisdiction.

This conflict is not merely speculative for United States companies operating in Brazil. In 2015, a Brazilian court fined Microsoft's local subsidiary and arrested and criminally charged a Microsoft official in Brazil for violating a Brazilian court order to turn over Brazilian Data stored in the United States.[21] Similarly, in 2016, a Brazilian court fined Facebook 1.38 million Real for violating a court order to disclose foreign-stored data to Brazilian au-

---

[21] *See International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Comm. On the Judiciary*, 114th Cong. 3 (2016) (written statement of Brad Smith, President and Chief Legal Officer of Microsoft), https://judiciary.house.gov/wp-content/uploads/2016/02/brad-smith-testimony.pdf ("Instead, when we have refused to violate U.S. law by complying with unilateral and extraterritorial Brazilian orders, government authorities in Brazil have levied fines against our local subsidiary and in one case even arrested and criminally charged a local employee."); *see also* Brad Smith, *In the Cloud We Trust*, Microsoft, https://news.microsoft.com/stories/inthecloudwetrust/ (last visited Jan. 16, 2018.

thorities pursuant to a drug investigation.[22] Facebook's regional vice president was later criminally charged for non-compliance with the court order.[23]

---

[22] *See* Reuters, *Ministério Público Defende Correção Em Multa de R$ 1,38 Mi Para Facebook* [*Public Prosecutor's Office Supports Adjustment of R$1.38 Million Fine Applied to Facebook*] (July 2, 2017, 12:12 PM), http://link.estadao.com.br/noticias/empresas,mpf-defende-multa-superior-a-r1-38-mi-para-facebook-no-brasil,70001656255 (original and official translation attached at Appendices A and B).

[23] *See* G1 São Paulo, *Justiça abre processo contra vice do Facebook na América Latina por desobediência de ordem judicial* [*Prosecutors Go After Facebook VP in Latin America for Failure to Comply with Court Order*] (Nov. 4, 2017, 9:50 PM), https://g1.globo.com/sao-paulo/noticia/justica-abre-processo-contra-vice-do-facebook-na-america-latina-por-desobediencia-de-ordem-judicial.ghtml (original and official translation attached at Appendices C and D).

In addition, on at least three occasions, Brazilian courts have ordered telecommunications providers to block access to WhatsApp due to the failure by Facebook (as owner of WhatsApp) to turn over customer communications pursuant to a Brazilian court order. *See* Vinod Sreeharsha, *WhatsApp Is Briefly Shut Down in Brazil for a Third Time*, N.Y. Times, July 19, 2016. On one of these occasions, Facebook also was fined and had one of its officers arrested for the violations. *See* Jonathan Watts, *Brazilian Police Arrest Facebook's Latin America Vice-President*, The Guardian (Mar. 1, 2016 10:35 AM), https://www.theguardian.com/technology/2016/mar/01/brazil-police-arrest-facebook-latin-america-vice-president-diego-dzodan. In each case, Facebook has explained that it could not comply with the Brazilian court orders because WhatsApp does not store its customer communications, a situation that was not a direct conflict with the SCA. *See* Reuters, *Brazil Court Blocks Facebook Funds Over WhatsApp Dispute: Report*

The Marco Civil has provided clarity into the circumstances under which Brazilian law enforcement officers may seek information, but has not resolved the conflict with United States law. As a result, the Federação das Associações das Empresas Brasileiras de Tecnologia da Informação in Brazil (Federation of Associations of Brazilian Companies in Information Technology, or "ASSESPRO") has filed a Declaratory Action of Constitutionality in the Brazilian Federal Supreme Court seeking clarification of the obligation of Brazilian courts to apply MLATs and other Brazilian laws to Brazilian law enforcement requests for electronic communications stored by foreign companies.

In support of ASSESPRO in that action, Facebook Brazil filed a brief as *amicus curiae* attaching an affidavit by former United States Attorney General Eric Holder. *See* Affidavit of Eric Holder filed in Ação Declaratória de Constitucionalidade n. 51, Supremo Tribunal Federal (Dec. 5, 2017) [hereinafter Holder Aff.], Appendix E. In his affidavit, Mr. Holder outlines to the Brazilian Federal Supreme Court the dilemma faced by United States technology companies doing business in foreign countries, including in Brazil. Specifically, Mr. Holder explains that Section 2702 of the SCA prohibits electronic communications service providers subject to

---

(June 30, 2016 8:32 PM), https://in.reuters.com/article/brazil-facebook-whatsapp/brazil-court-blocks-facebook-funds-over-whatsapp-dispute-report-idINKCN0ZH3F4). The cases demonstrate, however, the severe penalties Brazilian courts are willing to impose on United States service providers for violations of the Marco Civil.

United States jurisdiction from disclosing the communications of their users to any other person unless one of the statute's exceptions applies. Holder Aff. ¶¶ 8, 11-13 (Appendix E at 20a, 22a-23a). He further makes clear that there is no exception for responding to a foreign law enforcement request, even where the foreign request is the result of a valid legal proceeding such as one arising from the Marco Civil, or where it relates to "non-U.S. persons." *Id.* ¶¶ 8, 15 (Appendix E at 20a, 24a). Mr. Holder also explains the penalties that a company can receive in the United States for violating the SCA.[24] *Id.* ¶ 18 (Appendix E at 26a).

Although these examples—and Mr. Holder's affidavit to the Brazilian Federal Supreme Court—all concern conflicts arising from Brazilian law enforcement requests for private electronic communications held by United States companies, the converse conflict also exists when an internet service provider subject to both United States and Brazilian law receives a warrant issued pursuant to Section 2703 of the SCA for electronic communications that qualify as Brazilian Data. Complying with such a warrant subjects the provider to the real risk of penalties in Brazil for unlawful disclosure of

---

[24] As an example to the Brazilian Court of the perils faced by a company that fails to follow Section 2702 of the SCA, Mr. Holder cites *In re Google Referrer Header Privacy Litigation,* 87 F. Supp. 3d 1122 (N.D. Cal. 2015), in which Google agreed to a settlement of $8.5 million for alleged violations of the SCA.

Brazilian Data as set forth in Article 12.[25] Because the Marco Civil is only three years old, that particular conflict has not yet arisen.[26] Given Brazilian authorities' aggressive enforcement of the Marco Civil and the prevalence of United States service providers within Brazil, however, a company confronted with such a conflict will face a serious risk no matter what action it takes.

---

[25] *See, e.g.*, Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations For U.S. Policymakers and Industry Leaders*, 2 LAWFARE RESEARCH PAPER SERIES, No. 3, July, 2014, at 18 ("While the Marco Civil was signed into law on April 23, 2014 with the most potent localization provision rescinded, one provision remained, Article 11, which deeply troubles international business interests, in that it extends the reach of Brazilian law to any Internet service in the world with Brazilian users. A firm based in the United States whose services are used by Brazilians could, for example, be penalized for adhering to its domestic data-disclosure laws if they conflict with Brazil's. Penalties include fines of up to ten percent of a firm's Brazilian revenues or even termination of the offending company's services in Brazil.").

[26] The warrant in this case was issued on December 4, 2013, prior to the enactment of the Marco Civil in 2014. Other *amici curiae* have identified other legislation regarding electronic data privacy enacted since the since the issuance of the warrant at issue in this case. *See* Brief of the Government of the Kingdom of Great Britain and Northern Ireland as *Amicus Curiae* in Support of Neither Party (2017), (No. 17-2) at 5-6 (discussing the United Kingdom's Data Retention and Investigatory Powers Act of 2014 and the Investigatory Powers Act of 2016); Brief of the European Commission on Behalf of the European Union as *Amicus Curiae* in Support of Neither Party (2017), (No. 17-2) at 2, 8-16 (discussing the European Union's General Data Production Regulation, adopted in 2016 and set to become effective in May 2018).

