No. 17-2

IN THE

Supreme Court of the United States

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN EMAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

UNITED STATES OF AMERICA,

Petitioner,

—v.—

MICROSOFT CORPORATION,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF OF PRIVACY INTERNATIONAL, HUMAN AND DIGITAL RIGHTS ORGANIZATIONS, AND INTERNATIONAL LEGAL SCHOLARS AS *AMICI CURIAE* IN SUPPORT OF RESPONDENT

LAUREN GALLO WHITE
RYAN T. O'HOLLAREN
WILSON, SONSINI, GOODRICH & ROSATI, P.C.
One Market Plaza Spear Tower, Suite 3300
San Francisco, California 94105
(415) 947-2000
lwhite@wsgr.com
rohollaren@wsgr.com

BRIAN M. WILLEN
Counsel of Record
BASTIAAN G. SUURMOND
WILSON, SONSINI, GOODRICH & ROSATI, P.C.
1301 Avenue of the Americas, 40th Floor
New York, New York 10019
(212) 999-5800
bwillen@wsgr.com
bsuurmond@wsgr.com

Attorneys for Amici Curiae

(*Counsel continued on inside cover*)

Caroline Wilson Palow
Scarlet Kim
Privacy International
62 Britton Street
London, EC1M 5UY
United Kingdom
caroline@privacyinternational.org
scarlet@privacyinternational.org

QUESTION PRESENTED

Whether construing the Stored Communications Act ("SCA") to authorize the seizure of data stored outside the United States would conflict with foreign data-protection laws, including those of Ireland and the European Union, and whether these conflicts should be avoided by applying established canons of construction, including presumptions against extra-territoriality and in favor of international comity, which direct U.S. courts to construe statutes as applying only domestically and consistently with foreign laws, absent clear Congressional intent.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

PAGE(S)

Cases

Statutes and Rules

Treaties and Agreements

PAGE(S)

Constitutional Provisions

Foreign and International Regulations

PAGE(S)

PAGE(S)

Other Authorities

PAGE(S)

PAGE(S)

IDENTITY AND INTEREST OF *AMICI CURIAE*

Pursuant to Supreme Court Rule 37, Privacy International, joined by numerous human rights and digital rights organizations, as well as leading international legal scholars, respectfully submit this brief as *amici curiae* in support of Respondent Microsoft Corporation.[1]

Established in 1990, Privacy International is a non-profit, non-governmental organization based in London, the United Kingdom ("U.K."), which defends the right to privacy around the world. Privacy International conducts research and investigations into government and corporate surveillance activities with a focus on the policies and technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States, the U.K., and Europe, including the Court of Justice of the European Union and the European Court of Human Rights. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional, and international laws that protect this fundamental right. As a part of this mission, Privacy International works with various partner organizations across the world to identify and address threats to privacy. Based on its commitment to privacy and human

[1] Pursuant to Rule 37.6, amici affirm that no counsel for a party authored this brief in whole or in part, that no such counsel or a party made a monetary contribution intended to fund the preparation or submission of the brief, and that no person other than amici, their members, or their counsel made such a monetary contribution. Both parties have provided blanket consent to the filing of amicus briefs in this case.

rights, Privacy International has a strong interest in this controversy.

In addition, the following human rights and digital rights organizations and legal scholars join Privacy International in this amicus brief:

1. Artículo 12
2. Asociación por los Derechos Civiles
3. Members of the Association of Spanish Constitutionalists[2]
4. Australian Privacy Foundation
5. Bits of Freedom
6. Civil Rights Defenders
7. Derechos Digitales América Latina
8. Digital Freedom and Rights Association
9. Elektronisk Forpost Norge (Electronic Frontier Norway)
10. European Digital Rights[3]

---

[2] Members of the Association of Spanish Constitutionalists have signed on as amici in their individual capacities as constitutional law scholars. Their identities and institutions are listed in the Appendix.

[3] European Digital Rights ("EDRi"), which is an association of 35 civil and human rights organizations, joins this brief in its associational capacity with the exception of three members—Digital Rights Ireland, the Electronic Frontier Foundation, and Open Rights Group. These three members do not join this brief as part of EDRi as they are submitting separate briefs in their individual capacities. In addition, seven EDRi members also join this brief in their individual capacities: Bits of Freedom, Digital Freedom and Rights Association, Elektronisk Forpost Norge, Foundation for Information Policy Research, Panoptykon, Privacy International, and Vrijschrift.

11. Fundación Datos Protegidos
12. Fundación Karisma
13. Foundation for Information Policy Research
14. Hiperderecho
15. Human Rights Watch
16. International Cyber Law Studies in Korea
17. IPANDETEC
18. Italian Coalition for Civil Liberties and Rights
19. La Quadrature du Net
20. Liberty
21. Open Net (Korea)
22. Panoptykon Foundation
23. Red en Defensa de los Derechos Digitales
24. Renaissance Numérique
35. Professor Simon Chesterman
26. Vrijschrift

The interest statements of these organizations can be found in the Appendix.

SUMMARY OF ARGUMENT

Foreign and international legal regimes widely recognize the fundamental right of individuals to privacy in their electronic data. There are now approximately 120 countries around the world with laws that specifically protect people's personal data from unwanted inspection and transfer, including Ireland, where the email records at issue in this case are stored. These laws reflect an international

consensus that data privacy is a fundamental aspect of individual liberty.

Interpreting the Stored Communications Act ("SCA") to authorize extraterritorial search warrants would significantly impair these privacy rights by allowing the United States Government to seize and review data hosted on foreign soil without regard for the laws protecting that data in those countries. In this case, for example, the warrant demanding Microsoft customer emails stored in Ireland flatly conflicts with Irish and European Union law, which prohibit the transfer of personal data to law enforcement officials in the United States outside of official government-to-government channels established to process such transfers, including through mutual legal assistance treaties ("MLATs"). Similar violations of foreign law would occur in countless other cases if the Government is given the expansive authority to issue extraterritorial warrants that it now seeks. That result would set the stage for repeated violations of the data-privacy rights of people around the world.

This would perhaps be a different case if U.S. law clearly directed this result. But it does not. There is no indication that Congress ever thought about—much less approved—giving the Executive the sweeping authority to obtain warrants for the seizure of personal data stored outside the United States. Nothing in the statute contemplates that result, and Congress certainly gave no indication that it was opening the door to a new species of warrant that would be used to override the data-protection laws of numerous foreign governments. In these circumstances, established principles of statutory interpretation should lead this Court to reject the Government's broad reading of the SCA.

The presumption against extraterritoriality instructs courts to construe statutes to have only domestic reach, unless their terms specifically contemplate foreign application. This presumption reflects and reinforces the importance of minimizing conflict between U.S. law and the laws of foreign nations. Such conflict is especially likely here, given the number and variety of laws that protect personal data worldwide and regulate the transfer of personal data across jurisdictions. Foreign governments have legally binding obligations, including under international human rights law, to respect and protect such data from unwanted intrusion. Those obligations would be swept aside if the U.S. Government could simply issue warrants to companies in the United States demanding personal information stored abroad, without regard for any other country's laws. The presumption against extraterritorial application counsels strongly against that result.

These considerations are reinforced by principles of comity, under which courts applying U.S. law work to avoid unreasonable interference with the sovereign authority of other nations. To better ensure transnational harmony, comity creates a presumption against reading domestic statutes to conflict with the laws of foreign governments. Comity considerations apply here because construing the SCA's warrant provisions to authorize the seizure of personal data outside the United States would conflict with the data-protection laws of Ireland, the European Union, and other governments around the world, which insist that data requests for general criminal investigations be made through official channels—rather than through unilateral warrants issued to private companies.

