No. 17-2

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

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

BRIEF OF *AMICI CURIAE* DIGITAL RIGHTS IRELAND LIMITED AND THE OPEN RIGHTS GROUP IN SUPPORT OF RESPONDENT MICROSOFT CORPORATION

OWEN C. PELL
Counsel of Record
SUSAN L. GRACE
WHITE & CASE LLP
1221 Avenue of the Americas
New York, New York 10020
(212) 819-8200
opell@whitecase.com

Counsel for Amici Curiae Digital Rights Ireland Limited and the Open Rights Group

278154

COUNSEL PRESS

(800) 274-3321 • (800) 359-6859

QUESTION PRESENTED

Whether 18 U.S.C. § 2703 authorizes a U.S. court to issue a warrant that compels a U.S.-based provider of email services to disclose data stored outside of the United States, even when that data is subject to and would be available under EU and Irish MLATs which were expressly designated by the President and Congress as "self-executing."

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TREATIES AND STATUTES

Page

OTHER AUTHORITIES

Page

Page

Page

STATEMENT OF INTEREST OF THE *AMICI CURIAE*[1]

Digital Rights Ireland Limited ("DRI") is an Irish non-profit public interest organization committed to the protection of civil and political rights in the digital age. It has litigated before the European Court of Justice and elsewhere in a number of landmark cases on the status of digital rights. Specifically, DRI has been adverse to service providers like Microsoft with respect to data privacy issues, including in the seminal European Court of Justice case *Schrems* v. *Commissioner*.[2] But DRI also favors consistent and predictable practices relating to the release of data to law enforcement authorities and sees the U.S.-EU Mutual Legal Assistance Treaties as an important way of balancing fundamental privacy rights with the public interest relating to effective law enforcement.

DRI is concerned about the legal, moral, and technical implications of a regime which, without regard to Irish regulatory or judicial oversight, would deliver to a U.S. prosecutor personal data that is located in Ireland and subject to Irish and EU law. DRI believes that the position of the United States ignores valid Irish jurisdictional concerns, notwithstanding the terms of a binding and self-executing treaty between the United States and the

---

1. This brief is filed with the written consent of all parties. No counsel for a party authored this brief in whole or in part, nor did any person or entity, other than *Amici* or its counsel, make a monetary contribution to the preparation or submission of this brief.

2. Case C-362/14, *Schrems* v. *Comm'r*, ECLI:EU:C:2015:650.

European Union that provides for the balancing of the legitimate state interests of Ireland and the United States through mutual legal assistance applications.

The Open Rights Group ("ORG") is a non-profit company founded in 2005 by digital activists. ORG is one of the United Kingdom's most prominent voices defending freedom of expression, privacy, innovation, consumer rights, and creativity on the Internet. It is currently supported by around 3,000 active supporters and is advised by a council of leading experts drawn from academia, media, the technology and entertainment industries, and the legal profession.

ORG believes that people have the right to control their technology and data, and that strong data protection laws, including as established in the European Union, are an important part of preserving personal privacy rights. It believes that law enforcement agencies must be able to cooperate for the purpose of combatting crime, and that this cooperation is in practice efficiently accomplished by using local law and the processes provided by treaties such as the Mutual Legal Assistance Treaties at issue here. DRI and ORG have a substantial interest here because of the adverse precedent that could be set as to the protections provided for data located in Ireland and Europe under Irish and European law.

SUMMARY OF ARGUMENT

The United States seeks to enforce a warrant to compel Microsoft Corporation ("Microsoft") to produce in the United States email data stored in Ireland with a Microsoft subsidiary. The warrant was issued under the

Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 *et seq.*, enacted as Title II of the Electronic Communications Privacy Act ("ECPA").

But in seeking to enforce its warrant, the United States has wholly ignored—indeed, its brief never *once* cites—the U.S.-Ireland Mutual Legal Assistance Treaty that was ratified in connection with the U.S.-European Union Mutual Legal Assistance Treaty.[3] These treaties *expressly* provide for assistance in cases just like this one. These treaties also were *expressly* designated by the President and Congress as "self-executing" in response to the Court's decision in *Medellin* v. *Texas*, 552 U.S. 491 (2008). The United States has made no argument that the treaties do not apply. Rather, it simply ignores them. This Court should not allow this, especially when the MLATs would *both* allow the needs of U.S. law enforcement to be met, while protecting fundamental rights under European law *and* respecting Ireland's jurisdiction over the data in question—jurisdiction never challenged by the United States. As shown below, these treaties were designed to limit the enforcement jurisdiction of U.S. and EU

3. *See* Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters signed 18 January 2001, Ir.-U.S. Jul. 14, 2005, T.I.A.S. No. 10-0201.35 [hereinafter Irish MLAT]; Agreement on Mutual Legal Assistance, EU–U.S., Jun. 25, 2003, T.I.A.S. No. 10-201.1 [hereinafter, the EU MLAT and with the 27 EU Member State MLATs ratified simultaneously, the EU MLATs]. The EU and Irish MLATs are referred to collectively as "the MLATs."

authorities without hindering crime fighting or the war on terror, and the warrant should be quashed on that basis.

1. The United States does not dispute that data privacy is a fundamental right protected under Irish and EU law. Under Irish and EU law, a data subject does not lose their data privacy rights by entrusting their data to a service provider, including a non-EU service provider like Microsoft. It also is not challenged that data located in Ireland is subject to Irish jurisdiction and EU law and Irish law. Notwithstanding those principles, EU data privacy rights do not exist in a vacuum. EU data privacy laws were developed to recognize that individual privacy rights must be balanced with public needs that rely on the free flow of data, including society's right to protect itself against crime and terrorism. Thus, EU law is designed to balance individual rights and law enforcement needs, *including* through the processes implemented by the MLATs. Accordingly, the data content maintained by Microsoft-Ireland belongs to the author and owner of the account and Microsoft may not simply take that data and disclose it to U.S. law enforcement authorities. However, the criminal law exceptions in EU law *would* permit Irish authorities to obtain and provide that data *under the Irish MLAT*.