InternetLab identifies these potential conflicts to the Court to demonstrate that warrants such as those issued to Microsoft in this case have foreign application regardless of the location of the company or person producing the requested communications. *See, e.g.*, *Morrison*, 561 U.S. at 269 ("The probability of incompatibility with the applicable laws of other countries is so obvious that if Congress intended such foreign application 'it would have addressed the subject of conflicts with foreign laws and procedures.'") (quoting *E.E.O.C. v. Arabian Am. Oil Co.*, 499 U.S. 244, 256 (1991)*; see also RJR Nabisco., Inc. v. European Comty.,* 136 S. Ct. 2090, 2107 (2016) ("It is to say only that there is a potential for international controversy that militates against recognizing foreign-injury claims [under the RICO private right of action] without clear direction from Congress.").

As discussed more fully in Section I above, the Court's decision in *Aérospatiale*, is also instructive here. There, the Court recognized that the act of producing documents pursuant to United States law puts a party in a position of breaking the law of one country by complying with the law of another, and that in such circumstances the courts of the United States are obligated to recognize the extraterritorial impact of that production. *Aérospatiale,* 482 U.S. at 543-44. The same is true here, and this Court should recognize that Section 2703 has a foreign application when used to obtain private communications subject to dual jurisdiction with another country whose laws conflict with those of the United States with respect to those communications.

III. THE MLAT PROCESS IS THE BEST MEANS OF RESOLVING THE DIFFICULT INTERNATIONAL POLICY DECISIONS INHERENT IN LAW ENFORCEMENT REQUESTS FOR FOREIGN DATA

Rather than construing Section 2703 of the SCA to allow the United States government to reach data in violation of other sovereigns' laws, this Court should acknowledge that the difficult policy decisions implicit in United States' efforts to obtain electronic communications stored abroad are better left to other branches of government. Although some such foreign policy decisions certainly could be made by the United States Congress through revisions to the SCA, InternetLab submits that foreign relations are better served by permitting the executive branch to negotiate and execute reforms to the MLAT system that then can be ratified by the United States Senate.

A. MLATs Are Widely Used To Request Foreign Assistance In Domestic Criminal Investigations And Prosecutions And Incorporate Privacy, Due Process, And Comity Considerations

The United States has now entered into MLATs with more than sixty foreign nations and used these MLATs to target various crimes.[27] "MLATs

---

[27] *See* Hon. Virginia M. Kendall & T. Markus Funk, *The Role of Mutual Legal Assistance Treaties in Obtaining Foreign Evidence*, 40 Litigation 2, 3 (2014). Alternate means of obtaining

are shifting from an obscure specialty issue to a key component of law enforcement in our world of globalized communications and are central to international debates about the structure of the Internet."[28] They are widely used to request foreign assistance in domestic criminal investigations and prosecutions.[29] Congress also has recognized that

---

foreign evidence that still respect comity also exist. "Where there is no treaty, or where the treaty's mechanisms may be overly burdensome, a nation may still rely on principles of comity in submitting a letter rogatory to effect a cross-border data request." Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. Ann. Surv. Am. L. 687, 702 (2017). In addition, as explained in the affidavit of former U.S. Attorney General Eric Holder to the Brazilian Federal Supreme Court, the U.S. Department of Justice frequently works with foreign partners to facilitate disclosures of information under the provision of Section 2702 of the SCA excepting from its reach disclosures of private communications made "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." 18 U.S.C. § 2702(b)(8). Holder Aff. ¶ 14 ("During my term as Attorney General, I was personally involved in emergency responses of foreign countries, in which a U.S. provider disclosed information to the DOJ under the terms of the emergency exception, and the DOJ, in turn, forwarded this information to our foreign partner.") (Appendix E at 23a).

[28] Swire & Hemmings, 71 N.Y.U. Ann. Surv. Am. L. at 703.

[29] *See* Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, Harv. Nat'l. Sec. J. (Jan. 28, 2015, 1:05 PM), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/.

MLATs are critical for prosecutors to effectively combat crime. "Reflecting the realization that MLATs are now a well-worn tool in the prosecutors' toolbox, Congress [in 2009] passed the Foreign Evidence Efficiency Act, 18 U.S.C. § 3512 . . . to help streamline the MLAT process and make it easier for the United States to respond to MLAT requests . . . ."[30]

MLATs include safeguards to protect the due process and privacy rights of users whose electronic data is requested. For example, under the U.S.-Ireland MLAT at issue in this case, any requests for the "search, seizure, and delivery of any item to the Requesting Party . . . is carried out in accordance with the laws of that Party." U.S.-Ireland MLAT, art. 14(1). Similarly, under the U.S.-Brazil MLAT, "[r]equests shall be executed in accordance with the laws of the Requested State." U.S.-Brazil MLAT, art. 5(3). The "laws of that Party" or "the laws of the Requested State" will include the underlying privacy protections of the receiving country, including the country's constitution. Accordingly, any electronic data requested under these MLATs will be produced only after consideration of the due process and privacy protections of the producing country. In this way, MLATs are the tool for foreign productions that is most protective of the due process and privacy considerations of the receiving country. In addition, because MLATs are the product of negotiations between nations, MLATs are the

---

[30] Kendall & Funk, 40 Litigation at 2 (internal quotation marks omitted).

tool for foreign productions that is most consistent with notions of comity and respect for foreign sovereigns.

B. The Current Challenges Of The MLAT Process Can Be Cured Through MLAT Reform

The United States and various states attorneys general as *amicus curiae* argue that if Section 2703 is interpreted to prohibit warrants for electronic data located abroad, the government will lose a critical means of accessing evidence necessary for law enforcement and national security.[31] The answer to this problem, however, is not to interpret Section 2703 of the SCA to permit warrants for foreign data. Rather, the foreign and domestic policy issues raised by requests for information to and from foreign countries are best resolved through reform of the current MLAT system, not through the judiciary.[32]

---

[31] Pet. Br. at 44 ("Without the Section 2703 warrant process, the government lacks an equally effective means of accessing electronic data critical to law enforcement and national security."); Brief for State of Vermont et al. as *Amici Curiae* in Support of Petitioner, *United States v. Microsoft*, (2017), (No. 17-2) at 2 ("Law enforcement agencies in Amici States, like their federal counterparts, routinely use this essential investigative tool in a wide variety of important criminal investigations around the country.") (internal quotation marks omitted).

[32] *See, e.g.*, *Kiobel v. Royal Dutch Petroleum Co.,* 569 U.S. 108, 124 (2013) ("The presumption against extraterritoriality guards against our courts triggering such serious foreign policy consequences, and instead defers such decisions, quite appropriately so, to the political branches."). Policy considera-

Many currently proposed reforms to the MLAT system would resolve the specific problems identified by the parties and *amici curiae* here and would do so with the benefit of consultation and agreement between international governments, as well as U.S. executive and legislative approval of such policy measures.

The United States complains that the alternative MLAT process is ineffective because it is "slow and uncertain." Pet. Br. at 44. Proponents of reform agree, however, that one key requirement for any reform effort is increased efficiency. As explained in a report on MLAT reform for the Global Network Initiative:

> The process for requesting and providing mutual legal assistance must be made more efficient. Government A should not have to wait longer than 30 days for a complete response from Government B about their request for data, except (a) where additional time is needed to evaluate the potential human rights implications of the MLA request or (b) for particularly complex requests. Efficiency is critical so that law enforcement sees MLA as the best way to access data across jurisdictions,

---

tions also could be addressed through attempts by Congress to rehabilitate the SCA, but MLATs are a better vehicle for ensuring proper consideration of the privacy, due process, and comity implications of obtaining private electronic communications located abroad.

> rather than demanding data localization or attempting to apply local law extraterritorially.[33]

To the extent that a thirty-day response time is too long for some law enforcement needs, exceptions to any authorization requirement could be permitted in cases of true emergency, such as when there is danger of death or serious injury.[34]

Other proposals for MLAT reform that target delay and administrative hurdles include:

> (1) increase[ing] resources to the Department of Justice's Office of International Affairs (OIA); (2) streamlin[ing] the process, by minimizing the number of steps and reducing the amount of time required to complete steps where possible; (3) improve[ing] transparency, such as by creating an online

---

[33] Andrew K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, Global Network Initiative 7 (Jan. 2015), https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf [hereinafter *Data Beyond Borders*].

