# Brief of EU Data Protection and Privacy Scholars as Amici Curiae in Support of Respondent

*April 17, 2018. Case No. 17-2. United States of America v. Microsoft Corporation*

Amici Curiae; Brkan, M.; Castets-Renard, C.; Cole, M.D.; Dommering, E.; Forgó, N.; Korff, D.; Kosta, E.; Ligeti, K.; Mariottini, C.M.; Métille, S.; Mitrou, L.; Pollicino, O.; Pretschner, A.; Robinson, G.; Ryngaert, C.; Spindler, G.; Valcke, P.; Van Calster, G.; van Eijk, N.; Weber, R.H.; Zuiderveen Borgesius, F.

**Publication date**
2018

**Document Version**
Final published version

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 EU DATA PROTECTION AND PRIVACY SCHOLARS AS *AMICI CURIAE* IN SUPPORT OF RESPONDENT

VINCENT LEVY
DANIEL M. SULLIVAN*
**Counsel of Record*
MATTHEW V.H. NOLLER
KEVIN D. BENISH
HOLWELL SHUSTER & GOLDBERG LLP
750 Seventh Avenue
New York, NY 10019
(646) 837-5151
dsullivan@hsgllp.com

*Counsel for Amici Curiae*

January 18, 2018

## TABLE OF CONTENTS


INTEREST OF *AMICI CURIAE* ..... 1

SUMMARY OF THE ARGUMENT ..... 1

ARGUMENT ..... 3

I. The Presumption Against Extraterritoriality Is At Its Apex When There Is An Evident Risk Of Conflict Between U.S. And Foreign Law .... 3

II. Enforcing The SCA Warrant Against Microsoft Creates An Evident Risk Of Conflict With EU Law ..... 6

A. Complying With The SCA Warrant Would Likely Violate The GDPR ..... 7

B. The Budapest Convention Does Not Authorize The SCA Warrant ..... 13

III. To Avoid Conflicts Between U.S. And Foreign Law, The Court Should Limit The SCA To Data Stored In The United States ..... 15

CONCLUSION ..... 17

APPENDIX ..... 18

## TABLE OF AUTHORITIES

**Cases**

Barcelona Traction, Light & Power Co. Ltd. (Belg. v. Spain), 1970 ICJ 3 (Feb. 5) ..... 5

*Benz* v. *Compania Naviera Hidalgo, S.A.*, 353 U.S. 138 (1957) ..... 4

*EEOC* v. *Arabian Am. Oil Co.*, 499 U.S. 244 (1991) ..... 4

*Hartford Fire Ins. Co.* v. *California*, 509 U.S. 764 (1998) ..... 4, 5, 15

Island of Palmas Case (U.S. v. Neth.), (1928) II RIAA 829 ..... 5

*Kiobel* v. *Royal Dutch Petroleum Co.*, 569 U.S. 108 (2013) ..... 4, 15, 16

*Murray* v. *Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64 (1804) ..... 5

*RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 209 (2016) ..... 1, 3, 4, 15

*Walsh* v. *National Irish Bank*, [2013] 1 ESC 2 ..... 5, 6

**Treaties and Agreements**

Agreement on Mutual Assistance, U.S.-European Union, June 25, 2003, T.I.A.S. No. 10-201.1 ..... 9, 12

Council of Europe Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167, E.T.S. 185 ..... 2, 13, 14
preamble ..... 13
art. 18 ..... 13, 14
art. 19 ..... 13
art. 32 ..... 14

EU Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 02:
art. 8 ..... 7

European Convention on Human Rights, June 1, 2010, C.E.T.S. No. 005:
art. 8 ..... 7

Treaty Between the United States of America and the Federal Republic of Germany on Mutual Legal Assistance in Criminal Matters, Oct. 14, 2003, T.I.A.S. No. 09-1018:
art. 1 ..... 14

Treaty on Mutual Legal Assistance, U.S.-Ir., Jan. 18, 2001, T.I.A.S. No. 13,137 ..... 9, 12