Comity opposes expansively interpreting a federal statute to undermine the judgments of foreign governments about how to protect data within their territories and thereby safeguard the fundamental data-privacy rights that they ensure. That is especially so because conflicts between U.S. and foreign law on these issues put the companies that provide data-hosting services (and other valuable online services) in the untenable position of potentially having to violate the laws of other countries in order to comply with warrants issued in the United States. Comity principles are designed to avoid this dilemma, in the process ensuring that law enforcement does not, at least without clear authorization from Congress, erode the data-protection laws adopted by governments worldwide.

In short, proper respect for the laws and interests of other nations—embodied in bedrock principles of domestic statutory interpretation—should lead this Court to affirm the Second Circuit's judgment in this case and hold that U.S. law does not authorize warrants for personal data stored outside the United States.

ARGUMENT

I. Jurisdictions Around the World Have Enacted Data-Protection Laws that Protect Individual Privacy Rights, and Those Laws Would Be Undermined if the SCA Were Read to Allow Warrants That Reach Data Stored Outside the United States

International human rights law recognizes a fundamental right to privacy, including privacy in one's electronically-stored personal communications. This right is reflected and given concrete form in the

legal regimes of countries around the world, including through statutes, constitutional provisions, and international agreements that regulate data processing by both private entities and government actors. To construe the SCA to authorize warrants that would compel the production of foreign-stored data would both conflict with numerous foreign laws and seriously undermine the individual rights to privacy and data protection that those laws were designed to protect.

A. International Human Rights Law Recognizes a Fundamental Right to Privacy in Personal Electronic Data

Data-protection laws that secure the right to individual privacy are an increasingly important aspect of international law. The right is enshrined in the foundational documents of the international human rights system, and it has only become more detailed and prominent in the digital age.

Article 12 of the Universal Declaration of Human Rights ("UDHR") proclaims that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence …. Everyone has the right to the protection of the law against such interference or attacks." G.A. Res. 217 (III) A, UDHR, art. 12 (Dec. 10, 1948). The UDHR has formed the basis for the major international human rights treaties that similarly enshrine the right to privacy, including the International Covenant on Civil and Political Rights ("ICCPR"), which has been ratified by the United States.[4] Article 17 of the ICCPR provides

---

[4] *See* G.A. Res. 2200 (XXI) A, ICCPR, preamble, art. 17 (Dec. 16, 1966); G.A. Res. 44/25, Convention on the Rights of the Child, preamble, art. 16 (Nov. 20, 1989); G.A. Res. 45/158, International Convention on the Protection of the Rights of All

that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." According to the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, "the right to privacy" includes "the ability of individuals to determine who holds information about them and how ... that information [is] used." U.N. Doc. A/HRC/23/40, ¶ 22 (Apr. 17, 2013).

Reflecting the fundamental principles set forth in the UDHR, Article 8 of the European Convention on Human Rights ("ECHR") provides that "[e]veryone has the right to respect for his private and family life, his home and his correspondence," and interference with that right is only justified under certain, limited circumstances. ECHR, art. 8(2). Under the ECHR, as construed by the European Court of Human Rights ("ECtHR"), personal data in digital form (such as the content of one's emails) is considered part of one's "private life." *Copland v. United Kingdom*, 45 Eur. Ct. H.R. 235, ¶ 41 (2007). The ECtHR has further held that copying and/or storage of an individual's communications constitutes an interference with the right to privacy under Article 8. *See M.N. & Others v. San Marino*, App. No. 28005/12, ¶¶ 51-55 (Eur. Ct. H.R. July 7, 2015); *see also Wieser v. Austria*, 46 Eur. H.R. Rep. 54 (2008) (Austrian government's seizure of

---

Migrant Workers and Members of Their Families, preamble, art. 14 (Dec. 18, 1990); European Convention on Human Rights ("ECHR"), preamble, art. 8, Nov. 4, 1950, 213 U.N.T.S. 222; American Convention on Human Rights, preamble, art. 11, Nov. 21, 1969, 1144 U.N.T.S. 143; *see also* G.A. Res. 71/199, Right to Privacy in the Digital Age, preamble (Dec. 19, 2016); Human Rights Council Res. 34/7, Right to Privacy in the Digital Age, preamble (Mar. 23, 2017).

electronic records violated Article 8); *Sommer v. Germany*, App. No. 73607/13 (Eur. Ct. H.R. Apr. 27, 2017) (collecting and storing a person's electronic records constitutes an interference with Article 8).[5]

For decades, therefore, international human rights mechanisms have concluded that the unauthorized processing of personal data infringes on the right to privacy, and have emphasized the importance of data-protection laws in enforcing that basic right. For example, the United Nations has addressed privacy on multiple occasions, and has issued standards and guidance for countries legislating on the subject. As early as 1988, the U.N. Human Rights Committee, the treaty body charged with monitoring implementation of the ICCPR, recognized the need for data-protection laws to safeguard the fundamental right to privacy recognized by Article 17 of the ICCPR:

> The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be

---

[5] Relatedly, and contrary to the Government's contention that an individual's right to privacy is not violated until the moment data is disclosed to law enforcement (Br. at 26-32), international human rights law recognizes a violation of the right to privacy at the moment when data is copied. The European Court of Human Rights has emphasized this point in the context of Article 8 of the ECHR. In *Weiser v. Austria*, for example, the court held that the copying of electronic data constituted a "seizure" of that data, which interfered with the complainant's right to privacy under Article 8. 46 Eur. H.R. Rep. 54, ¶ 61; *see also San Marino*, App. No. 28005/12, ¶¶ 54-55 ("It is undeniable that copying constitutes a way of acquiring and therefore seizing data" and "amounts to interference for the purposes of Article 8.").

> regulated by law. ... [E]very individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files … have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

U.N. Doc. HRI/GEN/1/Rev.9, General Comment No. 16: Article 17, ¶ 10.

In 2011, the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression issued a report similarly noting that "the protection of personal data represents a special form of respect for the right to privacy." U.N. Doc. A/HRC/17/27, ¶ 58 (May 16, 2011). The Report further noted that "[t]he necessity of adopting clear laws to protect personal data is further increased in the current information age, where large volumes of data are collected and stored by intermediaries, and there is a worrying trend of States obliging or pressuring these private actors to hand over information of their users." *Id.* ¶ 56. In December 2016, the U.N. General Assembly passed by consensus a Resolution on the Right to Privacy in the Digital Age, G.A. Res. 71/199, which reaffirmed previous General Assembly resolutions on the subject, and emphasized that "States must respect international human rights obligations regarding the right to privacy … when they require disclosure of personal data from third parties, including private

companies." G.A. Res. 71/199, at 3; *accord* Human Rights Council Res. 34/7.

The recognition by international human rights law that the right to privacy includes a right to data protection is reflected in the Charter of Fundamental Rights of the European Union, which includes both a right to privacy (Article 7) and an independent right to data protection (Article 8). Applying the Charter, the Court of Justice of the European Union ("CJEU") has held that the mere retention of usage data, even if it is never accessed, interferes with both of these rights, thereby making clear the link between the right to privacy and the right to data protection. *See* Joined Cases C-293/12 & C-594/12, *Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine & Nat. Res.*, ECLI:EU:C:2014:238, ¶ 29 (Apr. 8, 2014). The CJEU recognized that "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance." *Id.* ¶ 37. Thus, the Court held, "[t]he retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data-protection requirements arising from that article." *Id.* ¶ 29 (citing Joined Cases C-92/09 & C-93/09, *Volker und Markus Schecke Gbr v. Land Hessen*, ECLI:EU:C:2010:662, ¶ 47 (Nov. 9, 2010)).