[34] *See, e.g.*, Jennifer Daskal & Andrew K. Woods, *Cross-Border Data Requests: A Proposed Framework*, LawFare (Nov. 24, 2015, 8:00 AM), https://www.lawfareblog.com/cross-border-data-requests-proposed-framework ("Emergencies: Exceptions to the authorization requirement are permitted in situations of true emergency—when there is danger of death or serious bodily injury and there is an immediate need that makes compliance with the authorization requirement impracticable.").

> MLA[T] submission form; and (4) promot[ing] the use of MLA[Ts] globally and demonstrate the U.S. government's commitment to an effective process.[35]

MLAT reform also could resolve the potential problem identified by the United States here of using the MLAT process where data is rapidly moving between jurisdictions, or even split into multiple parts located in multiple jurisdictions.[36] As explained by one proponent of MLAT reform, there is nothing unique about the mobility of data. "[F]or as long as global trade has existed, people have been commingling and moving their assets in and out of different jurisdictions and courts have man-

---

[35] Swire & Hemmings, 71 N.Y.U. Ann. Surv. Am. L. at 716. President Barack Obama's Review Group on Intelligence and Communication Technologies identified these same areas for improvement in a report published in 2013. *See* Richard A. Clarke et. al., *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* at 226-229, OBAMA WHITE HOUSE ARCHIVES (Dec. 12, 2013) https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[36] The United States argues that interpreting Section 2703 to permit warrants seeking foreign data is critical "[b]ecause Google constantly moves data around the world, the location of the data at any given moment in time is difficult or impossible to ascertain—a problem compounded by splitting a single email into separate pieces of data." Pet. Br. at 45.

aged to adapt their old, territorial rules to assets that cross territories."[37]

To minimize administrative delay, MLAT reform advocates also have suggested requiring countries to "develop an electronic system for submitting, managing, and responding to MLA[T] requests."[38] Executive branch support of MLATs could come from prioritizing responses to MLATs and providing additional staff to evaluate and process outgoing requests for MLAT.[39] The United States has already started to implement such reforms. *See* Holder Aff. at ¶ 35 (discussing Department of Justice actions in 2015 and 2016 to implement "a more centralized system to process requests and reduce response times," enhance "technological resources," and support "training efforts to assist key foreign partners in submitting MLAT requests that comply with their MLAT treaties and with U.S. law.") (Appendix E at 34a).

As a potential substitute for the current MLAT process, in July 2016, the U.S. Department of Justice proposed legislation to address issues related to

---

[37] Andrew K. Woods, *Against Data Exceptionalism*, 68 Stan. L. Rev. 729, 756 (2016); *see also id.* at 758 ("But mobility, as a feature of an asset class, is hardly unique to data. Consider money, which can be wired from one location to another in an instant. Courts have little trouble determining the location of money for the purposes of asserting jurisdiction over the asset. The same is true for nearly everything, given the speed of modern communications and transportation networks.").

[38] Woods, *Data Beyond Borders* at 2, 7-8.

[39] *Id.* at 2.

transferring of cross-border data.[40] The proposed reciprocal legislation would have "permit[ted] UK law enforcement to make direct requests to US-based providers for emails and live chats that are sought in the investigation of serious crime."[41] Requests could be made only with respect to noncitizen targets outside the United States. For data belonging to a US citizen or legal permanent resident, wherever located, or to any person physically located in the United States, regardless of citizenship, the MLAT process would remain the default.[42]

This proposed legislation sought to move away from the treaty-based MLAT system in certain instances and instead require "lighter touch" bilateral agreements between the United States and the United Kingdom and eventually, other countries.[43]

---

[40] *See* U.S. Dep't of Justice, Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism (2016).

[41] Jennifer Daskal & Andrew K. Woods, *Congress Should Embrace the DOJ's Cross-Border Data Fix* at 3, JUST SECURITY (Aug. 1, 2016) https://www.justsecurity.org/32213/congress-embrace-dojs-cross-border-data-fix/ [hereinafter *Cross-Border Data Fix*].

[42] *Id.*

[43] Tiffany Lin & Mailyn Fidler, *Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement* at 2, Berkman Klein Center for Internet & Society (Sept. 2017), https://dash.harvard.edu/bitstream/handle/1/33867385/2017-09_berklett.pdf?sequence=1. Such reciprocal agreements could be possible only with foreign countries that meet neces-

Although this proposed legislation was not enacted, its submission demonstrates that Congress has actively considered the policy implications associated with the MLAT process as recently as 2016.

Reversing the Second Circuit's decision here would allow the United States government to disregard the legal regimes of other countries and to unilaterally undermine MLAT agreements concerning foreign evidence previously ratified by the United States Senate. Such an outcome not only is contrary to this Court's precedent in *Morrison, RJR Nabisco* and *Aérospatiale,* but it also is wholly unnecessary given the robust MLAT system already in place and the many possible ways to improve it that have been proposed. MLAT reforms also are the best method for ensuring proper consideration of due process, privacy, and comity in gathering or providing foreign evidence. Such reforms also permit full consideration of the related foreign and domestic policy concerns by both the executive and legislative branches of the United States government.

* * *

CONCLUSION

This Court should affirm the judgment of the Second Circuit Court of Appeals and hold that the warrant issued to Microsoft in this matter was an improper extraterritorial application of 18 U.S.C. § 2703(b)(1)(A).

---

sary "substantive and procedural protections for privacy and civil liberties." Daskal & Woods, *Cross-Border Data Fix.*

Respectfully submitted,

AMY NEUHARDT
Counsel of Record
JESSICA PHILLIPS
ISRA BHATTY
BIBEANE METSCH
BOIES SCHILLER FLEXNER LLP
1401 New York Avenue, NW
Washington, D.C. 20005
(202) 237-2727
aneuhardt@bsfllp.com

January 18, 2018

APPENDIX

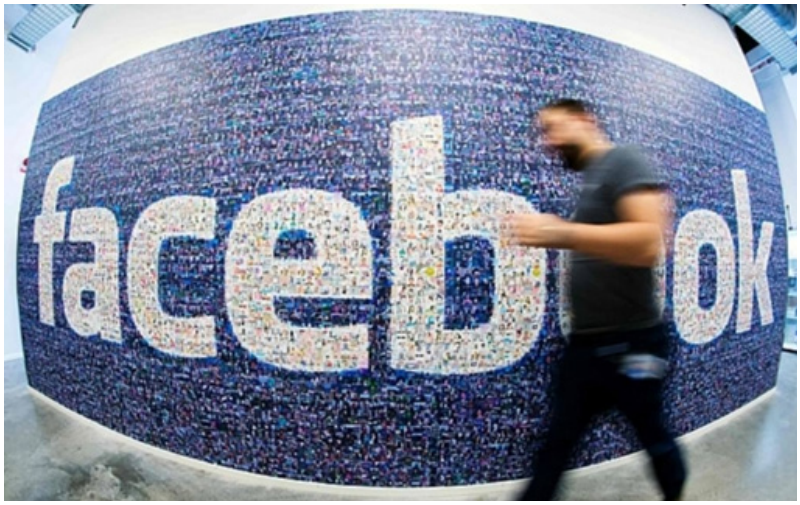
APPENDIX A — ARTICLE BY REUTERS, DATED FEBRUARY 7, 2017 (ENGLISH)

PUBLIC PROSECUTOR'S OFFICE SUPPORTS ADJUSTMENT OF R$1.38 MILLION FINE APPLIED TO FACEBOOK

The public prosecutor's office is referring to information wiretapped in February 2016; Facebook is alleged to have failed to comply with an order to release information related to persons under investigation for drug trafficking

2/7/2017 – 12:12 p.m.

By Redação Link – With Reuters



Order was issued by a court in February 2016; Facebook is alleged to have failed to comply

Appendix A

The Federal Public Prosecutor's Office (MPF) yesterday told the court that it supports a review of the R$1.38 million fine that Facebook must pay for the failure to comply with a court order from February 2016. If the Regional Federal Court for the 2nd Region, in Rio de Janeiro, accepts the argument, the amount will be adjusted with interest and monetary correction for the period between May 2016, when the fine was applied, and the hearing date for Facebook's appeal, which should be considered in the coming days.