**Statutes and Regulations**

EU Directive 95/46, 1995 O.J. (L281) 31 ..... 6
art. 29 ..... 8

Regulation (EU) 2016/679, Apr. 27, 2016, 2016 O.J. (L119) 1 ..... *passim*
recital 115 ..... 8
art. 1 ..... 7
art. 3 ..... 3, 7
art. 4 ..... 3, 7
art. 5 ..... 7

art. 6 ..... 7, 11
art. 44 ..... 10
art. 45 ..... 9, 11
art. 46 ..... 9, 11
art. 47 ..... 9, 11
art. 48 ..... *passim*
art. 49 ..... 9, 10, 11, 12

**Other Authorities**

Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677 (2015) ..... 15

Article 29 Working Party, Statement on Data Protection and Privacy Aspects of Cross-Border Access to Electronic Evidence (Nov. 29, 2017) ..... 8, 10

Article 29 Working Party, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (Nov. 25, 2005) ..... 11

Cybercrime Convention Comm., Council of Europe, *T-CY Guidance Note #3: Transborder Access to Data (Article 32*) (Nov. 5, 2013) ..... 14

Cybercrime Convention Comm., Council of Europe, *T-CY Guidance Note #10: Production Orders for Subscriber Information (Article 18 Budapest Convention)* (Mar. 1, 2017) ..... 14

Electronic Privacy Information Center, *Article 29 Working Party*, https://goo.gl/Xkg7PZ ..... 8

Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & Contemp. Probs. 231. (2015) .....8

Letter from Peter J. Kadzik, Assistant Attorney Gen., to Joseph R. Biden (July 15, 2016) .....16

Restatement (Fourth) of Foreign Relations Law: Jurisdiction (Am. Law Inst., Tentative Draft No. 2 2016) .....5

*Transfers Abroad*, Office of the Data Protection Commissioner (Ir.), https://goo.gl/ezLigF.....11

Yevgeniy Sverdlik, *Research: There are Now Close to 400 Hyper-Scale Data Centers in the World*, Data Cntr. Knowledge (Dec. 21, 2017), https://goo.gl/Vxg2sa .....15

## INTEREST OF *AMICI CURIAE*

*Amici* are European experts in data protection, privacy law, and related issues. Because of their extensive expertise in these areas, *Amici* are in a unique position to highlight conflicts between U.S. and foreign law that are almost certain to arise if the Government is permitted to obtain data stored in Ireland under the Stored Communications Act (SCA).

A full list of *Amici* and their respective academic positions is set forth in the Appendix.[1]

## SUMMARY OF THE ARGUMENT

The presumption against extraterritoriality reduces the risk of conflicts between U.S. and foreign law by requiring that Congress, rather than the courts, decide whether and to what extent U.S. statutes apply abroad. Although the presumption applies even when an extraterritorial application of U.S. law would not conflict with the laws of another country, the presumption is "at its apex" when there is an evident risk of conflict. *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2107 (2016).

This case presents just such a situation. Enforcing the SCA warrant in this case would require Microsoft to transfer its customer's data from Ireland to the United States. Regulation (EU) 2016/679, Apr. 27, 2016, 2016 O.J. (L119) 1, the European Union's General Data Protection Regulation (GDPR), regulates this transfer, imposing detailed requirements that Microsoft must follow, and that the SCA warrant does not satisfy. In particular, the GDPR prohibits

---

[1] All parties have filed blanket consents to the filing of *amicus* briefs. No counsel for a party authored this brief in whole or in part, and no person other than *Amici*'s counsel made a monetary contribution to fund the preparation or submission of this brief.

data transfers that are based solely on a foreign government's unilateral demand. Instead, the GDPR requires the use of the Mutual Legal Assistance Treaty (MLAT) between the United States and Ireland, one of a system of bilateral treaties designed to aid law enforcement in exactly the circumstances present here. But the Government has chosen not to proceed through the MLAT. Microsoft, therefore, cannot produce the data the Government seeks without violating the GDPR.