B. Numerous Foreign Governments Have Developed Specific Legal Regimes to Protect Individuals' Data from Unwanted Intrusion

Reflecting the fundamental right to privacy embodied in international law, governments around the world have enacted specific laws that seek to limit unauthorized data processing by both state and private actors. Most directly relevant to this case, European Union law (as implemented by E.U. member states) regulates when, how, and to what extent private entities and governments may process people's personal information and transfer it to third parties or foreign countries.

More specifically, both the Data Protection Directive ("DPD") and the General Data Protection Regulation ("GDPR"), which will soon replace the DPD as the data-protection regulatory structure for the entire European Union, prohibit data transfers to countries outside the E.U. absent specific exceptions. *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) ("DPD"); Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) ("GDPR"). This framework is rooted in the fundamental right to privacy (*see, e.g.*, GDPR, art. 1, recitals 1, 2, 11), and has grown to embrace a variety of industries and the technological developments of the internet era. *See, e.g.*, Article 29 Working Party, Opinion 05/2012 on Cloud Computing (July 1, 2012) (interpreting DPD principles in the context of cloud computing within the E.U.). The protections for personal data provided by both E.U. and Irish law are discussed in detail below. *See infra* Section I.D.

Today, more than 120 countries around the world have enacted comprehensive data-protection legislation

detailing access and disclosure requirements for personal data, and several other countries are in the process of passing such laws. *See* Graham Greenleaf, *Global Tables of Data Privacy Laws and Bills*, 145 Privacy L. & Bus. Int'l Rep. 14-26 (2017). These regulatory frameworks are diverse, but they are all designed to protect individuals' data and reflect a judgment that such protections are an important aspect of individual rights. A few examples illustrate the nature of these protections.

In Argentina, the Personal Data Protection Law sets out a statutory framework for processing personal data. Section 5 requires that an individual data subject give express, written consent before her data is processed. Argentina Personal Data Protection Law, No. 25,326, § 5 (Oct. 30, 2000) ("PDPL"). Sections 5 and 12 specify that transfers of data outside of Argentina are only permitted when the transferee country has ensured an "adequate" level of data protection or unless a specified exception applies, such as international judicial cooperation. *Id.* §§ 5, 12. In addition, the Argentine Constitution gives citizens a right to access and amend personal data stored by both public and private entities. Argentine National Const., § 43.

South Korea enshrines the right to privacy in its constitution, S. Korean Const., art. 17, and has enacted a comprehensive regulatory system for data processing and transfer. *See* S. Korea Personal Information Protection Act (Sept. 30, 2011) ("PIPA"). PIPA expressly gives individuals the right to be informed of processing, to consent to processing, to access processed information, to suspend processing, and to request that their data be corrected or deleted. *Id*. arts. 35-37, 50. To transfer an individual's personal information to an overseas entity, South

Korea's Act on the Promotion of IT Network Use and Information Protection ("Network Act") requires a data processor to first obtain the user's consent regarding the information at issue, the destination, the third party's name and contact information, and the third party's stated purpose. *See* Network Act, art. 21. Requests from foreign law enforcement entities are exempted from these requirements, but must be routed through an appropriate MLAT or similar agreement. *Id.*; PIPA, art. 18(6).

In Australia, the thirteen "Australian Privacy Principles" govern the lawful collection, use, and disclosure of data by corporations. Australia Privacy Amendment (Enhancing Privacy Protection) Act, sched. 1 (No. 192, 2012). For example, Principle Six prohibits the disclosure of personal information absent either consent by the individual or a specifically enumerated exception, such as authorization by an Australian law or court order. *Id.* To transfer any data outside of Australia, a data processor also must ensure that the recipient abides by the same Principles. Australia's Information Commissioner, a legislatively-created position, is vested with authority to enforce the Principles, and has a range of powers which include auditing compliance and seeking both injunctive relief and civil penalties for violators (up to $400,000 for individuals and $2.1 million for corporations). Privacy Amendment Act, at 194, § 80W(5); Australia Crimes Act (No. 12, 1914), Compilation No. 118, at 219, § 4AB (Sept. 20, 2017).

C. Foreign Governments Have Entered into Specific Agreements to Regulate International Data Transfers and Law Enforcement Data Requests

In light of the increasing importance and variety of data-protection regimes around the world, states today generally recognize each other's right to protect data privacy consistent with international standards. This is evident from the various agreements and treaties that countries have entered into to harmonize data transfers to and from other states. Without these agreements, countries and companies would face daunting compliance costs and the rate of international cooperation and commerce would suffer. The rights to privacy and data protection would likewise be impaired if nations resorted to directly seizing data held abroad outside the procedures established by these international, regional, and national legal frameworks—exactly the power the U.S. Government seeks in this case.

Mutual legal assistance treaties ("MLATs") are one of the dominant mechanisms for governing cross-border law enforcement requests for data transfers. The United States is currently a party to over 70 of these treaties with different governments around the world. *See* U.S. Dep't of State, Bilateral Treaties in Force as of Jan. 1, 2017, https://perma.cc/8BXX-WFA7; Charles Doyle, Congressional Research Service, *Extraterritorial Application of American Criminal Law*, at 23 (Oct. 31, 2016). As applicable here, the MLAT between the U.S. and Ireland ("U.S.-Ireland MLAT") provides for mutual assistance "in connection with the investigation, prosecution, and prevention of offenses," including in the "execution [of] requests for searches and seizures." U.S.-Ireland MLAT, art. 1(1)-(2)(f), Jan. 18, 2001, S. Treaty Doc.

107-9. Article 14 of the treaty sets out specific procedures for search and seizure, including requests for the search, seizure, and delivery of any item in the territory of the requested party. *Id.* art. 14(1).

The U.S.-Ireland MLAT is supplemented by the U.S.-E.U. MLAT, which was specifically negotiated by the U.S. and the E.U. to aid in cross-border investigations and overhaul evidence and extradition procedures across the Atlantic. It was entered into as part of a comprehensive effort to consolidate those procedures and minimize red tape. *See* U.S.-E.U. MLAT, at v (Executive Summary), June 25, 2003, S. Treaty Doc. No. 109-13. The U.S.-E.U. MLAT provides "for the use of expedited means of communication in addition to any authority already provided under bilateral treaty provisions." *Id.* art. 3(1)(d).

In addition, the U.S. and the E.U. have concluded an "Umbrella Agreement" to provide privacy and data-protection safeguards, including judicial redress, for personal data transferred under U.S.-E.U. MLATs, or otherwise exchanged between U.S. and E.U. law enforcement authorities. Umbrella Agreement, 2016 O.J. (L 336) 5.[6] Beyond the MLAT process, law enforcement data requests between the U.S. and E.U. may also proceed under two sector-specific frameworks, one on financial data (the Terrorist Finance Tracking Programme ("TFTP") Agreement, 2010 O.J. (L 195) 5), and one on airline passenger name records (the Passenger Name Record ("PNR") Agreement, 2012 O.J. (L 215) 5).

---

[6] While there are ongoing debates about whether to make additional changes to the MLAT process, that does not justify the U.S. Government's outright avoidance of that process by issuing extraterritorial warrants.

In addition to these bilateral agreements, the Budapest Convention on Cybercrime, a multiparty treaty ratified by the U.S. and signed by every E.U. member state, provides a streamlined mechanism to facilitate cross-border data requests between law enforcement authorities. *See* Chart of Signatures and Ratifications of Treaty 185, https://perma.cc/XU59-CEGY. As relevant here, the Budapest Convention creates a specific framework for cross-border requests. For example, it requires signatories to "adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

> (a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
>
> (b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control."