Early last year, Facebook refused to wiretap information of Mário Jorge Carneiro dos Santos Júnior and Gabriel Ribeiro Espíndola, two suspects of international drug trafficking and conspiracy to traffic. The targets of the information disclosure request were the suspects' profiles on Facebook and the Facebook Messenger instant messaging application.

The court set the fine at R$20 thousand per day at the time, for failure to comply with the court order. After a search was conducted by the Federal Police at the company's office on May 13, 2016, the judge decided that the information could not be obtained.

Facebook alleged in the action that they were unable to provide the information required by the court because it was stored on servers abroad. According to Facebook, the only way to obtain the information would be through a request to the Justice System in the United States under MLAT, a cooperation agreement that exists between the two countries for criminal cases. In the opinion sent to the

Federal Regional Court for the 2nd Region, the MPF states that "there is no technical impediment that may justify the company's refusal to perform their legal obligations. What in fact exists is a separation imposed by a business model adopted by Facebook and a legal subterfuge based on international rules."

In response to an inquiry from Estado, Facebook informed that they "have a profound respect for the Court and is compliant with Brazilian laws." The company stated their belief that the fine is improper. "We will use the recourses guaranteed by law."

According to the Federal Regional Court (TRF–2nd Region), the MPF also opined that the daily fine should not be jointly applied to both Facebook Brazil and the employee who received the court order. For the prosecutors, the charge against the employee was filed based on a misunderstanding by the judge, who suggested that the individual subject to fines is the company's President.

Appendix A

T&T Translation Services Inc.
89-33 Pontiac Street
Queens Village, NY 11427
Tel: +1-646-827-1163
Fax: +1-516-977-3110
E-mail: yuan@transtt.com

CERTIFICATION

I, Timothy Yuan, hereby certify that I speak and write both the Portuguese and English languages; that I have translated the foregoing article published by the Estado de São Paulo newspaper on February 7, 2017, entitled "Public Prosecutor's Office Supports Adjustment of R$1.38 Million Fine Applied to Facebook," to the best of my ability; and that it is a true and correct translation to the best of my knowledge, information, and belief.

/s/	January 16, 2018
Signature	Date

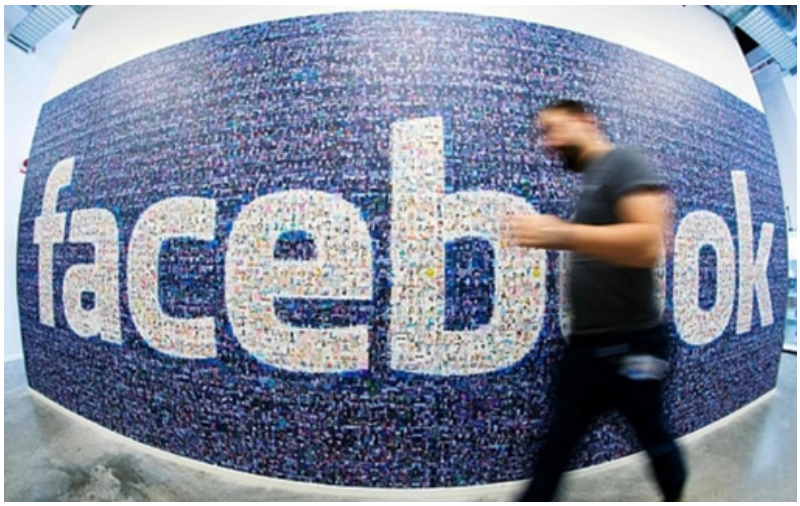
APPENDIX B — ARTICLE BY REUTERS, DATED FEBRUARY 7, 2017 (PORTUGUESE)

MINISTÉRIO PÚBLICO DEFENDE CORREÇÃO EM MULTA DE R$ 1,38 MI PARA FACEBOOK

Órgão público se refere a caso de interceptação de dados em fevereiro de 2016; Facebook teria descumprido ordem para revelar dados de investigados por tráfico de drogas

07/02/2017 - 12h12

Por Redação Link - Com Reuters



Ordem foi dada pela justiça em fevereiro de 2016; Facebook teria descumprido

Appendix B

O Ministério Público Federal (MPF) informou ontem à Justiça que é favorável à revisão da multa de R$ 1,38 milhão que o Facebook deve pagar por descumprir uma ordem judicial em fevereiro de 2016. Se o parecer for aceito pelo Tribunal Regional Federal da 2ª região, no Rio de Janeiro, o valor será corrigido com juros e correção monetária referentes ao período entre maio de 2016, quando a multa foi definida, e a data do julgamento sobre o recurso do Facebook, que deve acontecer nos próximos dias.

No início do ano passado, o Facebook se recusou a interceptar dados de Mário Jorge Carneiro dos Santos Júnior e Gabriel Ribeiro Espíndola, dois suspeitos de tráfico internacional de drogas e associação para o tráfico. Os alvos da quebra de sigilo eram os perfis dos suspeitos no Facebook e no aplicativo de mensagens instantâneas Facebook Messenger.

A Justiça definiu, à época, multa de R$ 20 mil por dia em virtude do não cumprimento da ordem judicial. Depois de uma busca realizada pela Polícia Federal no escritório da empresa, em 13 de maio de 2016, o juiz decidiu que os dados não poderiam ser obtidos.

O Facebook alegou no processo a impossibilidade de oferecer as informações solicitadas pela Justiça porque elas estão armazenadas em servidores fora do País. A única forma de obter as informações, segundo o Facebook, seria por meio de uma solicitação à Justiça dos Estados Unidos, mediante acordo de cooperação na área penal entre os dois países, o MLAT. No parecer enviado ao

Tribunal Regional Federal de 2ª região, o MPF opina que "não há inviabilidade técnica que possa fundamentar a recusa de cumprir a obrigação legal. O que há, na verdade, é uma blindagem interposta por um modelo de negócio adotado pelo Facebook e o subterfúgio jurídico baseado em regras internacionais".

Procurado pelo Estado, o Facebook informou que "tem profundo respeito pela Justiça e cumpre a legislação brasileira". A empresa afirmou que acredita que a multa é indevida. "Vamos utilizar os recursos garantidos pela Justiça."

No parecer ao Tribunal Regional Federal (TRF-2ª Região), o MPF também opinou que a multa diária não deve ser aplicada em conjunto ao Facebook Brasil e a seu funcionário, que recebeu a ordem judicial. Para a procuradoria, a denúncia contra o funcionário partiu de um equívoco do juiz, que deu a entender que a pessoa física sujeita a multas é o presidente da empresa.

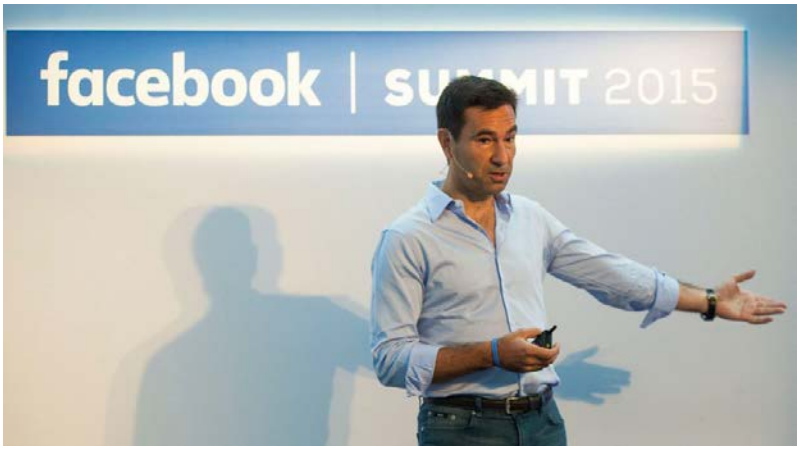
APPENDIX C — ARTICLE BY G1 SÃN PAULO, DATED APRIL 11, 2017 (ENGLISH)

PROSECUTORS GO AFTER FACEBOOK VP IN LATIN AMERICA FOR FAILURE TO COMPLY WITH COURT ORDER

Diego Jorge Dzodan was actually arrested in March of last year in São Paulo. Facebook said that they respect Brazilian laws and are cooperating "with the authorities to the best of their technical and legal ability."