2. The MLAT procedures were negotiated to balance territorial interests relating to evidence gathering with data privacy interests. The EU MLATs were the culmination of over forty years of international discussions around how best to protect privacy and economic property interests inherent in personal data and its movement within and across national borders. The EU MLAT (and the 27 EU Member State MLATs ratified with it) was a milestone foreign policy event, and was hailed as an important development in the war against terror.

3. The MLATs recognize the territorial significance of where data is located, and also expressly create a framework for the United States to access the personal data at issue. In ratifying the MLATs, the President and Senate specifically recognized that the MLATs were designed to create access to evidence located beyond the territorial reach of U.S. courts. Thus, the U.S. Executive and Legislative Branches understood that EU nations have the right to regulate information located within their borders, *and* that the United States will respect that territorial prerogative by working *within* the MLATs to gain law enforcement access to data located in the EU.

4. Based on this Court's decision in *Medellin*, in presenting the EU MLATs for ratification, the President made clear—and the Senate made clear in its report favoring ratification—that the EU MLATs were *self-executing*. The MLATs also are the most recent statement of U.S. foreign policy regarding data stored in the EU, and postdate the SCA warrant provision at issue. In the EU MLATs the United States chose to limit its enforcement jurisdiction: Rather than rely on SCA warrants that would create conflicts with EU law, the U.S. agreed to establish specific procedures that allow U.S. law enforcement to gain access to data located within the territorial jurisdiction of EU Member States. It is undisputed that the SCA does not by its terms address the specific issue presented, while the MLATs specifically *do*. As such, there is a straightforward path to harmonizing the SCA with the EU MLATs.

5. The United States has offered no evidence that the EU MLATs are not working properly; indeed, recent statements by the Attorney General actually suggest the opposite, and a pending Congressional amendment of the

SCA endorses MLAT procedures. As such, contrary to the government's suggestion, there is no evidence that "[w]ithout the Section 2703 warrant process, [it] lacks an equally effective means of accessing electronic data critical to law enforcement and national security." Brief for Petitioner 44 (hereinafter "U.S. Brief"). Accepting the U.S. position here would mean that by entrusting their data to *any* internet service provider a data subject loses control over their data as to *any jurisdiction* in the world where that service provider is subject to government compulsion. That is not U.S. law, and runs counter to the MLATs.

6. The United States also may not use expedience to ignore treaties that the President and Congress designated as self-executing, which treaties by their terms direct EU and U.S. law enforcement authorities to use MLAT procedures as opposed to jurisdictional compulsion. By arguing that mutual assistance treaties "are not universal" (U.S. Brief 44), the government asks the Court (i) to ignore self-executing treaties that directly apply here and (ii) to render an advisory opinion just to simplify prosecutorial action in all cases. But this Court does not render advisory opinions. As important, this Court does not allow prosecutorial expediency to defeat recognized rights, such as the EU data privacy rights recognized by the United States in the EU and Irish MLATs.

The United States and Ireland are two friendly democracies with a long history of cooperation and mutual understanding on sovereign matters, dating from 1924 and the early Irish Free State. Cooperation in law enforcement is routine. *Amici* have no objection to the principle that a

U.S. Attorney can get access to the emails of a suspected criminal located outside the United States. But in doing so, the United States must respect EU and Irish law by using the MLAT procedures that were established to balance respective sovereign interests here.

ARGUMENT

I. DATA PRIVACY IS A FUNDAMENTAL HUMAN RIGHT PROTECTED IN IRELAND, BUT THOSE PROTECTIONS ARE DESIGNED NOT TO IMPEDE CRIMINAL INVESTIGATIONS.

Microsoft Ireland Operations Limited ("Microsoft-Ireland") is a wholly owned subsidiary of Microsoft and is a company registered in Ireland.[4] The datacenter hosting the email account at issue is operated by Microsoft-Ireland.[5] The email data is not stored in the United States, and nothing in the record suggests that the data subject who owns the data is a U.S. person or is not an EU person.[6] As important, there is nothing in the record showing that the data was placed in Ireland to avoid U.S. jurisdiction or to impede any actual or potential investigation.

Based on these undisputed facts, no matter how the SCA is understood, it cannot be doubted that Ireland has jurisdiction over the data located in its territory, has a right to regulate that data under Irish and EU law, and has a legitimate interest in how that data is handled.

---

4. *See* J.A. 30.

5. *See id.*, at 30, 34.

6. *See id.*, at 31, 34.

A. Data Privacy In Ireland Is A Fundamental Human Right.

Irish law on data privacy is guided by EU law. The basic principles for the protection of personal data and privacy are enshrined as fundamental human rights in the foundational documents of the European Union. The European Union Charter of Fundamental Rights (the "Charter") provides that "[e]veryone has the right to respect for his or her private and family life, home and communications,"[7] that "[e]veryone has the right to the protection of personal data concerning him or her" and that "[personal data] must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[8] The Treaty on the European Union provides that the Charter has a status in the EU legal order equivalent to the founding treaties themselves.[9] The Treaty on the Functioning of the European Union also declares that "[e]veryone has the right to the protection of personal data concerning them."[10] Ireland is a party to the Charter and thus is bound, with respect to Microsoft Ireland and the data it stores for its customers (i.e., including the data subject here).[11]

---

7. Charter on Fundamental Rights of the European Union art. 7, Oct. 6, 2012, 2012 O.J. (C 326) 2, 397.

8. *Id.,* at art. 8, 397.

9. Consolidated Version of the Treaty on European Union art. 6, Oct 26, 2012, 2012 O.J. (C 326) 1, 13, 19 [hearinafter TEU].

10. Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct 26, 2012, 2012 O.J. (C 326) 1, 47, 55 [hereinafter TFEU].