Council of Europe, Convention on Cybercrime, art. 18 (Nov. 23, 2001).[7]

Significantly, these transnational mechanisms all contemplate that government requests for data be routed through official channels using procedures

---

[7] Outside the E.U., the U.S. and Australia have entered into similar agreements on multiple occasions. *See* Memorandum of Understanding on Enhancing Cooperation in Preventing and Combating Crime, U.S.-Austl., Nov. 16, 2011; Agreement for the Sharing of Visa and Immigration Information, U.S.-Austl., Aug. 27, 2014, TIAS 14-1212.

established by the governments that are parties to the agreements. Those channels are specifically tailored to accommodate differences in regulatory standards and the needs of law enforcement. These agreements generally do not authorize law enforcement to obtain information held in one country merely by presenting a request to a private company in another country. As discussed below, moreover, the data-protection laws of many foreign jurisdictions (including the E.U.) specifically require that international law enforcement requests for individuals' data comply with the MLAT procedure. *See* Letter from Viviane Reding to Sophie in 't Veld, Member of the European Parliament (June 24, 2014), https://perma.cc/TF5X-V377 ("[W]here governments need to request personal data held by private companies and located in the EU, requests should not be directly addressed to the companies but should proceed via agreed formal channels of co-operation between public authorities, such as the mutual legal assistance agreements or sectorial EU-US agreements authorising such transfers."); *see also* U.S.-E.U. Q&A Excerpt from Press Conference (Jan. 4, 2018), https://perma.cc/3STM-3LAJ (French government asserting that MLATs must be used for transatlantic data transfers).

D. Allowing the United States to Use a Warrant to Obtain Personal Data Stored Abroad Would Conflict with Irish and European Law

The data at issue in this case are emails stored by Microsoft in Dublin, Ireland. These emails constitute personal information that is specifically protected by the data privacy laws in that country. Irish data-privacy laws do not allow for the transfer of those emails outside of Ireland in response to the warrant

in this case. For the United States to seize such foreign-stored data by issuing a warrant to a private company would circumvent both the applicable data-protection regime and the MLAT process, thereby undermining prior efforts by the Executive and Legislative branches to facilitate international cooperation in criminal investigations.

As a party to the ECHR and an E.U. member state, Ireland has committed to protecting the fundamental rights to privacy and protection of personal data. Ireland does so in part through the Irish Data Protection Act, which implements the DPD, as well as through the upcoming GDPR, which will replace the DPD and apply directly in all E.U. member states beginning in May 2018.[8] Chapter 5 of the GDPR provides four general grounds for lawfully transferring data to countries outside the E.U.: (1) an "adequacy decision," "where the Commission has decided that the third country … ensures an adequate level of protection" for personal data (GDPR, art. 45); (2) the combined provision of an "appropriate safeguard[]," such as a contractual tool or legally binding rule, plus the availability of "enforceable data subject rights and effective legal remedies for data subjects" (*id.* arts. 46-47); (3) one of

[8] Because the GDPR is poised to officially supplant the DPD this year, this discussion focuses primarily upon the structure and text of the GDPR. As a "regulation," the GDPR will become binding law in E.U. member states when it comes into effect on May 25, 2018, and will not require implementing legislation. Treaty on the Functioning of the European Union, 2012 O.J. (C 326) 47, art. 288 Notwithstanding the forthcoming change of regime, the DPD and GDPR share much of the same DNA, and the following analysis of the GDPR generally applies equally to the DPD, which was in force during prior proceedings in this case.

a specified list of "derogations for specific situations" (*id.* art. 49); or, alternatively, (4) the existence of an "international agreement, such as a mutual legal assistance treaty" (*id.* art. 48).

Only the fourth ground, the existence of an MLAT or other international agreement, could potentially have applied to permit the data transfer sought in this case.[9] But, by attempting to seize data held in Ireland with a warrant served on a private company in the United States, the U.S. Government has acted in direct conflict with this provision of E.U. law. Article 48 of the GDPR was adopted specifically to address circumstances where "third countries adopt … legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States"—

---

[9] It is unclear whether the other grounds are permissible alternatives for lawfully transferring data to countries outside the E.U. in the law enforcement context. Nevertheless, even if they were, they could not operate to permit the data transfer sought in this case. No transfer could have been based on the first ground (adequacy) because the Commission does not currently recognize the United States as providing an adequate level of protection. *See* GDPR, art. 45; European Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries, https://perma.cc/8BAX-XHVG. The second ground could not apply because the warrant in this case was not subject to any recognized safeguards (GDPR, art. 46(2)-(3)), nor was the requested data sought "on condition that enforceable data subject rights and effective legal remedies for data subjects are available" (*id.* art. 46(1)). Finally, the third ground could not apply because none of the derogations specified in Article 49 apply here. *See* GDPR, arts. 49, 85-91; *see also* Statement of the Article 29 Working Party, at 9 (Nov. 29, 2017), https://perma.cc/NSM9-7RVL (explaining that international agreements such as MLATs generally must be obeyed when law enforcement authorities in third countries request access or disclosure from EU data controllers).

including court orders requiring the transfer or disclosure of personal data, which are not based on an applicable international agreement. GDPR, recital 115. Article 48 provides that "[a]ny judgment of a court ... of a third country requiring a controller or processor to transfer or disclose personal data *may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty,* in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter." *Id.* art. 48 (emphasis added).

In other words, the law applicable in Ireland, where the data at issue is located, specifically prohibits law enforcement demands for personal data through warrants that proceed outside the MLAT process. As the Article 29 Working Party,[10] has explained:

> EU data protection law provides that existing international agreements such as a mutual assistance treaty (MLAT), must—as a general rule—be obeyed when law enforcement authorities in third countries request access or disclosure from EU data controllers. The circumvention of existing MLATs or other applicable legal basis under EU law by a third country's law enforcement

[10] The Article 29 Working Party is the principal E.U. advisory body on E.U. data-protection law. Constituted under Article 29 of the E.U. DPD (Council Directive 95/46), it is composed of representatives from all 28 E.U. member states' data-protection authorities ("DPAs"). The Article 29 Working Party's opinions and interpretations of the law are frequently cited by E.U. and national courts, and relied upon by national DPAs.

> authority is therefore an interference with the territorial sovereignty of an EU member state.

Statement of the Article 29 Working Party, at 9 (Nov. 29, 2017), https://perma.cc/NSM9-7RVL; *accord* Letter from European Union's Article 29 Working Party to Satya Nadella, CEO of Microsoft (Sept. 22, 2014), https://perma.cc/48VG-3Z27; Br. of the European Commission on Behalf of the E.U. as Amici Curiae in Supp. of Neither Party at 8-12.

The warrant at issue here runs squarely afoul of this requirement. If enforced, it would bring about the seizure by U.S. law enforcement authorities of personal data held in Ireland without the Government going through the channels created for that purpose by the MLAT process. As such, interpreting U.S. law to authorize such a warrant would directly conflict with the Irish and E.U. laws protecting the emails at issue where they actually reside. That result would undermine both the right to privacy in the personal information contained in those emails and the interests that Ireland and the E.U. have in protecting such data by directing that law enforcement demands proceed through the channels designated specifically for this scenario.

E. The Extraterritorial Warrant Authority the Government Seeks Would Lead to Conflicts with Other Data-Protection Regimes Around the World

These concerns extend far beyond this specific warrant. Indeed, this case is just the tip of the iceberg in terms of the conflicts between U.S. and foreign law that would arise by allowing the Government to obtain warrants under the SCA for personal data stored outside the United States.