The Government has not addressed the GDPR's relevance to this case. It does argue, however, that the Council of Europe Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167, E.T.S. 185 [hereinafter Budapest Convention], requires the United States to apply the SCA abroad. That argument is incorrect. In fact, consistent with EU data protection law, the Budapest Convention does not authorize countries to unilaterally collect data stored in other countries.

The judiciary, this Court has cautioned in similar circumstances, is not well-situated to anticipate and address the international discord that could result from a conflict between the SCA and the GDPR. It is rather the political branches that have the expertise in foreign relations necessary to weigh the competing considerations involved. The Court should therefore interpret the SCA to apply only to data stored within the United States, leaving to Congress the decision whether and under what circumstances to authorize the collection of data stored in other countries.

## ARGUMENT

As this case comes to the Court, all parties agree the SCA does not apply extraterritorially. U.S. Br. 17. The only question is whether enforcing a warrant that requires Microsoft to gather and produce data it stores in Ireland is an extraterritorial application of the SCA.

*Amici* believe the answer to that question is yes. Complying with the SCA warrant here would trigger—and likely violate—European data-privacy laws, thus confirming its extraterritoriality. Despite the Government's assertions, the acts of accessing, copying, and transferring personal data stored in Ireland will take place within the European Union and trigger EU law. *See* GDPR art. 3 (defining GDPR's territorial scope); *id.* art 4(2) (defining "processing" sufficient to trigger GDPR's application). The Court should not assume that Congress intended the SCA to create such a conflict with foreign law. Instead, the Court should adopt a clear rule against applying the SCA to data stored abroad.

### I. The Presumption Against Extraterritoriality Is At Its Apex When There Is An Evident Risk Of Conflict Between U.S. And Foreign Law.

This Court has long recognized "that, in general, United States law governs domestically but does not rule the world." *RJR Nabisco*, 136 S. Ct. at 2100 (internal quotation marks omitted). In recognition of this "basic premise," the Court has recognized a presumption against extraterritoriality, under which a statute does not apply extraterritorially unless it "affirmatively and unmistakably" provides otherwise. *Id.*

The presumption's primary rationale is to avoid "unintended clashes between [the United States'] laws and those of other nations which could result in international discord." *Kiobel* v. *Royal Dutch Petroleum Co.*, 569 U.S. 108, 115 (2013) (internal quotation marks omitted). For that reason, the Court has held that "the need to enforce the presumption is at its apex" when there is an evident risk of conflict between U.S. and foreign law. *RJR Nabisco*, 136 S. Ct. at 2107. The Court lacks the necessary expertise in the "delicate field of international relations" to decide whether such a conflict will create international discord or, if so, whether that discord is justified by other interests. *Kiobel*, 569 U.S. at 115–16 (quoting *Benz* v. *Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957)). The presumption against extraterritoriality leaves those questions to Congress, which "alone has the facilities necessary to make fairly such an important policy decision." *Id.* (quoting *Benz*, 353 U.S. at 147).

A risk of conflict between a U.S. statute and foreign law also indicates that the application of the statute is impermissibly extraterritorial. Domestic applications of a statute are unlikely to trigger foreign law, which typically does not govern conduct within the United States. *Cf. Hartford Fire Ins. Co.* v. *California*, 509 U.S. 764, 798–99 (1998) (finding no conflict between U.S. and British law where British law did not prohibit conduct required by U.S. law). Conflicts arise when applying U.S. law would regulate conduct that foreign law also regulates, which will tend to be conduct taking place in another country.