11. The significance of data privacy as a constitutional and fundamental human right under EU law has deep historical roots

The first EU directive on data protection[12] ("Data Protection Directive") was adopted in 1995 to reconcile and harmonize different approaches to data protection that had evolved among EU Member States. Its provisions were supplemented in 2002 by the ePrivacy Directive.[13] This framework was then updated in the General Data Protection Regulation ("GDPR"),[14] which entered into force in 2016, and will become applicable in May 2018. *See* Brief for the European Commission on Behalf of the European Union as *Amicus Curiae* 2 (hereinafter EC Amicus Brief); Brief for Jan Philipp Albrecht et. al, Members of the European Parliament as *Amici Curiae* 7-8 (hereinafter MEP Amicus Brief).

EU law is clear (and the United States does not dispute) that an EU data subject does *not* lose their data privacy rights by entrusting their data to a service provider, including a non-EU service provider like Microsoft. EU law also is clear that data located in Ireland is subject to EU law and Irish jurisdiction. For example, as explained by the European Commission, various provisions of the GDPR protect the rights of data subjects with respect to the processing (which would include movement) of data

---

in European history and culture. *See* Brief for Gesellschaft für Freiheitsrechte e.V. as *Amicus Curiae* 1-3, 6-10 [hereinafter GFF Amicus Brief].

12. Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter Data Protection Directive].

13. Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

14. Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

located in the EU by a third-party. *See* EC Amicus Brief 10. The European Court of Justice ("CJEU") also has confirmed that the transfer of personal data to a third party, such as a public authority, is an interference with a data subject's fundamental rights,[15] and the disclosure of the contents of electronic communications is a "*particularly serious*" interference.[16] Thus, it is a serious offence, with serious penalties, to transfer personal data to a country outside the EU absent assurance that standards for protecting personal data are in place.

B. EU Law Is Designed To Balance Individual Rights And Law Enforcement Needs, Including Through Use Of The MLATs.

EU data privacy rights do not exist in a vacuum. As set forth above, EU data privacy laws were developed to recognize that individual privacy rights must be balanced with public needs that rely on the free flow of data, including society's right to protect itself against crime and terrorism. Indeed, as shown by the MEP Amicus Brief, EU data privacy law has been shaped by parliamentarians who are deeply involved in the EU's fight against terrorism.[17]

---

15. Case C-1/15, Opinion Pursuant to Art. 218(11) TFEU, ¶ 124, ECLI:EU:C:2017:592.

16. Case C-293/12, *Digital Rights Ireland Ltd.* v. *Minister for Communications*, ¶ 39, ECLI:EU:C:2014:238 (emphasis added).

17. *See* MEP Amicus Brief 1, 3 (as to MEPs Jan Philipp Albrecht and Birgit Sippel).

The GDPR, for example, was developed and debated over four years. It reflects both the sensitivity of European citizens to the privacy of their personal data, as well as the need for personal data to be freely moved within the EU, including for reasons of public need. Hence, the GDPR contains exceptions to ensure that the rights of the individual do not unjustifiably obstruct the legitimate activities of Member States in the fields of security and law enforcement.[18]

An explicit protection under EU law is that personal data will not be transferred to a non-EU country unless the receiving state-party has in place safeguards to ensure that the data will receive equivalent protection to that afforded in the EU.[19] "Adequacy of protection" was at the heart of the CJEU decision in *Schrems*.[20] There, the CJEU annulled a European Commission decision[21] approving the EU "Safe Harbour Principles" for data protection[22] on the basis that the corresponding U.S. Department of Commerce's guidance for implementing those Principles did not meet the adequacy of protection standard.[23] In

18. As explained by the European Commission, EU Member States are parties to a group of treaties relating to using cooperation among states to prevent conflicts of laws from impeding criminal law enforcement, as well as cybercrime and terrorism. *See* EC Amicus Brief 3-4, 3 n.7.

19. Data Protection Directive, *supra* note 12, at 45.

20. *See* Case C-362/14, *Schrems* v. *Comm'r*, ECLI:EU:C:2015:650.

21. Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC).

22. *See id.* Annex I, at 10–12.

23. *See id.* Annex II, at 13–25.

the wake of this decision, the European Commission and United States negotiated the EU-U.S. Privacy Shield, which restores the legal basis for data transfers to U.S. organizations certified under the Privacy Shield Program. The Privacy Shield—which is based on the GPDR—does *not* permit Microsoft simply to take data stored in the EU and disclose it to U.S. law enforcement authorities. But, the criminal law exceptions in EU law *would* permit Irish authorities to obtain and provide that data *under the Irish MLAT*.[24] As such, the EU MLATs are an integral part of the EU legal structure for data privacy protection.

Thus, the GDPR, the Privacy Shield, *and* the EU and Irish MLATs are important here for two reasons. *First*, they show that as a matter of U.S. legal and foreign policy the U.S. government in its dealings with the EU has repeatedly recognized the territorial jurisdiction of EU Member States with respect to data stored within their borders. *Second*, far from viewing EU law as something that frustrates law enforcement, both the United States and EU have accepted EU law and established ways to handle data transfer matters *in order to avoid* the conflicts that both already know will otherwise occur if a private entity like Microsoft-Ireland is compelled to provide personal data stored in the EU to U.S. authorities. This is why the United States, the EU and 27 EU Member States negotiated the U.S.-EU MLAT and the corresponding 27 bilateral MLATs.[25] As stated by the European Commission, "[t]he GDPR thus makes [the MLATs] the preferred option for [data] transfers." EC Amicus Brief 14.

---

24. The same result would be available under German law. *See* GFF Amicus Brief 12, 14-17.

25. *See supra* note 3. The EU MLAT entered into force on February 1, 2010.

II. MLAT PROCEDURES WERE NEGOTIATED TO BALANCE TERRITORIAL INTERESTS RELATING TO EVIDENCE GATHERING WITH DATA PRIVACY INTERESTS.