By G1 São Paulo

4/11/2017 6:38 p.m. Updated on 4/11/2017 9:50 p.m.



Diego Dzodan, Facebook Vice President for Latin America at a social media event in 2015. (Photo: Personal Archive/ Diego Dzodan)

Appendix C

Federal Prosecutors have filed an action against Diego Jorge Dzodan, Facebook Vice-President for Latin America. The executive faces charges of failure to comply with a court order. In a statement, Facebook said that they respect Brazilian laws and are cooperating "with the authorities to the best of their technical and legal ability."

"The alleged crime that gave rise to the action does not allow wiretapping and the charge of failure to comply does not allow the accused to be taken into custody. Facebook Brazil is disputing the legality of the action and we will explore all available legal recourses," the company added in a statement.

According to the Federal Public Prosecutor's Office (MPF) in São Paulo, which filed the charge, Dzodan disobeyed three orders from the 2nd Federal Criminal Court of Rio de Janeiro. After a petition from the Prosecutor's Office in Rio de Janeiro, the Court ordered the release of messages from a person accused of criminal conspiracy for the international trafficking of drugs and from one other person.

For Federal Judge Renata Lotufo, the charge showed signs of "sufficient evidence of criminal involvement and materiality." The crime of failure to comply has an established sentence of 15 days to 6 months of imprisonment and a fine.

Appendix C

Another Case

Dzodan, an Argentinian national, was actually arrested in March of last year in São Paulo. The charge that resulted in the arrest is not related to the new charge and was filed by prosecutors in the state of Sergipe. At the time, the prosecutors in that state said that the social media company disobeyed a court decision that ordered the release of information exchanged on WhatsApp between drug-trafficking suspects. Facebook is the owner of WhatsApp since early 2014. **The executive was released after spending one day in jail**.

The investigation leading to Dzodan's arrest had begun after a drug seizure in the city of Lagarto, located 75 km from Aracaju. Judge Marcel Montalvão asked Facebook to inform the names of the users of a WhatsApp account used to exchange information about drugs. The company did not obey the Court, which last year applied a daily fine of R$50 thousand. As the company continued to fail to comply with the order, the amount of the fine was raised to R$1 million.

Facebook already prohibits the use of the social media app for drug sales. In February 2016, the company changed their usage policy for the site and the Instagram photo app in order to also bar users from selling weapons.

In practical terms, page and profile owners already were not allowed to sell weapons but small companies could use the quick ad creation tool for this purpose. The change barred this practice. However, the social media company's policy does not extend to WhatsApp.

Appendix C

According to Deputy Aldo Amorim, a member of the Federal Police Anti Organized Crime Unit in Brasília, the investigation began in 2015 and came across the need to obtain information related to exchanges of messages on WhatsApp, which was requested from Facebook and not provided in recent months.

He also revealed that escalating fines were applied and that such fines will stop only when the company provides the required information. The fines started at R$50 thousand, increased to R$500 thousand and then to R$1 million per day.

Also according to the deputy, there is a criminal organization in the city of Lagarto and Facebook's failure to provide the information is obstructing the police investigation. He also said that any communication company operating in Brazil must follow Brazilian laws, whatever the country of origin.

Appendix C

T&T Translation Services Inc.
89-33 Pontiac Street
Queens Village, NY 11427
Tel: +1-646-827-1163
Fax: +1-516-977-3110
E-mail: yuan@transtt.com

CERTIFICATION

I, Timothy Yuan, hereby certify that I speak and write both the Portuguese and English languages; that I have translated the foregoing article published by G1 on April 11, 2017, entitled "Prosecutors Go After Facebook VP in Latin America for Failure to Comply with Court Order," to the best of my ability; and that it is a true and correct translation to the best of my knowledge, information, and belief.

/s/	January 16, 2018
Signature	Date

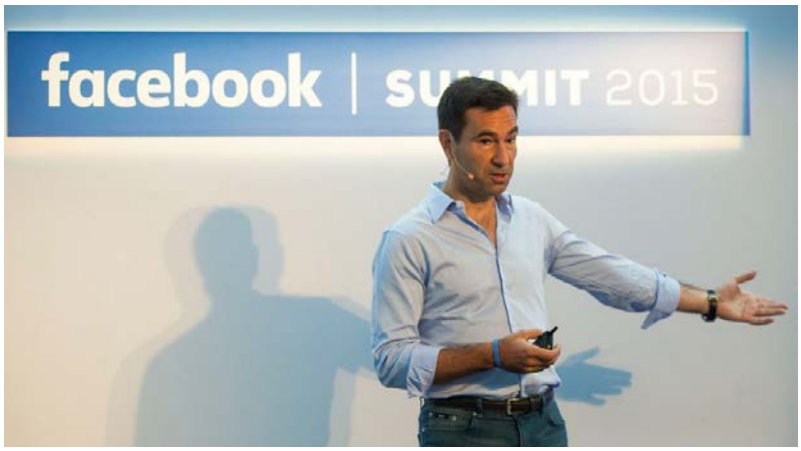
APPENDIX D — ARTICLE BY G1 SÃN PAULO, DATED APRIL 11, 2017 (PORTUGUESE)

JUSTIÇA ABRE PROCESSO CONTRA VICE DO FACEBOOK NA AMÉRICA LATINA POR DESOBEDIÊNCIA DE ORDEM JUDICIAL

Diego Jorge Dzodan chegou a ser preso em março do ano passado em São Paulo. Facebook disse que respeita a legislação brasileira e coopera "no limite máximo da nossa capacidade técnica e jurídica com as autoridades".

Por G1 São Paulo

11/04/2017 18h38 Atualizado 11/04/2017 21h50



Diego Dzodan, vice-presidente do Facebook para América Latina, em evento da rede social de 2015. (Foto: Arquivo Pessoal/Diego Dzodan)

Appendix D

A Justiça Federal abriu processo contra o vice-presidente do Facebook na América Latina, Diego Jorge Dzodan. O executivo irá responder por desobediência de ordem judicial. Em nota, o Facebook disse que respeita a legislação brasileira e coopera "no limite máximo da nossa capacidade técnica e jurídica com as autoridades".

"O suposto crime que deu origem ao caso não autoriza interceptação e a acusação de desobediência não autoriza prisão em flagrante. O Facebook Brasil está questionando a legalidade do processo e vamos explorar todos os recursos legais disponíveis", acrescentou a empresa em nota.

Segundo o Ministério Público Federal (MPF) em São Paulo, responsável pela denúncia, Dzodan descumpriu três ordens da 2ª Vara Federal Criminal do Rio de Janeiro. Após pedido da Procuradoria no Rio de Janeiro, a Justiça havia determinado a quebra do sigilo de mensagens de um acusado de associação criminosa para tráfico internacional de drogas e de mais uma pessoa.

Para a juíza federal Renata Lotufo, a denúncia demonstrou "indícios suficientes da autoria e materialidade delitivas". O crime de desobediência estabelece pena de 15 dias a 6 meses de prisão, e multa.

Outro caso

Dzodan, que é argentino, chegou a ser preso em março do ano passado em São Paulo. A ação que culminou na prisão não tem relação com o novo processo e foi tomada a

pedido da Justiça de Sergipe. Na ocasião, a Justiça daquele estado disse que a rede social descumpriu decisão judicial de compartilhar informações trocadas no WhatsApp por suspeitos de tráfico de droga. O Facebook é dono do WhatsApp desde o começo de 2014. **O executivou foi solto após ficar um dia na cadeia**.

A investigação que culminou na prisão de Dzodan foi iniciada após uma apreensão de drogas na cidade de Lagarto, a 75 km de Aracaju. O juiz Marcel Montalvão pediu que o Facebook informasse o nome dos usuários de uma conta no WhatsApp em que informações sobre drogas eram trocadas. A empresa não atendeu a Justiça, que aplicou, no ano passado, multa diária de R$ 50 mil. Como a empresa ainda assim não cumpriu a determinação, o valor foi elevado para R$ 1 milhão.