As noted above, over 120 countries around the world have enacted comprehensive data-protection legislation, and several other countries are in the process of passing such laws. *See* Greenleaf, *supra*, at p. 13. As relevant here, these data-protection regimes have several features that stand in the way of the extraterritorial warrant procedure that the Government seeks to obtain under the SCA.

Most importantly, like the E.U. regime discussed above, many countries require that all data requests from foreign authorities proceed through an established MLAT or other bilateral agreement. *See, e.g.*, Argentina PDPL, § 12(2)(e); S. Korea PIPA, art. 18(6); S. Korea Network Act, art. 21; Ley Federal de Protección de Datos Personales en Posesión de Los Particulares (Mexico Data Protection Law), art. 37(I) (July 6, 2010); Protección de Datos Personales y Acción de "Habeas Data" (Uruguay Data Protection Law), Law No. 18.331, art. 23 (Aug. 11, 2008); *see also* Organization of American States, Inter-American Convention on Mutual Assistance in Criminal Matters, https://perma.cc/RTH3-E5AK. The United States has entered into MLATs with the countries in each of these cited examples. *See* U.S. Dep't of State, Bilateral Treaties in Force as of Jan. 1, 2017, at 11 (Argentina), 250 (S. Korea), 292 (Mexico), 473 (Uruguay), https://perma.cc/8BXX-WFA7. It would therefore violate their respective data-protection laws for the U.S. Government to circumvent the MLAT framework by demanding the direct transfer of personal data from a private service provider.

In addition, and absent specified exceptions (such as compliance with an MLAT or other international agreement), many jurisdictions also may require an "adequacy" determination by the country's regulators

before data may be exported abroad, or may require that a transferer obtain an individual's "consent" before information may be processed and exported to a foreign country.[11] An adequacy decision usually involves examining the data-protection and privacy laws (and practices) of the country requesting transfer, and determining whether its regime satisfies certain standards. Argentina, for example, keeps an updated list of the countries deemed "adequate." Argentina Regulation 60-E/2016 (Nov. 18, 2016). Japan's Protection of Personal Information Act ("PPIA"), as amended in 2017, similarly includes a plan to "white list" those countries which have "adequate" data-protection laws. Japan Act on the Protection of Personal Information, No. 57 (May 30, 2003, as amended May 30, 2017). As an example of an individual consent requirement, South Korea's Network Act confers a right for individuals to be informed of, and consent to, the destination of their data and the purpose for which it was requested. *See* Network Act, art. 21; PIPA, art. 18(2)(6). Uruguay likewise mandates that, before such a transfer takes place, individuals must provide "free, prior, express and informed consent, which must be documented." *See* Law No. 18.311, art. 23.

The warrant procedure that the Government seeks would not have complied with either of these types of transfer regulations. The United States has not been designated as adequate by Argentina and it is

[11] It is not necessarily the case in each of these jurisdictions that adequacy and/or consent operate as permissible alternatives to the MLAT process for law enforcement data requests. But even if they were, in the examples described above neither adequacy nor consent could operate to permit the data transfer sought in this case.

unlikely to qualify for Japan's "white list." *See* Regulation 60-E/2016, art. 3; Stephen Gardner, *Moving Data Between Japan, U.S.? Use Asia Privacy Rules System*, Bureau of National Affairs, Sept. 27, 2017, https://perma.cc/XF5D-6MCY (quoting PPIA international affairs official indicating status of current white list discussions between Japan and E.U. and U.S.). Similarly, U.S. legal provisions that permit delayed notice would likely conflict with the notice and consent requirements of other regimes. *See* Fed. R. Crim. P. 41(f)(3) (allowing judges issuing warrants to allow for delayed notice); 18 U.S.C. § 2705 (same).

In short, the Government's expansive construction of the SCA to authorize extraterritorial warrants threatens widespread conflict between U.S. law and foreign data-protection regimes. Such conflict would both erode the powerful interests that foreign governments have in protecting data held within their borders and threaten the fundamental individual liberties that these laws protect. Beyond all that, the Government's approach puts a wide range of private companies that store user data—including email service providers, cloud-hosting platforms, internet service providers, and countless others—in the untenable position of having to choose between violating the law of the country where data is actually located and disregarding a search warrant issued by the United States.

II. To Avoid Unnecessary Conflict with Foreign Law, This Court Should Not Read the SCA as Authorizing Warrants for Data Held Outside the United States

Established principles of law provide the solution to these problems. Under various doctrines, courts are instructed to interpret and apply domestic statutes in ways that minimize, rather than exacerbate, potential frictions between U.S. law and the laws of other governments. These principles apply here, and they point decisively against giving the Government broad power under the SCA to obtain warrants that allow the unilateral seizure of personal data held outside the United States, in potential violation of foreign data-protection laws.

A. Because Congress Has Not Clearly Authorized Warrants for Foreign-Held Data, the Presumption Against Extraterritorial Application Applies

"It is a 'longstanding principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States ....' This principle … rests on the perception that Congress ordinarily legislates with respect to domestic, not foreign matters." *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010) (quoting *EEOC v. Arabian American Oil Co.* (*Aramco*), 499 U.S. 244, 248 (1991)). The presumption against extraterritoriality reinforces that "United States law governs domestically but does not rule the world." *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 454-55 (2007).

Reading statutes to generally avoid extraterritorial effect helps avoid unnecessary friction between U.S. law and other countries' laws. As this Court has

explained, the presumption "serves to protect against unintended clashes between our laws and those of other nations which could result in international discord." *Aramco*, 499 U.S. at 248; *see also RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2107 (2016) ("Although 'a risk of conflict between the American statute and a foreign law' is not a prerequisite for applying the presumption against extraterritoriality, where such a risk is evident, the need to enforce the presumption is at its apex." (citation omitted)).

In order to avoid such conflict, a domestic statute will not be applied to regulate conduct, property, or persons outside of the United States unless there is a "clear indication" to the contrary. *Morrison*, 561 U.S. at 248. In *Morrison*, therefore, this Court read Section 10b of the Securities Exchange Act to not apply to sales of securities outside the United States that are not listed on a U.S. exchange, in order to avoid "the interference with foreign securities regulation that application of § 10(b) abroad would produce." *Id.* at 269. The Court explained that 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.'" *Id.* (citation omitted). Likewise, in *Aramco*, this Court read Title VII's protections against employment discrimination as not applying outside the United States in part because the statute, prior to its amendment in 1991, "fail[ed] to address conflicts with the laws of other nations." 499 U.S. at 256.

This same principle applies to the provision of the SCA at issue here. The Government seeks to apply the SCA to authorize warrants that would result in the seizure of data that resides in Ireland (and

potentially in any other foreign country). Such warrants would be an extraterritorial application of U.S. law under any ordinary understanding—they would allow the U.S. Government to directly control the copying, transfer, and use of personal property located on foreign soil. Accordingly, to apply the statute in this way, there would have to be a compelling indication that Congress actually intended that result when it enacted the SCA. But there is nothing like that here. As Judge Lynch rightly observed, "[t]here is no indication whatsoever in the text or legislative history that Congress intended [the SCA or the broader Electronic Communications Privacy Act ("ECPA")] to have application beyond our borders." Pet. App. at 57a (Lynch, J., concurring). Indeed, there is no evidence that Congress ever contemplated—much less specifically endorsed—the use of extraterritorial warrants under the SCA. The most that could be said is that the statute is ambiguous on that issue. But, as this Court has explained, "[w]hen a statute gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255. Simply put, silence and ambiguity are not enough to invite the myriad conflicts between U.S. law and foreign law that the Government's position invites.