Before 2003, the United States had entered into individual MLATs with twenty EU nations, including Ireland. But, the United States then proposed a comprehensive MLAT overhaul so as to allow for the simultaneous implementation of modified MLATs with all twenty-seven EU Member States.[26] This was a milestone foreign policy event, including because it encompassed issues beyond the MLATs themselves. The U.S.-EU MLAT marked the first law enforcement agreement between the United States and the EU, and also allowed the United States and the EU to complete a comprehensive extradition agreement.[27]

Remarkably, the United States does not even cite the EU MLAT, yet argues that "MLATs are often not an effective alternative to requiring disclosure of emails under the SCA." U.S. Brief 44. By contrast, in urging ratification of the EU MLAT, President Bush took a different tack,

---

26. The U.S. had pre-existing MLATs with 20 EU Member States which were updated by the EU MLAT (Austria, Belgium, Cyprus, Czech Republic, Estonia, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Poland, Romania, Spain, Sweden, the Netherlands, and the United Kingdom). The EU MLAT also established new treaty-based MLAT relationships with seven EU countries (Bulgaria, Denmark, Finland, Malta, Portugal, Slovakia, and Slovenia) with which the United States had no prior MLAT relationship. *See* S. Exec. Rep. No. 110-13, at 3-4 (2008).

27. *See* S. Treaty Doc. No. 109-13, at iii; v-vi (2006).

hailing the agreement as an important development in the war against terror.[28] Thus, contrary to the U.S. Government's assertion that mutual assistance somehow is "impractical" or "detrimental" to law enforcement (U.S. Brief 41, 44), the then Republican Administration asserted just the opposite to Congress. The Bush Administration said that one "innovation" of the EU MLAT was that it "establishes a comprehensive and uniform framework for limitations on the use of personal and other data."[29] By allowing "uniform improvements and expansions in coverage across much of Europe," the EU MLAT "will enable the strengthening of an emerging institutional relationship on law enforcement matters between the United States and the European Union, during a period when the EU is actively harmonizing national criminal law procedures and methods of international cooperation."[30] These statements by the Executive Branch in the exercise of its foreign affairs power highlight three important aspects of the EU MLATs that strongly favor quashing the warrant here.

A. The MLATs Are The Culmination Of Over Forty Years Of U.S. Policy As To Data Protection.

The balancing of rights and interests addressed by the MLATs has been the subject of U.S. and EU foreign policy discussions for over forty years. That an individual has rights in their data—and that this data has value—was recognized by President Nixon:

---

28. S. Treaty Doc. No. 109-13, at iii; v.

29. *Id.*

30. *Id.* at vi (Overview).

> Many of the good things in life that Americans take for granted would be impossible, or impossibly high-priced, without data retrieval systems and computer technology. But until the day comes when science finds a way of installing a conscience in every computer, we must develop human, personal safeguards that prevent computers from becoming huge, mechanical, impersonal robots that deprive us of our essential liberties.
>
> Here is the heart of the matter: What a person earns, what he owes, what he gives to his church or to his charity is his own personal business and should not be spread around without his consent. When personal information is given or obtained for one purpose, such as a loan or credit at a store, it should not be secretly used by anyone for any other purpose.
>
> To use James Madison's terms, in pursuing the overall public good, we must make sure that we also protect the individual's private rights.[31]

President Nixon was prescient in seeing that data not only related to privacy interests, but to significant economic interests as well. As the market has now strongly confirmed, personal data has undeniable economic substance like other forms of personal property. The market valuations of internet service providers, as well

---

31. President Richard Nixon, Radio Address About the American Right to Privacy (Feb. 23, 1974) (transcript available at http://www.presidency.ucsb.edu/ws/?pid=4364).

as the flow of money toward internet start-ups that are based on gaining access to different forms of personal data highlight that data is very much an asset that resembles a commodity. It can be bought and sold, it can be "mined," fees can be charged for access to it, and its value can be enhanced by the speed and volume with which it can be analyzed and moved. But complicating our understanding of how to manage the liberty interests represented by data is its protean nature—data can include information created and collected without a data subject's taking any action, and data routinely resides in a "cloud" or moves "in the ether" while undoubtedly being housed in physical space within hardware maintained in fixed locations. Thus, inherent in Nixon's observations about data were legal tensions that suffused how U.S. and EU executive and legislative bodies approached data privacy and the movement of personal data.

During the 1970s it became evident that the potential for varying national legislation on data privacy could hamper the free flow of data that was critical both to individual rights and economic interests. Recognizing the potential harm that would result from varying legal regimes, in 1980 the Organisation for Economic Co-Operation and Development ("OECD") issued a set of recommendations designed to harmonize national data privacy legislation in order to prevent interruptions in international data flow, while otherwise upholding human rights.[32] Consistent themes included the idea that data

32. *See* OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD C(80)58/Final (Sept. 23, 1980). As of 1980, the OECD was made up of United States and 24 other nations (17 from Europe) including Ireland. The OECD recommendations

belongs to the data subject, and that entrusting data to a service provider does not divest the data subject of their rights.[33] These recommendations were endorsed by all OECD members, including the United States, and have been instrumental in guiding EU and U.S. data privacy legislation – even if the precise machinery for achieving these common goals has varied.[34] It was against this backdrop that the United States (with the ECPA) and EU (with directives culminating in the GDPR) enacted laws *and* negotiated the MLATs.

B. The MLATs Recognize The Territorial Significance Of Where Data Is Located.

Contrary to the position now taken by the United States, in formulating and ratifying the MLATs the United States expressly recognized that its ability to obtain evidence located outside the United States is firmly rooted in the territorial location of data. The U.S. Senate

---

were based on the express premise that "transborder flows of personal data create new forms of relationships among countries that require the development of compatible rules and practices." *Id.*

33. *See id.* at ¶ 10 ("Use Limitation Principle") ("[p]ersonal data should not be disclosed, made available or otherwise used for purposes other than those [for which it was collected] except a) with the consent of the data subject; or b) by the authority of law").