O Facebook já proíbe que a rede social seja usada para vender drogas. Em fevereiro de 2016, alterou a política de uso do site e do aplicativo de fotos Instagram para impedir também que os usuários comercializassem armas. Na prática, donos de páginas e perfis já não podiam vender material bélico, mas pequenas microempresas podiam usar a ferramenta de criação de anúncios rápidos para isso. Com a alteração, essa prática foi vetada. A política da rede, no entanto, não se estende ao WhatsApp.

Segundo o delegado Aldo Amorim, membro da Diretoria de Combate ao Crime Organizado da Polícia Federal em Brasília, a investigação foi iniciada em 2015 e esbarrou na necessidade informações relacionadas as trocas de mensagens via whatsapp, que foram solicitadas ao Facebook e não fornecida ao longo dos últimos meses.

Ele revelou ainda que foram aplicadas multas gradativas e que essas multas só irão cessar quando a empresa repassar as informações necessárias. Os valores das multas iniciaram em R$ 50 mil, passando para R$ 500 mil e, depois, R$ 1 milhão diários.

Ainda de acordo o delegado, existe uma organização criminosa na cidade de Lagarto e o não fornecimento das informações do Facebook está obstruindo o trabalho de investigação da polícia. Ele disse também que toda empresa de comunicação que atua no Brasil deve seguir a legislação brasileira, independente do seu país de origem.

APPENDIX E — AFFIDAVIT OF ERIC HOLDER FILED IN AÇÃO DECLARATÓRIA DE CONSTITUCIONALIDADE N.51, SUPREMO TRIBUNAL FEDERAL (DECEMBER 5, 2017)

AFFIDAVIT

I, Eric H. Holder, Jr., of Washington, D.C., United States of America, HEREBY SWEAR THAT:

1. I am a partner at the law firm of COVINGTON & BURLING LLP in Washington, D.C. I submit this affidavit in support of the action initiated by ASSESPRO NACIONAL in order to describe the internationally recognized mechanisms available under United States law that facilitate Brazilian law enforcement requests for stored electronic communications hosted by United States service providers.[1] I have knowledge of the facts set forth below.

2. I am an attorney in good standing of the District of Columbia bar and the New York bar. I received my law degree from Columbia Law School and my undergraduate degree from Columbia College. Currently, in my private practice, I advise clients on complex investigations and litigation matters, including those that are international in scope and those that involve significant regulatory enforcement issues.

---

1. Federação das Associações das Empresas Brasileiras de Tecnologia da Informação (The Federation of Associations of Brazilian Companies in Information Technology).

3. From February 2009 to April2015, I served as the 82nd Attorney General of the United States. The Attorney General is the head of the U.S. Department of Justice ("DOJ" or the "Department"). The Attorney General is appointed by the President of the United States and confirmed by the U.S. Senate. As Attorney General, I was responsible for representing the United States in legal matters, including the investigation and prosecution of domestic and international crimes, and advising the President and heads of executive departments on various legal issues.

4. One of my primary objectives as Attorney General was to support the Department's efforts to combat increasingly transnational criminal conduct. During my tenure, for example, the Department investigated and prosecuted a variety of transnational criminal threats, including networks used for human trafficking, narcotics distribution, money laundering, and arms smuggling.

5. International cooperation was—and remains—critical to our efforts to fight transnational crime, and during my time at DOJ we created a number of initiatives to foster such cooperation. For example, we created the International Organized Crime Intelligence and Operations Center (IOC-2), which relies heavily on cooperation with foreign law enforcement to combat international organized crime.[2]

---

2. Department of Justice Office of Public Affairs, *Attorney General Announces Center to Fight International Organized Crime*, May 29, 2009, https://www.justice.gov/opa/pr/attorney-general-announces-center-fight-international-organized-crime.

6. Including my time as Attorney General, I have served in the U.S. government for more than thirty years, having been appointed to various positions requiring U.S. Senate confirmation by Presidents Obama, Clinton, and Reagan. I began my legal career at the Public Integrity Section of the DOJ, the unit that investigates and prosecutes public corruption. In 1988, President Reagan appointed me to serve as a judge of the Superior Court of the District of Columbia. In 1993, I accepted an appointment from President Clinton as U.S. Attorney for the District of Columbia, a position I held until I became the Deputy Attorney General in 1997. From 2001 until my confirmation as Attorney General, I was a partner at Covington & Burling, where I represented various clients in major civil, criminal, and investigative matters.

7. The purpose of this affidavit is to discuss an increasingly prevalent circumstance in international law enforcement: when law enforcement in one country determines that emails or other electronic communications stored by a foreign technology company are relevant to a criminal investigation, and seeks to obtain such communications as part of that investigation. This situation, which is typically referred to as a cross-border data request, presents a number of issues under U.S. domestic and international law.

8. In particular, and as discussed in greater detail below, the U.S. Stored Communications Act ("SCA") generally prohibits electronic communications service

providers subject to U.S. jurisdiction from disclosing the communications of their users to any other person unless one of the statute's exceptions applies. Responding to foreign law enforcement requests is not among those exceptions, and service providers therefore generally cannot directly respond to such unilateral requests (i.e., requests made directly from the foreign law enforcement entity to the U.S. provider) without violating U.S. law and subjecting themselves to substantial penalties.

9. However, the United States has entered into a considerable number of international agreements with foreign countries and territories that enable the U.S. government to assist foreign law enforcement officials with their investigations while, at the same time, adhering to U.S. law. Mutual Legal Assistance Treaties (MLATs) are the most prevalent mechanism used by law enforcement for this purpose, and such a treaty exists between the United States and Brazil. In addition, a multilateral convention for mutual legal assistance exists between all thirty-five independent states of the Americas (known as the Inter-American Convention on Mutual Assistance in Criminal Matters). Such international agreements afford the Brazilian government the opportunity to obtain stored communications records from U.S. service providers without raising conflicts with U.S. law.

Appendix E

I. Subject to Enumerated Exceptions, U.S. Law Generally Prohibits Service Providers from Disclosing Users' Communications Content To Any Other Person.

10. The SCA protects the privacy of stored electronic communications.[3] As a technical matter, the statute applies to two defined categories of services: electronic communication services and remote computing services. U.S. courts have interpreted these categories to include social media service providers such as Facebook. In *Crispin v. Christian Audigier, Inc.,* for example, a federal district judge in California applied the SCA to subpoenas directed at Facebook, MySpace, and Media Temple, holding that such services provided private messaging services similar to traditional email platforms, and therefore could not disclose such messages without orders that meet the appropriate legal criteria.[4]

11. The centerpiece of the SCA is a prohibition on the disclosure of customer communications content to any other person. Section 2702(a) of Title 18 provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." There is a similar prohibition applicable to remote computing services in Section 2702(b).

---

3. 18 U.S.C. §§ 2701-2711.

4. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).

12. For purposes of the SCA, 1he definition of "content" is drawn from another U.S. statute that protects the privacy of information: the U.S. Wiretap Act, which generally prohibits the interception of communications content as it travels from sender to recipient.[5] The Wiretap Act defines "content" as "any information concerning the substance, purport, or meaning of that communication."[6] A stored email's content, for example, includes the body of the email and the email's subject line. The email's sender and recipient information (sometimes referred to as "to/from" information), as well as the date and time stamp and a subscriber's address or name, are generally considered "noncontent." An apt comparison in the physical world is a traditional letter in a person's mailbox—in this scenario, the letter's "content" is the substance of the letter itself, whereas the address information on the envelope constitutes noncontent.

13. The SCA's prohibition on the disclosure of content is subject to several enumerated exceptions. The exceptions are set out in Section 2702(b) of Title 18, and allow (but do not require) providers to divulge the contents of a communication (1) to the intended recipient of that communication; (2) with the lawful consent of the sender or recipient; (3) to U.S. law enforcement, if authorized by law (for example, upon receipt of an SCA warrant, as discussed below); (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

---

5. 18 U.S.C. § 2510 *et seq.*

6. 18 U.S.C. § 2510(8).