B. International Comity Militates Strongly Against Applying U.S. Law to Authorize Warrants that Would Violate the Data-Protection Laws of Foreign Governments

Another equally established rule of statutory interpretation reinforces this result. "[T]his Court ordinarily construes ambiguous statutes to avoid unreasonable interference with the sovereign authority of other nations." *F. Hoffmann-La Roche Ltd. v. Empagran S. A.*, 542 U.S. 155, 164 (2004). This results from principles of international comity, which instruct nations "to respect the sovereign rights of other nations by limiting the reach of its laws and their enforcement." *Sosa v. Alvarez-Machain*, 542 U.S. 692, 761 (2004) (Breyer, J., concurring).

For centuries, as Justice Story observed, comity "has become incorporated into the code of national law in all civilized countries." *Van Reimsdyk v. Kane*, 28 F. Cas. 1062, 1063 (C.C.D.R.I. 1812) (No. 16,871) (Story, J.); *see also* Joseph Story, *Commentaries on the Conflict of Laws*, § 38 (2d ed. 1841) (1834) ("The phrase 'comity of nations,' … is the most appropriate phrase to express the true foundation and extent of the obligation of the laws of one nation within the territories of another."). Comity's role in keeping U.S. law in harmony with the transnational legal order dates back to the Founding era. *See, e.g.*, *Banks v. Greenleaf*, 2 F. Cas. 756, 757 (C.C.D. Va. 1799) (No. 959) (Washington, J.) (referencing Ulrich Huber, *De Conflictu Legum Diversarum in Diversis Imperiis* (Ernest G. Lorenzen trans. 1919) (1689)); *Emory v. Grenough*, 3 U.S. (3 Dall.) 369, 370 n.* (1797) (dismissing for lack of jurisdiction, but setting forth a translated extract from Ulrich Huber's treatise). As a rule of interpretation, the doctrine seeks to avoid

reading ambiguous U.S. laws in ways that "would be an interference with the authority of another sovereign, contrary to the comity of nations, which the other state concerned justly might resent." *Am. Banana Co. v. United Fruit Co.*, 213 U.S. 347, 356-57 (1909).

Like the presumption against extraterritoriality, comity seeks to avoid or minimize conflicts between different legal regimes. As this Court has explained, the doctrine "cautions courts to assume that legislators take account of the legitimate sovereign interests of other nations when they write American laws. It thereby helps the potentially conflicting laws of different nations work together in harmony—a harmony particularly needed in today's highly interdependent commercial world." *Empagran*, 542 U.S. at 164-65; *accord Sosa*, 542 U.S. at 761 (Breyer, J., concurring). Thus, while comity "is neither a matter of absolute obligation ... nor of mere courtesy and good will," *Hilton v. Guyot*, 159 U.S. 113, 163-64 (1895), its application is compelling in cases where, as here, there is a significant potential for conflicts between an expansive understanding of U.S. law and the laws of foreign nations. *See Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 798-99 (1993) (comity should apply where there is a true conflict between domestic and foreign law).[12]

---

[12] Closely related to international comity, the founding-era canon known as the "*Charming Betsy* doctrine" holds that "an act of Congress ought never to be construed to violate the law of nations if any other possible construction remains." *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804); *accord Weinberger v. Rossi*, 456 U.S. 25, 32 (1982) (statute should not be construed to abrogate international agreements absent clear Congressional intent). Just as comity encourages construction of federal laws to avoid conflicts with the laws of

In keeping with these principles, this Court has regularly applied comity to limit the reach of U.S. laws that would otherwise create friction with the laws of other countries. *See, e.g.*, *N.Y. Cent. R.R. v. Chisholm*, 268 U.S. 29, 32 (1925) (referring to "comity of nations" in holding that Federal Employers' Liability Act could not be applied to assert cause of action based on injuries sustained in Canada); *Lauritzen v. Larsen*, 345 U.S. 571, 582, 592-93 (1953) (citing "considerations of comity" in holding that Jones Act did not apply to claim brought by a Danish seaman to recover for injury on a Danish ship); *Spector v. Norwegian Cruise Line Ltd.*, 545 U.S. 119, 130 (2005) (plurality opinion) (Kennedy, J.) (invoking "international comity" in concluding that the Americans with Disabilities Act does not apply to matters affecting internal affairs of foreign-flag ships). In *Empagran*, for example, this Court invoked comity as a reason for declining to extend the Sherman Act to certain foreign anticompetitive conduct. 542 U.S. at 169. There, comity was useful in helping to avoid "an act of legal imperialism, through legislative fiat" by applying U.S. law to regulate foreign conduct involving foreign injury. *Id.* at 169. Likewise, in *McCulloch v. Sociedad Nacional de Marineros de Honduras*, 372 U.S. 10, 20-21 (1963), this Court held that the NLRA does not apply to foreign-flagged vessels in light of the "possibility of international discord" that would be created—especially the friction resulting from "the concurrent application of the Act and the Honduran Labor Code that would result with our approval of jurisdiction."

---

foreign nations, the *Charming Betsy* doctrine serves the complementary purpose of preventing interpretations of federal laws that would violate international law.

These principles apply here, and counsel in favor of a more limited application of the warrant power authorized by the SCA. The Government seeks to read an at-best ambiguous statute to confer upon it the power to seize data held within the territory of a foreign nation and protected by that country's laws. That result would create clear conflicts between U.S. law and the laws of a potentially wide array of foreign governments, specifically including Ireland in this case. As discussed above, such laws are an important expression of the rights of those governments to protect both data located in their territory and the individual right to privacy in such data, as recognized by international human rights law.

The government's approach would create additional international friction by undermining the MLAT process. As discussed above, the United States is currently a party to over 70 MLATs with different governments, each of which includes detailed, negotiated procedures for law enforcement evidence gathering between the U.S. and independent nations. And, according to the laws governing many of those jurisdictions (including Ireland and the E.U.), the MLAT procedure is the required mechanism for a foreign government's law enforcement officials to obtain data located in another sovereign's territory for purposes of general criminal investigations. Comity counsels powerfully against an interpretation of U.S. law that would allow the Executive to override the determinations that foreign partners have made to regulate law enforcement data requests within their territory. *Accord Société Nationale Industrielle Aérospatiale v. District Court*, 482 U.S. 522, 546 (1987) ("American courts should therefore take care to demonstrate due respect … for any sovereign interest expressed by a foreign state"). Applying

comity in this fashion would also reinforce the broader principles underlying the doctrine, by encouraging cross-border cooperation. *See, e.g.*, *id.* at 555 (Blackmun, J. concurring) (comity principles "reflect the systemic value of reciprocal tolerance and goodwill"); *JP Morgan Chase Bank v. Altos Hornos de Mexico*, 412 F.3d 418, 423 (2d Cir. 2005) ("[I]nternational comity is clearly concerned with maintaining amicable working relationships between nations" (citation omitted)).

Beyond all that, considerations of comity apply here because to allow the U.S. Government to issue search warrants that require derogation of foreign data-protection laws would put the electronic communications service providers who receive those warrants in an untenable position—caught between conflicting legal regimes where "compliance with the laws of both countries is otherwise impossible." *Hartford Fire*, 509 U.S. at 799. The comity doctrine is intended to prevent exactly that result. *See, e.g.*, *Empagran*, 542 U.S. at 167-69 (comity discourages application of U.S. law to regulate foreign conduct where U.S. law differs from that of the foreign nation and where the countries "disagree dramatically" about how their laws should be enforced); *In re Vitamin C Antitrust Litig.*, 837 F.3d 175, 194 (2d Cir. 2016) (addressing, in the context of comity, the level of deference owed to a foreign government's interpretation of its own laws when that interpretation requires a party "to comply with conflicting legal requirements"), *cert. granted in part*, No. 16-1220, 2018 WL 386563 (Jan. 12, 2018).