34. *See* OECD, Thirty Years After The OECD Privacy Guidelines 8 (2011), http://www.oecd.org/sti/ieconomy/49710223.pdf. For example, while the EU has enacted overarching data privacy regulations for all industries and sectors, the United States has taken an *ad hoc* approach, enacting legislation addressing particular privacy protections as to particular industries (e.g., financial services, health care, and credit reporting).

specifically recognized that the EU MLATs were *designed* to create access to evidence located beyond the territorial reach of U.S. courts:

> In order for the United States to successfully prosecute criminal activity that is transnational in scope, it is often necessary to obtain evidence or testimony from a witness in another country. While U.S. federal courts may issue subpoenas to U.S. nationals overseas, they lack the authority to . . . subpoena evidence in a foreign country.[35]

Nowhere did the Senate observe that U.S. service providers offered an easy or assured path around territorial issues of data privacy. To the contrary, the Senate acknowledged that, without the MLATs, the U.S. government's ability to obtain evidence located in another country could also be limited by "domestic information-sharing laws [of the foreign state], such as bank and business secrecy laws[.]"[36] Thus, the U.S. Executive and Legislative Branches understood that EU nations have the right to regulate information located within their borders, and that the United States will respect that territorial prerogative by working *within* the MLATs to gain law enforcement access to data located in the EU.

35. S. Exec. Rep. No. 110-13, at 2.

36. *Id.*

C. The EU MLATs Expressly Create A Framework For The United States To Access The Personal Data At Issue.

Article 9 of the EU MLAT (which repealed Article 7 of the earlier Irish MLAT)[37] provides for limits on the use of personal data and replaced a use limitation used in prior MLATs.[38] Specifically, EU MLAT Article 9 was expressly designed to reconcile the very differences between US and EU law at issue here.[39] As explained by the President:

> Article 9(1) permits the requesting State to use evidence or information it has obtained from the requested State for its criminal investigations and proceedings [and] for preventing an immediate and serious threat to public security.[40]

Article 9(2)(a) then specifies that Article 9(1) does not preclude the requested State from imposing additional conditions, but Article 9(2)(b) makes clear that "generic restrictions with respect to the legal standard in the requesting State for processing personal data may *not* be imposed by the requested State as a condition under paragraph 2(a) to providing evidence or information."[41] This provision was so important that an Explanatory Note

37. *See* S. Treaty Doc. No. 109-13, at xxvii.

38. *See id.* at xiv.

39. *See id.* at xv.

40. *Id.* at xiv-xv.

41. *Id.* at xv (emphasis added).

was included as part of the EU MLAT to drive home the importance of the MLAT procedures.

The Explanatory Note clarifies Article 9 by stressing that (i) these MLAT procedures were specifically designed to allow for a balancing of the competing sovereign interests inherent in cases like this, and (ii) generally MLAT procedures tilt *in favor* of data being provided (i.e., in favor of law enforcement):

> Article 9(2)(b) is meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases. Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting State would raise difficulties so fundamental as to be considered by the requested State to fall within the essential interests grounds for refusal. *A broad, categorical, or systematic application of data protection principles by the requested State to refuse cooperation is therefore precluded. Thus, the fact the requesting and requested States have different systems of protecting the privacy of data* (such as that the requesting State does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting State uses means other than the process of deletion to protect the privacy or the accuracy of the personal

> data received by law enforcement authorities), *may as such not be imposed as additional conditions under Article 9(2a).*[42]

Thus, the United States made clear that the procedures in the EU MLAT not only were acceptable to it, but that these procedures created a bright-line rule as to how the United States and Europe would balance their respective sovereign interests in the handling of personal electronic data. Yet, it is precisely these procedures that the United States now seeks to flaunt.

III. THE SELF-EXECUTING MLAT TREATIES REPRESENT THE DECISION OF THE EXECUTIVE AND LEGISLATIVE BRANCHES TO LIMIT U.S. ENFORCEMENT JURISDICTION.

The EU MLATs are the most recent statement of U.S. law regarding the data privacy issues presented here. They recognize the territorial nature of data location *and* that EU law must be balanced against U.S. law enforcement needs (and vice versa), and provide a mechanism precisely designed to reconcile the competing legal interests in this specific case. Under these circumstances, allowing the U.S. government to ignore them so as to compel a service provider over whom it has jurisdiction to transfer data would set a dangerous precedent on many levels.

---

42. EU MLAT, *supra* note 3, at 27 (Explanatory Note) (emphasis added).

A. Data Stored Abroad But Entrusted To A Service Provider Does Not Belong To The Service Provider And Ease Of Access Cannot Change That.

The government argues that the SCA should be given extraterritorial effect because "[w]ithout the Section 2703 warrant process, [it] lacks an equally effective means of accessing electronic data critical to law enforcement and national security." U.S. Brief 44. This argument is directly contrary both to U.S. and EU law recognizing (i) that entrusting data to a service provider does not divest the data subject of his/her rights in the data; *and* (ii) that data located in an EU nation is subject to EU law. Indeed, accepting the government's position would mean that by entrusting their data to *any* internet service provider a data subject loses control over that data as to *any jurisdiction* in the world where that service provider is subject to government compulsion. That is not U.S. law, and runs counter to the MLATs and their recognition of how issues of concurrent jurisdiction should be addressed.

As troubling, the United States has made no record to support its assertion that MLAT procedures are so unworkable that only by compelling service providers can it protect U.S. interests. Indeed, the record is exactly the opposite—and shows that the Irish MLAT works. The former Attorney General of Ireland, Mr. Michael McDowell, was in office when the Irish and EU MLATs were negotiated, and testified below that these treaties were intended "to serve as the means for law enforcement authorities in the respective countries to obtain evidence located in the other treaty party." J.A. 48. McDowell also confirmed that "Ireland rarely refuses requests

for information made under the treaties" and that "the current MLAT procedures for fulfilling these requests are efficient and well-functioning." *Id.* at 49. There is no evidence to the contrary in the record.