(5) as necessary to render the provider's service or to protect their rights or property; (6) to the U.S. National Center for Missing and Exploited Children, as authorized by the Victims of Child Abuse Act of 1990; (7) to a U.S. law enforcement agency if the contents were inadvertently obtained and appear to pertain to the commission of a crime; and (8) to a U.S. government entity if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure.

14. With respect to the final exception for disclosures in emergency situations, it is worth noting that even though this provision may be utilized only for disclosures to U.S. law enforcement entities, the Department of Justice frequently works with foreign partners to facilitate disclosure of information under this exception in response to emergency situations in foreign countries. During my time as Attorney General, I was personally involved in responding to emergencies in foreign countries, where a U.S. provider disclosed information to the DOJ pursuant to the emergency exception, and the DOJ then provided that information to our foreign partner.

15. Several courts have interpreted this list of exceptions to be exhaustive, which is to say that it is unlawful for providers to disclose customer content in any circumstance other than an enumerated exception.[7]

---

7. *See, e.g.*, *In re Subpoena Duces Tecum to AOL, LLC,* 550 F. Supp. 2d 606, 609 (E.D. Va. 2008); *O-Grady v. Superior Court,* 139 Cal. App. 4th 1423, 1447 (2006) ("[s]ince [the SCA]

Since there is no exception in Section 2702(b) for disclosures to foreign law enforcement, U.S. providers are generally forbidden from disclosing customer content to foreign law enforcement, even if the foreign law enforcement request is predicated on valid legal process issued under foreign law.

16. The fact that a foreign law enforcement request might pertain to a non-U.S. person does not take the request outside the scope of this prohibition; the SCA's privacy protections apply to all users of covered services, regardless of the user's nationality. In *Suzlon Energy Ltd. v. Microsoft Corp.,* for example, a U.S. court of appeals held that the SCA's protections extend to the contents of communications of foreign citizens. The court reasoned that the statute's plain language does not distinguish between U.S. and non-U.S. citizens—it applies to all "users," which are defined as "*any* person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use."[8] The court also noted that limiting the SCA to only U.S. persons would put service providers in an

---

makes an exception for for civil discovery and no repugnancy has been shown between a denial of such discovery and congressional intent or purpose, the Act must be applied, in accordance with its plain terms, to render unenforceable the subpoenas."); *Thayer v. Chiczewski,* No. 07 C 1290, 2009 WL 2957317, at * 5 (N.D. Ill. Sept. 11, 2009) (citing *In re Subpoena Duces Tecum to AOL* in support of the proposition that the SCA created a "zone of privacy" to protect internet users).

8. 18 U.S.C. § 2510(13) (emphasis added).

untenable position. Upon receipt of each request for communications content, providers would have to determine the citizenship of the account holder—a "costly, fact-intensive, and difficult determination."[9]

17. Similarly, the fact that a foreign law enforcement request might be directed to a provider's subsidiary located in the foreign jurisdiction would generally not alter the applicability of the SCA's prohibition on disclosure of content to foreign law enforcement. In many instances, foreign affiliates of U.S. providers do not have access to customer information. More fundamentally, it is not generally a defense to liability under the SCA for a provider, otherwise subject to the statute, to pass customer content through a local subsidiary before producing it in response to a foreign law enforcement request.

18. Violations of the SCA carry the possibility of substantial penalties for service providers. If a user or a class of users[10] sues a provider for unlawfully

---

9. The court noted that such a determination would involve considering whether the account holder was "at all times a U.S. citizen, or later became a citizen, or was a resident alien with some Fourth Amendment protection, or if there were other reasons to provide Fourth Amendment rights." *Suzlon Energy Ltd.,* 671 F.3d at 730.

10. Google, for example, had to pay $8.5 million to settle a class action brought by users claiming that Google unlawfully violated their internet privacy rights by disclosing their communications to third parties. *See In re Google Referrer Header Privacy Litigation,* 87 F. Supp. 3d 1122 (N.D. Ca. 2015) (approving settlement for $8.5 million of consumer class action for alleged violation of the SCA).

disclosing their communications, a court may award the victim users damages amounting to the sum of actual harm suffered plus any profits made by the provider as a result of the violation.[11] At minimum, the court must award the victim user or users $1,000 per violation.[12] In addition, courts are authorized to award punitive damages for willful or intentional violations.

II. In General, Only a Search Warrant May Compel the Disclosure of Customer Content Under U.S. Law.

19. As discussed in the previous section, one of the exceptions to the prohibition on the disclosure of content information is if the content is sought by U.S. law enforcement, as authorized by U.S. law. Section 2703 of Title 18 of the U.S. Code sets out the procedures that U.S. federal, state, and local law enforcement entities must follow to obtain customer content information under the SCA.

20. Although the SCA itself creates several different procedures for law enforcement to obtain customer content information, the law—which was enacted in 1986—is in this respect outdated. In 2010, a U.S. court of appeals held that customers have a reasonable expectation of privacy in their email content, which means that the Fourth Amendment to the U.S. Constitution requires the government to obtain a

11. 18 U.S.C. § 2707.

12. *Id.* at § 2707(c).

warrant before an email provider can be compelled to produce the customer emails.[13]

21. In contrast with other forms of legal process (like a subpoena), a search warrant has two features that help protect privacy against unreasonable governmental incursions. First, search warrants must be issued on probable cause, which is a standard that requires the government to establish a meaningful link between their investigation and the customer content at issue. Second, search warrants cannot be issued by the investigating agency itself, but must instead be issued by an impartial magistrate.

22. As a general matter, following the court of appeals decision in 2010, law enforcement in the United States will obtain a warrant to compel a technology company to disclose customer content.[14]

III. International Agreements Have Been Crafted to Allow Law Enforcement to Investigate and Prosecute Transnational Crime While Respecting National Sovereignty.

23. As set out in Section I above, U.S. technology companies are generally forbidden from disclosing customer

---

13. *See U.S. v. Warshak,* 631 F.3d 266 (6th Cir. 2010).

14. *See* David Kravets, "Google Tells Cops to Get Warrants for User E-Mail, Cloud Data," WIRED (Jan. 23, 2013); MICROSOFT 2017 LAW ENFORCEMENT REQUESTS REPORT (noting that a warrant is required to obtain Microsoft users' content, whereas a subpoena is required for noncontent).

content in response to foreign law enforcement requests. As set out in Section II, U.S. technology companies can be compelled to produce customer content in response to U.S. law enforcement, but generally only in response to a warrant.

24. The fact that U.S. technology companies cannot generally be *directly* compelled to produce customer content to foreign law enforcement does not, however, mean that foreign law enforcement lacks any means to obtain such content. To the contrary, there are a range of international mechanisms by which a foreign law enforcement agency can make a request to the U.S. government, which can in turn "domesticate" the request by issuing a U.S. warrant to the technology company. In addition, when law enforcement agencies in multiple countries cooperate in transnational investigations, agencies in one country may assist their foreign partners by voluntarily sharing evidence obtained domestically pursuant to valid legal process. This form of informal international cooperation is often critical in addressing transnational criminal threats.

25. These international mechanisms were created precisely to avoid the type of conflicts-of-laws that are raised in this context by the SCA. Before the advent of the internet, when U.S. law enforcement agencies wanted to conduct a law enforcement operation on foreign soil, they generally needed to cooperate with their foreign counterparts, and vice versa. As the U.S. Federal Judicial Center's International Litigation Guide—a commentary that is frequently

relied upon by U.S. courts—has recognized, there are significant U.S. and international law issues that generally preclude U.S. law enforcement from unilaterally flying to another country to "conduct searches, question suspects, obtain documents, and proceed with arresting individuals for trial."[15]

26. The technology in this context is different, but the principles are the same. When a law enforcement agency in one country wants to conduct a law enforcement operation that implicates the sovereignty of another country, doing so unilaterally raises substantial domestic and international legal issues. International agreements have thus proved critical to allow law enforcement officials to investigate and prosecute transnational crimes while, at the same time, being respectful of international sovereignty. As a result, the Department of Justice directs its attorneys to take advantage of international agreements such as MLATs, letters rogatory, and other mechanisms when seeking evidence from other countries.[16]

---

15. Federal Judicial Center International Litigation Guide, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges* 1 (2014). *See also* Restatement (Fourth)-The Foreign Relations Law of the United States § 313 (noting that the "conduct of criminal investigations within the territory of a foreign statute without its permission may violate customary international law ... as well as the domestic laws of the foreign state.").