For these reasons, comity requires, at a minimum, that the SCA not be read to allow for extraterritorial search warrants without the clearest indication that Congress intended to confer that power. The statute's

complete silence on that question requires that it be read narrowly, to minimize transnational friction and better respect the rights of other governments to protect data in their own territories. This Court should reject a reading of federal law that would allow the Government to bring about widespread conflict with foreign laws and interfere with the authority of foreign sovereigns in ways that Congress never contemplated.

CONCLUSION

The Government's bid for a warrant power that would allow it to obtain electronic information located outside the United States would create serious conflicts between U.S. law and a broad range of foreign laws that protect individual privacy and human rights. Because Congress has not clearly authorized that sweeping result, this Court should reject it and affirm the judgment of the Second Circuit.

Respectfully submitted,

BRIAN M. WILLEN
Counsel of Record
BASTIAAN G. SUURMOND
WILSON, SONSINI, GOODRICH
& ROSATI, P.C.
1301 Avenue of the Americas,
40th Floor
New York, New York 10019
(212) 999-5800
bwillen@wsgr.com
bsuurmond@wsgr.com

LAUREN GALLO WHITE
RYAN T. O'HOLLAREN
WILSON, SONSINI, GOODRICH
& ROSATI, P.C.
One Market Plaza Spear Tower,
Suite 3300
San Francisco, California 94105
(415) 947-2000
lwhite@wsgr.com
rohollaren@wsgr.com

CAROLINE WILSON PALOW
SCARLET KIM
PRIVACY INTERNATIONAL
62 Britton Street
London, EC1M 5UY
United Kingdom
caroline@privacyinternational.org
scarlet@privacyinternational.org

Attorneys for Amici Curiae

APPENDIX

APPENDIX

AMICI CURIAE

Artículo 12 is a non-profit organization that defends the fundamental rights to privacy and data protection of all people in Mexico, but also throughout Latin America, in particular the rights of Internet and other information and communication technology users in the digital realm. It takes its name from Article 12 of the Universal Declaration of Human Rights of the United Nations, which guarantees the right to privacy.

Asociación por los Derechos Civiles ("ADC") is a non-governmental, non-partisan organization, created by a group of lawyers in 1995 to contribute to strengthening the legal and institutional culture that guarantees the fundamental rights of individuals, based on respect for the Constitution and democratic values. ADC promotes civil and social rights in its base country, Argentina, as well as in other Latin American countries through collaboration with partners in the region.

Members of the **Association of Spanish Constitutionalists ("ACE")** are professors and specialists in constitutional law, who seek to contribute to the improvement of research and teaching in this discipline. They join this brief in their individual capacity to express their concern regarding the guarantees of the right to privacy in communications and the right to data protection threatened in this case. The members of ACE who join this brief are:

- Mª Josefa Ridaura Martinez, Professor of Constitutional Law, University of Valencia; Secretary General, ACE

- Ignacio Villaverde, Professor of Constitutional Law (Chair), Secretary of the Social Council, University of Oviedo; Member, Board of Directors, ACE
- Luis Jimena Quesada, Professor of Constitutional Law (Chair), University of Valencia; Representative of Spain, European Committee of Social Rights, Council of Europe
- Enrique Belda Pedrero, Professor of Constitutional Law, University of Castilla-La Mancha; Member, Legal Advisory Council, Region of Castilla-La Mancha
- Rosario Serra Cristobal, Professor of Constitutional Law, University of Valencia
- Miryam Rodriguez Izquierdo, Professor of Constitutional Law, University of Sevilla
- Monica Arenas Ramiro, Professor of Constitutional Law, University of Alcalá de Henares
- Joaquin Sarrion Esteve, Ramon y Cajal Researcher, Professor of Constitutional Law, University UNED
- German Teruel Lozano, Professor of Constitutional Law, University of Murcia
- Fernando Perez Dominguez, Professor of Constitutional Law, University of Huelva

- Monica Martinez Lopez-Saez, Predoctoral researcher (FPU-MECD) in Constitutional Law
- Leire Burguera Ameave, Professor of Constitutional Law, University of UNED

The Australian Privacy Foundation is the primary association dedicated to protecting the privacy rights of Australians. The Foundation is a non-government organization and aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. It has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation is active on a wide range of privacy issues and works with consumer organizations, civil liberties councils, professional associations and other community groups on specific privacy issues.

Bits of Freedom is a non-profit, digital rights organization in the Netherlands, focusing on privacy and freedom of communication online. Working at the cutting edge of technology and law, Bits of Freedom strives to influence legislation and self-regulation, and empower citizens and users by advancing the awareness, use, and development of freedom-enhancing technologies.

Civil Rights Defenders is an independent non-profit organization that strives to defend people's civil and political rights in Sweden and internationally and to empower human rights defenders at risk. Issues that Civil Rights Defenders focus on include surveillance, data collection, and the rights to privacy and integrity both off- and online. To ensure that international human rights standards are upheld,

Civil Rights Defenders engages in strategic litigation. For this reason, Civil Rights Defenders has an interest in informing the Court about relevant human rights standards in this case.

Derechos Digitales América Latina is a digital rights organization based in Santiago de Chile, which focuses its work on the impact of digital technologies on the rights to freedom of expression, privacy, and access to knowledge in Latin America. Derechos Digitales' mission is to defend, promote, and develop human rights in digital environments using advocacy tools to inform policymakers, private companies, and the general public of Latin America. Founded in 2005, Derechos Digitales' work combines legal research, public policy, technology analysis, advocacy, and communications outreach. Derechos Digitales participates selectively in human rights litigation, including through direct public interest litigation in Chile, and by filing amicus briefs in Latin America and Europe. Derechos Digitales has an interest in this case, arising from its potential impact on the rights of technology users throughout the Latin American region.

The Digital Freedom and Rights Association ("DFRI") is a Swedish non-profit and non-partisan organization that promotes digital rights. DFRI's goal is a society with as little surveillance, tracking and wiretapping as possible. DFRI believes in freedom of speech, transparency and freedom of information, personal integrity, and the individual right to control the use of personal information and digital footprints.

Elektronisk Forpost Norge (Electronic Frontier Norway) ("EFN") is a cross-profession and cross-political organization furthering civil rights, privacy, freedom of expression, and the right to share. EFN

works for an open and democratic infrastructure and the use and availability of information in digital networks and the digital society. EFN believes that the digital society is comprised of technology, society and culture: hardware, software, storage, formats, protocols, digital communications, digital communities, and social media. EFN seeks to further the development of free culture, cultural and knowledge commons, free licenses, and a sharing culture.

European Digital Rights ("EDRi") is an association of 35 civil and human rights organizations (https://edri.org/members/) with members in 19 European countries and beyond. EDRi defends and promotes rights and freedoms in the digital environment. It focuses on the rights to privacy, data protection and freedom of expression and opinion online. Founded in June 2002, EDRi established an office in Brussels in 2009. EDRi (with the exception of its members Digital Ireland, the Electronic Frontier Foundation, and Open Rights Group) joins this amicus brief because of the international implications this case will have on the defense of privacy, data protection, and freedom of expression in the digital age. EDRi believes that appropriate and predictable frameworks for access to data for law enforcement purposes are essential to ensure human rights are protected.