McDowell's testimony is in line with a December 2017 speech by Attorney General Sessions extolling the MLATs and noting that the United States is working to make them even better. The Attorney General made clear that the MLATs were essential to U.S. law enforcement because of overlapping territorial jurisdiction: "We fully respect the importance of borders. Indeed, borders are an essential component of sovereignty, but if we work together—respectful of each other's rights—we can far more effectively stop transnational criminals."[43] Far from arguing that MLATs be circumvented via SCA warrants, the Attorney General instead declared: "Cooperation works—and at the Department of Justice, we know that firsthand."[44] Absent cooperation, "in many cases, justice cannot be done."[45] Addressing the issue of data stored abroad, the Attorney General said:

> The Department is also working towards the implementation of a framework with some of our closest allies that would supplement the MLAT process and reduce potential conflicts of law regarding the disclosure of electronic evidence.

43. Press Release, U.S. Dept. of Justice, Attorney General Sessions Remarks at the Global Forum on Asset Recovery Hosted by the United States and the United Kingdom (Dec. 4, 2017), https://www.justice.gov/opa/speech/attorney-general-sessions-delivers-remarks-global-forum-asset-recovery-hosted-united.

44. *Id.*

45. *Id.*

> That kind of framework would enhance public safety efforts in the U.S. and around the world.[46]

Having offered no principled objection to the EU MLATs, the government next argues that the problem is that mutual assistance treaties "are not universal." U.S. Brief 44. But that argument must fail on at least two grounds. *First*, it is not this case, and would turn this case into an advisory opinion on the SCA—something beyond this Court's constitutional competence.[47] *Second*, given that the EU and Irish MLATs by their terms *do* apply, the government is simply seeking to trump them on the grounds of expedience—since the United States lacks MLATs with all nations prosecutors should never have to use them even when we have MLATs in place. But this Court has rejected expedience as a way around recognized legal rights. *See Mincey* v. *Arizona*, 437 U.S. 385, 393 (1978) ("[T]he privacy of a person's home and property may not be totally sacrificed in the name of maximum simplicity in enforcement of the criminal law."). In the context of the warrant requirement, this Court has made clear that the rights at issue are not "an inconvenience to be somehow 'weighed' against the claims of police efficiency." *Coolidge* v. *New Hampshire*, 403 U.S. 443, 481 (1971) (citation omitted); *see also Mincey*, 437 U.S. at 393 ("The investigation of crime would always be simplified if warrants were unnecessary.").

---

46. *Id.*

47. *See, e.g., Alabama State Fed'n of Labor* v. *McAdory*, 325 U.S. 450, 461 (1945) ("This Court is without power to give advisory opinions. It has long been its considered practice not to decide abstract, hypothetical or contingent questions[.]" (internal citations omitted)).

If the government believes that we need more MLATs it can negotiate them, while also using the Irish MLAT already in place. If the government believes MLAT procedures could be more efficient, it can negotiate better procedures–as the Attorney General suggested may happen.[48] The government could also ask Congress to amend the SCA–and, indeed, identical bills to do so are currently pending in both houses of Congress.[49] But, those bills actually undercut the government's position because, rather than aligning the statute with the government's current interpretation, the bills set forth specific procedural safeguards to be followed *before* the government may demand that a service provider produce

48. MLAT reforms are underway; however, those efforts focus on deficiencies in *U.S.* processes for complying with MLAT requests from abroad. For example, in its FY 2015 Budget Summary, the Justice Department requested an additional $24 million to improve, and accelerate its handling of MLAT requests from abroad for evidence located in the United States. Thus, the government has stressed to Congress the need for the United States to hold up its end of the MLAT bargain. *See* U.S. Dep't of Justice, FY 2015 Budget and Performance Summary (2014), pt. 1, at 5 (2015 Budget Summary), https://www.justice.gov/sites/default/files/jmd/legacy/2013/11/21/fy15-bud-sum.pdf.

49. *See* International Communications Privacy Act, S. 1671, 115th Cong. (2017); H.R. 3718, 115th Cong. (2017). The Senate bill was introduced by Senators Hatch (R-Utah) and Coons (D-Del.). The House bill was introduced by Rep. Collins (R-Ga.) and is co-sponsored by Reps. Jeffries (D-N.Y.), DelBene (D-Wash.) and Issa (R-Calif.). Stressing the need to balance individual rights with state interest, Senators Hatch and Coons noted that federal courts "who have examined these issues continue to encourage Congress to fix this problem, and our legislation does just that." Press Release, Hatch, Coons Introduce International Communications Privacy Act (ICPA) (Aug. 1, 2017), https://www.hatch.senate.gov/public/index.cfm/2017/8/hatch-coons-introduce-international-communications-privacy-act-icpa.

foreign-stored data, and would create U.S. procedures for making MLAT requests move faster.[50]

By asking this Court to ignore EU and Irish MLATs that would resolve this case, and instead decide a case not before the Court—i.e., a case where no MLAT is available—the government is asking the Court to legislate, something this Court should not do. *See Herb's Welding* v. *Gray*, 470 U.S. 414, 427 (1985) ("[I]f Congress' coverage decisions are mistaken as a matter of policy, it is for Congress to change them. We should not legislate for them.").[51]

---

50. *See* S. 1671, Sec. 4; H.R. 3718, Sec. 4.