16. *See, e.g.*, Department of Justice, U.S. Attorneys' Manual: Criminal Resource Manual at 275-277; DOJ Office of Legal Education, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations at

IV. In Particular, Mutual Legal Assistance Treaties (MLATs) Play an Important Role in Enabling the United States to Assist the Efforts of Foreign Law Enforcement Officials.

27. U.S. law permits our government to enter into MLATs with foreign countries that enable our federal courts to respond to foreign law enforcement requests while adhering to our regulations, statutes, and our Constitution. In particular, Section 3512 of Title 18 authorizes federal courts to issue orders necessary to execute MLAT requests that have been approved by U.S. government attorneys at the Department of Justice.

28. The mechanics of MLATs are straightforward. When the government of a country party to a U.S. MLAT requests the assistance of the United States, the request is directed to the Department of Justice's Office of International Affairs ("OIA"). If an attorney from OIA approves of the request, the attorney must go to federal court and ask for judicial approval, in the same way the attorney would request approval of a traditional, domestic law enforcement order. Before approving the foreign request, the federal court must determine whether the request complies with the underlying MLAT treaty and U.S. law. However, there generally is a presumption of validity for requests that have already been approved by the OIA[17]

---

57 (instructing prosecutors to use the MLAT or letters rogatory process to retrieve evidence of computer crime from abroad).

17. *See In re Premises Located at 840 140th Ave., NW, Bellevue, Wash.*, 634 F.3d 557, 571 (9th Cir. 2011) ("when a request

29. MLATs are formal U.S. treaty obligations, which means they must be signed by the US. Executive Branch (generally by the U.S. Secretary of State) and ratified by the U.S. Senate. There is a long-standing bipartisan practice of negotiating, signing, and implementing MLATs in the United States, and the U.S. government has repeatedly recognized that MLATs represent a "formal, streamlined process by which States may gather information and evidence in other countries for use in criminal investigations and prosecutions.[18]

30. Today, MLATs are the principal means by which the United States fulfills foreign requests for evidence.[19] The United States currently is a party to MLATs with more than 65 countries and territories, including Brazil.[20]

---

for assistance under the MLAT arrives before a district court ... almost all the factors already would point to the conclusion that the district court should grant the request").

18. *See, e.g.,* Exec. Rept. 110-13; *see also* Exec. Rept. 110-14, "Treaty with Malaysia on Mutual Legal Assistance," Sen. Foreign Rel. Comm., 110th Cong. (Sept. 11, 2008).

19. Federal Judicial Center International Litigation Guide, *supra* n. 15, at 5.

20. 7 Foreign Affairs Manual 962.1; U.S. Department of State, *2016 International Narcotics Control Strategy Report* (INCSR).

Appendix E

V. Brazil Can Obtain a Valid SCA Warrant Via International Agreements, Such as the U.S.-Brazil MLAT.

31. As discussed in the previous section, Section 3512 of Title 18 authorizes federal courts to issue orders necessary to execute MLAT requests that have been approved by U.S. government attorneys at the Department of Justice. In particular, Section 3512 authorizes federal courts to issue search warrants in response to MLAT requests. Since search warrants are a valid means of compelling U.S. technology companies to disclose customer content under the SCA, MLATs generally provide foreign partners with the ability to obtain customer content from providers subject to U.S. jurisdiction, consistent with the SCA.

32. The Brazil-U.S. MLAT and the multilateral Inter-American Convention on Mutual Legal Assistance in Criminal Matters are not exceptions to this general rule. Executed over two decades ago, the MLAT between the United States and Brazil provides for law enforcement assistance in a variety of forms—from providing documents and locating persons or items to taking testimony of witnesses and executing requests for searches and seizures (such as SCA warrants). The treaty also contains a catchall provision, permitting the United States to assist Brazil in any way not prohibited by U.S. law.[21]

---

21. Mutual Legal Assistance Treaty Between the United States of America and Brazil art. 1(2), Treaty Doc. 105-42, 105th Cong. (signed Oct. 14, 1997).

33. Similarly, the multilateral Inter-American Convention provides for uniform legal assistance procedures and rules for cooperation across all thirty-five independent states of the Americas, including the United States and Brazil.[22] The scope of law enforcement assistance mechanisms included in the Inter-American MLAT is similar to the scope of measures permitted by the U.S.-Brazil MLAT discussed above, and Article 7 of the Convention notes that "any other procedure" may also be covered by the Convention upon agreement between the requesting and requested states.[23]

34. During my tenure as Attorney General of the United States, the U.S. Department of Justice repeatedly relied on the MLAT process to assist law enforcement abroad—and Brazilian law enforcement was no exception. For example, in 2011, Brazilian law enforcement authorities were investigating the 2006 Amazon midair collision between a Legacy jet and a Gol Airlines Boeing 737 that killed 154 people. After making an emergency landing, the American pilot and copilot of the Legacy jet were charged by Brazilian authorities with criminal negligence for causing the crash. When the pilots declined to return to Brazil for trial, the MLAT between the U.S. and Brazil allowed Brazilian law enforcement to pursue their investigation. Article 8(1) of the Brazil-U.S.

---

22. Inter-American Convention on Mutual Assistance in Criminal Matters with Related Optional Protocol, Treaty Doc. 105-25, 105th Cont. (signed Oct. 18, 2000).

23. *Id.* at art. 7.

MLAT requires the United States to compel the testimony of requested persons located in the U.S., and as a result, the American pilot and copilot were successfully questioned in the United States through written questions and video testimony.[24]

35. International cooperation has become even more critical to law enforcement efforts as communications have moved from physical mailboxes to digital inboxes. To be sure, the MLAT process has not always functioned perfectly during this shift into the digital age. Within a decade, requests for U.S. assistance from foreign authorities increased by nearly 60 percent, and response times for some requests experienced significant delays. As a result, during my tenure as Attorney General, the Department requested—and received—tens of millions of additional dollars to enhance our MLAT resources throughout the DOJ.[25] With these additional resources, the Department began implementing a more centralized system to process requests and reduce response times. In addition, the DOJ enhanced its technological resources and supported training efforts to assist key

24. William Glaberson, "A Trial in Brazil, With Testimony on Long Island," N.Y. Times (Mar. 30, 2011), http://www.nytimes.com/2011/03/31/nyregion/31plane.html.

25. U.S. Department of Justice, *FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Reform*, https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf. *See also* DOJ Criminal Division, *FY 2016 President's Budget* at 20, https://www.justice.gov/sites/default/files/jmd/pages/attachments/2015/02/02/10._criminal_division_crm.pdf.

foreign partners in submitting MLAT requests that comply with their MLAT treaties and with U.S. law.

VI. By Relying on the MLAT Process, Brazilian Law Enforcement Can Obtain Evidence From U.S. Companies While Avoiding Conflict With U.S. Privacy Law.

36. The legal assistance treaty between the United States and Brazil permits Brazil to submit requests for evidence under the control of service providers subject to U.S. jurisdiction. If a judge approves of a request, the service provider to whom the request is directed will be required to comply, just as it would be required to comply with a valid SCA warrant issued by U.S. law enforcement. In this way, the needs of Brazilian law enforcement can be met, even if U.S. law prevents it from directly compelling a U.S. provider to disclose the evidence it seeks.

37. At the same time, the U.S.-Brazil MLAT preserves the sovereignty of the United States by allowing U.S. law to govern the standards that must be met before U.S.-based evidence is produced to a foreign power as part of a criminal investigation. In this way, MLATs serve as a crucial means for advancing international comity and partnerships when it comes to combatting transnational crime—an effort that is, without question, in everyone's best interest.

/s/_____
ERIC H. HOLDER, JR.