Fundación Datos Protegidos is a non-profit organization based in Chile and formed in 2015 with the purpose of promoting and reinforcing the rights to privacy and personal data protection. Datos Protegidos supports public debate at the national and regional levels, which promotes the dignity, equality, and liberty of individuals in relation to privacy.

Fundación Karisma is a Colombian non-profit organization that responds to opportunities and threats arising in the context of "technologies for development," especially as they relate to the respect for human rights, personal freedoms and social equality. Founded in 2003, Karisma is one of the leading Latin American civil society organizations working on the promotion of human rights in the digital environment. Karisma's current priorities are access to knowledge, security and privacy, social innovation, freedom of expression, Internet governance, and gender and social equality, as they relate to information and communications technologies. Karisma has participated as amicus curiae in cases of freedom of expression and privacy before the Colombian Constitutional Court.

The Foundation for Information Policy Research ("FIPR") is an independent body that studies the interaction between information technology and society. FIPR's goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the U.K. and Europe.

Hiperderecho is a Peruvian non-profit organization founded in 2012 working to promote human rights in digital environments. Hiperderecho's mission is to enrich the public debate by promoting a wider understanding of technology policy issues and representing users' interests in public debates and legislative processes. Hiperderecho believes in the liberating power of technology and seeks to promote policies that respect that power and enhance it.

Human Rights Watch ("HRW") began reporting on abuses connected to the practice of state surveillance more than three decades ago as Helsinki Watch, and has continued ever since, with particular focus on mass surveillance practices since 2013. HRW's reports detail abuses of rights connected to surveillance around the globe (for example, in China, Ethiopia, Saudi Arabia, and the U.S.), and its advocacy involves legal analysis and submissions on the various legal authorities (actual or proposed) for surveillance practices to the relevant bodies of the United Nations ("U.N."), the U.S., the U.K., the U.N. High Commissioner for Human Rights, the Special Rapporteur for Freedom of Expression, the Special Rapporteur on Privacy, as well as analysis of the laws of many other countries in respect of these issues.

International Cyber Law Studies in Korea is a non-profit academic organization focused on the legal aspects of digital trade, data privacy, and cybersecurity. It promotes democratic values within an open, secure, stable, accessible, and peaceful ICT environment. It fully supports the protection of the fundamental right to privacy, as recognized by international human rights law, and the development of the MLAT process with respect to data.

IPANDETEC is a digital rights organization based in Panama City, Panama dedicated to promoting the use and regulation of ICTs and the defense of human rights in the digital environment. IPANDETEC focuses its work on data protection, privacy, Internet governance and open data. It represents the interests of Internet civil society in Panama and groups such as human rights defenders, activists, journalists, LGBTI, Afro-Panamanians, etc. Currently, IPANDETEC is trying to extend its work in other countries in Central America.

The Italian Coalition for Civil Liberties and Rights ("CILD") is a network of 35 civil society organizations founded in 2014 that protects and expands the rights and liberties of all, through a combination of advocacy, public education, and legal action. CILD works on asylum and international protection, migration, equality and anti-discrimination, justice, digital rights, and national security. In 2016 CILD developed the Civil Liberties in the Digital Age Programme, whose aim is to advance and expand human rights standards on the right to privacy, freedom of expression, association or movement, as well as limit mass surveillance and advocate for better oversight of intelligence and surveillance activities by the government. CILD does so through a combination of advocacy campaigning, lobbying, and strategic litigation.

La Quadrature du Net ("LQDN") is a French non-profit organization acting for the political and legal defense of human rights in the digital age. LQDN informs citizens about policy proposals and technological developments that adversely affect rights like freedom of expression and privacy on the Internet. It organizes advocacy campaigns at the French and European levels to promote sustainable, rights-respecting and empowering policies regarding digital technologies. Through the litigation working group "Les Exégètes amateurs," LQDN also works with French non-profit Internet access providers to challenge French and European surveillance and censorship laws in court. Over the past couple of years, it has successfully challenged blanket provisions regarding the surveillance powers of French intelligence agencies before the Council of State. Among other such initiatives, LQDN has also introduced a challenge before the Court of Justice of

the European Union regarding the "Privacy Shield" agreement between the United States and the European Commission.

Liberty (formally known as the **National Council for Civil Liberties)** is a cross-party, non-party membership organization founded in 1934. Liberty engages in campaigning, public education, lobbying, litigation, and the provision of free legal advice and information in order to promote civil liberties and human rights in the U.K., including the right to privacy and appropriate limits on government power. Liberty has led public opposition to, and European litigation challenging, the U.K.'s surveillance regime, including legal challenges to the U.K.'s Interception of Communications Act 1985, Regulation of Investigatory Powers Act 2000, Data Retention and Investigatory Powers Act 2014, and Investigatory Powers Act 2016. It has lobbied for greater privacy protections for personal data in the U.K. and the European Union.

Open Net (also known as **"Open Net Korea"** or **"Open Net (Korea)")** is a public interest association incorporated in South Korea in December 2012. Open Net engages in legislative lobbying, impact litigation, public campaigns, education, and research dedicated to protecting the Internet as an open space for democracy, equality, and collaboration. Open Net's campaigns consistently receive broad support. For instance, in 2014-15, over 11,000 people participated in a petition calling for a change to a law mandating the use of government backed certificates for most online payments. Privacy is among Open Net's main areas of concentration. Others include freedom of speech, intellectual property, net neutrality, internet governance, and technology regulation. Open Net has lobbied for laws and filed suits in an effort to improve

Korean law enforcement and surveillance practices so as to conform with international standards, including with respect to warrants, user notification, and data protection principles.

Panoptykon Foundation is a Polish civil society organization founded in 2009 to protect freedom and human rights in the context of electronic surveillance. The mission of Panoptykon Foundation is to keep surveillance under social control and within the framework of what is necessary and proportionate. In 2010 Panoptykon joined European Digital Rights as the first Polish civil society organization. Since then Panoptykon has developed a network of cooperating experts and supporters and a position as a "reference point" in the area of surveillance and human rights in Poland.

Red en Defensa de los Derechos Digitales ("R3D") is a Mexican non-profit, non-governmental organization dedicated to the defense of human rights in the digital environment, focusing in particular on the rights to privacy, freedom of expression and access to information. R3D uses various legal and communication tools to conduct policy research, strategic litigation, public advocacy, and campaigns with the objective of promoting digital rights in Mexico.

Renaissance Numérique is a non-profit and non-partisan French think tank dedicated to promoting an inclusive digital society. It brings together universities, large Internet companies, start-ups, and representatives of civil society to participate in defining a new economic, social and political model arising from the digital revolution. The think tank is committed to defending citizen rights on the Internet and democratic safeguards. Because this case

implicates the privacy and civil liberties of European citizens, Renaissance Numérique has an interest in informing this Court of the principles of the European rule of law, in particular concerning the protection of personal data and respect for the judicial framework.

Professor Simon Chesterman is Dean of the National University of Singapore Faculty of Law. For the past decade he has taught and researched on privacy, data protection, and the regulation and oversight of intelligence services. His books include *One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty* (Oxford: Oxford University Press, 2011) and *Data Protection Law in Singapore* (Singapore: Academy Publishing, 2014).

Vrijschrift is a grassroots volunteer-based organization based in the Netherlands that promotes the free flow of information, freedom of expression, free (as in libre) software, open content and data. Vrijschrift's interest in this case stems from its concern for the impact on free and open societies and the rule of law of competing law enforcement agency requests from different jurisdictions for private information held by third parties.