51. Indeed, in testifying on the pending bills—testimony cited to the Court (U.S. Brief 44-45), the government actually advocated strenuously for a *legislative* solution:

> Congress should consider targeted amendments to the SCA that will provide for the legitimate needs of law enforcement agencies in the United States to obtain, through lawful process, electronic communications stored abroad that are relevant to U.S. criminal investigations, as well as address foreign countries' legitimate public safety needs. At the same time, it should reduce the chance that providers will be caught in conflicting obligations between U.S. and foreign laws.
>
> . . .
>
> As the Microsoft decision fundamentally rests on statutory interpretation, Congress can correct it through a clarifying amendment to the statute.

Law Enforcement Access to Data Stored Across Borders: Facilitating Co-operation and Protecting Rights: Hearing Before the Subcomm. on Crime & Terrorism, S. Comm. on the Judiciary, 115th Cong. 6, 9 (May 24, 2017) (statement of Brad Wiegmann, Deputy Assistant Att'y Gen., DOJ).

B. The MLATs Are The Most Recent Applicable Statement Of U.S. Law And Policy By The Executive And Legislative Branches.

Although ignored in the U.S. Brief, the EU MLATs are entitled to great weight. They represent a strong and consistent statement of U.S. foreign policy as to principles of data privacy (including with regard to service providers), data location, and how issues of concurrent jurisdiction should be resolved. The EU MLATs were submitted to the Senate and ratified, and, as such, represent the U.S. government acting at its constitutional maximum. *See Youngstown Sheet & Tube Co.* v. *Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring).[52] The President and Congress also took the extra step of expressly stipulating the EU MLATs as "self-executing."[53] That is, the political branches that negotiated and approved the EU MLATs determined that they should "automatically have effect as domestic law" because the EU MLATs themselves "convey[] an intention that [they] be 'self-executing' and

52. Indeed, the Justice Department stressed to Congress that "the decision to proceed with the negotiation of law enforcement treaties such as these [was] made jointly by the Departments of State and Justice, after careful consideration of [their] international law enforcement priorities." *Treaties: Hearing Before the S. Comm. on Foreign Relations*, 110th Cong. 1 (May 20, 2008) (statement of Bruce C. Swartz, Deputy Ass't Attorney General, Criminal Division, DOJ). Mr. Swartz also stated that the State and Justice Departments "worked closely with the Department of Treasury, the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC) in negotiating the articles of the U.S.-EU [MLAT] that relate to their respective functions." *Id.*

53. *See* S. Exec. Rep. No. 110-13, at 11.

[were] ratified on these terms." *Medellin* v. *Texas*, 552 U.S. 491, 504-505 (Roberts, C.J.) (internal citation and quotation marks omitted). Thus, with regard to U.S. enforcement procedures, the EU MLATs "have the force and effect of a legislative enactment." *Id.* at 505-06 (quoting *Whitney* v. *Robertson*, 124 U.S. 190, 194 (1888)).

C. The Self-Executing MLATs Expressly Limit The Enforcement Jurisdiction Of The SCA Warrant At Issue.

As noted above, the MLATs are self-executing. The Senate stated that the EU MLATs were "generally designed to overcome" the problems posed by "the scope of foreign judicial assistance [being] limited by domestic information-sharing laws, such as bank and business secrecy laws."[54] Thus, the tension potentially created with EU data privacy laws when U.S. service providers stored data abroad as to non-U.S. data subjects would be the type of "problem" that now was "overcome" by the MLAT procedures without any further act of Congress.

As self-executing treaties, the EU and Irish MLATs have the force of binding federal law—even if the government would rather they did not exist in this case. In *Medellin*, this Court cited to *Whitney*, 124 U.S. at 194, to explain that a self-executing treaty

> is placed [by the Constitution] on the same footing, and made of like obligation, with an act of legislation. Both are declared by that instrument to be the supreme law of the land,

54. S. Exec. Rep. No. 110-13, at 2-3.

> and no superior efficacy is given to either over the other. When the two relate to the same subject, the courts will always endeavor to construe them so as to give effect to both . . . .

Here, the MLATs apply to this case because they are directed at the exercise of U.S. enforcement jurisdiction as to evidence located in Ireland and subject to Irish and EU law—which laws govern under the MLATs.[55] In the EU MLATs the United States chose to limit its enforcement jurisdiction: Rather than rely on SCA warrants that would create conflicts with EU law, the U.S. agreed to establish specific procedures to allow U.S. law enforcement to gain access to data located within the territorial jurisdiction of EU Member States. It is undisputed that the SCA does not by its terms address the specific issue presented, while the MLATs specifically *do*.[56] As such, there is a

---

55. For reasons that are unclear, the Irish Republic included in its *amicus* submission reference to how banking data is treated under Irish law. *See* Brief for Ireland as *Amicus Curiae* 5-7 [hereinafter Ireland *Amicus* Brief]. As the Second Circuit recognized, banking data is distinct from personal data such that precedents regarding subpoenas served on banks are not apposite here. *See* Pet. Cert., App. A 35a ("the Supreme Court has held that bank depositors have no protectable privacy interests in a bank's records regarding their accounts") (citation omitted). More importantly, the Ireland *Amicus* Brief ignores the fact that the EU and Irish MLATs specifically distinguish between banking data, as to which there is one protocol, and personal data for which there is Article 9, a different protocol. *See* EU MLAT, art. 4; Irish MLAT, art. 16 *bis.* Thus, Irish law on banking data does not inform the MLAT analysis here.

56. Thus, by harmonizing the EU MLATs with the SCA, this Court need not reach the issue of the extraterritorial reach of the

straightforward path to harmonizing the SCA with the EU MLATs.[57]

Having ignored the EU MLATs, the United States instead invokes the Council of Europe Convention on Cybercrime, as a treaty that it cares about and that somehow could be imperiled by the SCA warrant in this case not being enforced. U.S. Brief 47-49.[58] But, not only does the government cite the wrong provision of the Convention that applies here, it ignores the fact that the Convention on Cybercrime *both* directed the creation of precisely the types of procedures that were then created by the EU MLATs *and* gave primacy to the state where stored information is located—i.e., exactly what the EU MLATs do here.

SCA in this case. *Cf. Societe Nationale Industrielle Aerospatiale* v. *United States Dist. Court for S. Dist.*, 482 U.S. 522, 555 (1987) ("[T]he threshold question in a comity analysis is whether there is in fact a true conflict between domestic and foreign law. When there is a conflict, a court should seek a reasonable accommodation that reconciles the central concerns of both sets of laws.").

57. Moreover, to the extent they are deemed in conflict, the EU MLATs would take precedence, having been ratified in 2008, versus the SCA, passed as part of ECPA in 1986. In any event, unlike *Medellin*, this case does *not* involve an attempt to derive private rights or private causes of action from a treaty. Rather, the EU MLATs are being applied directly to their purpose, which is to limit U.S. enforcement jurisdiction with respect to data located within the territorial jurisdiction of an EU MLAT nation, Ireland. *See* EU MLAT Art. 2(5) *and* Irish MLAT Art. 1(4) (the treaties create no private rights of action).

58. Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13174, 2296 U.N.T.S. 167 [hereinafter Convention].

First, the United States relies on Article 18 of the Convention on Cybercrime (U.S. Brief 48).[59] But that article only directs states to adopt "legislative measures" which will allow persons subject to state jurisdiction, including service providers, to provide requested information.[60] Nowhere does the Convention resolve the EU-U.S. law issues later resolved by the EU MLATs. The Convention *does* specify that state parties "shall insure" that any procedures implemented will respect EU law as to data privacy rights—and cites the Charter.[61] The self-executing EU MLATs, ratified in 2008, then became the legislative measures contemplated by the Convention—and indeed, the Justice Department told Congress that "[w]here we have such treaties, we will proceed under

---

59. Article 18.1 of the Convention provides:

> Each Party shall 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.

60. In citing Article 18.1(a) (U.S. Br. 48), the government also ignores that Article 18.1(*b*) specifically refers to service providers—like Microsoft. This is significant because Article 18.1(b)—just like the EU MLATs—focuses on where data may be stored, not just where the service provider itself may be located.

61. *See* Convention, Art. 15.

those treaties."[62] Thus, the U.S. position here is directly contrary to what the Executive Branch told Congress.

Second, the United States ignores Article 32 of the Convention on Cybercrime, which specifically applies to "[t]rans-border access to stored computer data."[63] With respect to non-public data—like the data here—the Convention gives primary jurisdiction to the state where the data is stored. Thus, again, the EU MLATs became the legislative acts by which the United States and EU carried out the terms of the Convention as to trans-border access to stored data—including by giving primacy to the law of the state where data is stored. Here, that is Irish and EU law as applied through the Irish MLAT to data

---

62. *See Hearing on Law Enforcement Treaties:[inter alia,] Treaty Doc. 108-11, Council of Europe Convention on Cybercrime Before the S. Comm. on Foreign Relations*, S. Hrg. 108-721, 108th Cong. 32 (Jun. 17, 2004) (statement of Bruce C. Swartz, Deputy Ass't Attorney General, Criminal Division, DOJ) ("The provision of [Article 18] will not affect our bilateral mutual legal assistance agreements. Where we have such treaties, we will proceed under those treaties.").

63. Convention Article 32 provides:

> A Party may, without the authorisation of another Party:
>
> (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
>
> (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

stored in Ireland. Accordingly, it is only by giving effect to the EU MLATs that the United States actually would be complying with its treaty obligations.

In choosing to ignore the EU MLATs, either because the United States now wishes it had more of them or because some MLAT processes allegedly "can be slow and uncertain" (U.S. Brief 44), the United States would have this Court ignore two settled rules of treaty application. *First*, the United States has chosen to ignore the EU MLATs rather than apply them in a manner consistent with other federal laws. The EU MLAT Senate Report stated that the MLATs would "be implemented by the United States in conjunction with applicable federal statutes."[64] Nothing about the U.S. position is "*in conjunction with*" existing law. The United States has simply ignored the EU MLATs even though there is no dispute that the warrant at issue invades the province of Irish law and territorial jurisdiction.

Second, the U.S. position renders the MLATs either superfluous or a nullity. Rather, than striving to read the EU MLATs in conjunction with the SCA—as the Senate said would be done—the United States reads the MLATs as having no impact at all. But this effectively reads the MLATs out of existence, something that is contrary to *Medellin* and other cases. *See, e.g., Medellin*, 552 U.S. at 506 (self-executing treaties "have the force and effect of a legislative enactment"); *Factor* v. *Laubenheimer*, 290 U.S. 276, 303-304 (1933) (words of a treaty should be liberally construed so as to not render any terms meaningless or inoperative).

64. S. Exec. Rep. No. 110-13, at 10.

By using an SCA warrant to compel Microsoft to produce data protected under Irish and EU law only because that data was entrusted to Microsoft would be to ignore fundamental rights under Irish and EU law which the United States expressly agreed to respect under the EU and Irish MLATs. The U.S. position that the MLATs can be ignored is contrary to any concept of the MLATs having the force of federal law, and effectively renders the EU and Irish MLATs a nullity. Adopting the U.S. position would allow the government to substitute U.S. court compulsion for the process mandated by the MLAT procedures—and would destroy any incentive for any prosecutor ever to use the MLATs. Again, this would destroy the self-executing nature of the MLATs, and be contrary to their terms.

CONCLUSION

For the foregoing reasons, *Amici Curiae* urge the Court to affirm the decision of the Second Circuit or otherwise quash the warrant sought in this case.

Dated: January 18, 2018

Respectfully submitted,

Owen C. Pell
Counsel of Record
Susan L. Grace
White & Case LLP
1221 Avenue of the Americas
New York, New York 10020
(212) 819-8200
opell@whitecase.com

Counsel for Amici Curiae
Digital Rights Ireland Limited
and the Open Rights Group