The desire to avoid conflicts with foreign law puts the United States in good international company. Like the United States, other countries generally can enact extraterritorial laws. *Compare EEOC* v. *Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991) ("Congress has the

authority to enforce its laws beyond the territorial boundaries of the United States.") *with* Restatement (Fourth) of Foreign Relations Law: Jurisdiction § 201 (Am. Law Inst., Tentative Draft No. 2, 2016) (noting that "customary international law permits states to exercise non-territorial jurisdiction" under some circumstances). But international law encourages countries to "respect . . . each other by limiting the reach of their laws." *Hartford Fire Ins.*, 509 U.S. at 817 (Scalia, J., dissenting). International law limits "a nation's exercise of its jurisdiction to prescribe," *id.* at 815, and requires "every State . . . to exercise moderation and restraint as to the extent of the jurisdiction assumed by its courts in cases having a foreign element, and to avoid undue encroachment on a jurisdiction more properly appertaining to, or more appropriately exercisable by, another State," Barcelona Traction, Light & Power Co. Ltd. (Belg. v. Spain), 1970 ICJ 3, 64, ¶ 70 (Feb. 5) (separate opinion by Fitzmaurice, J.); *see also* Island of Palmas Case (U.S. v. Neth.), (1928) II RIAA 829, 838 (establishing that international law protects countries' "exclusive competence . . . in regard to [their] own territory"). This Court presumes that Congress follows these requirements. *See Murray* v. *Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804) (Marshall, C.J.).

With respect to cross-border discovery, Ireland in particular has adopted rules designed to avoid conflicts with foreign law. In *Walsh* v. *National Irish Bank*, [2013] 1 ESC 2 (Ir.), a decision Ireland highlights in its *amicus* brief, Ireland Br. at 5–7, the Supreme Court of Ireland considered whether it could order a bank to disclose information stored in a foreign country, when foreign law might prohibit such disclosure. *Id.* ¶¶ 1.1, 3.3. Even though in that case the

bank's own records (as opposed to the private correspondence of others) were at issue, the court held that, before requiring disclosure of foreign-stored information, Irish courts must determine (1) whether there is an alternative way to get the information, and (2) whether disclosure would violate foreign law. *Id.* ¶¶ 7.6–9.6. "Irish courts should not, without sufficient clarity as to the consequences of the proposed measure, make an order which might place a party in a position of having to find itself in breach of the laws of another country." *Id.* ¶ 9.4.

These authorities bolster this Court's commitment to avoid conflicts between domestic and foreign law through the presumption against extraterritoriality. In this case, the Court should not enforce the SCA warrant against Microsoft without first asking whether doing so could require Microsoft to violate foreign law. *Amici* are well-situated to answer that question.

## II. Enforcing The SCA Warrant Against Microsoft Creates An Evident Risk Of Conflict With EU Law.

As other *amici* explain, and as the Government does not dispute, enforcing the SCA warrant in this case would implicate foreign data-privacy laws. *E.g.*, European Comm'n Br. 8–16; Law Enforcement Officials Br. 4–8; New Zealand Privacy Comm'r Br. 12–14. The foreign law most relevant here is the GDPR, which takes effect on May 25, 2018, and will regulate the transfer of personal data stored within the European Union.[2] As relevant here, it applies to all compa-

[2] The GDPR replaces the European Union's 1995 Data Protection Directive (1995 Directive), 1995 O.J. (L281) 31, which has provisions similar to those in the GDPR. European Comm'n Br. 2 n.5.

nies that process personal data in the European Union. GDPR art. 3; *see also id.* art. 4(2) (defining "processing" to include "storage" of personal data). And while it was not in effect when the Government issued its warrant to Microsoft, it will be in effect by the time the Court issues its decision in this case, so it will govern any transfer of data from Microsoft's Irish servers to the United States. European Comm'n Br. 3.

The SCA warrant in this case likely does not comply with the GDPR's requirements. Enforcing the warrant would, therefore, create an evident risk of conflict by requiring Microsoft to violate EU law, thus illustrating the SCA's extraterritorial reach in this case.

### A. Complying With The SCA Warrant Would Likely Violate The GDPR.

1. As the GDPR recognizes, under EU law all "natural persons" have a "fundamental right[]" to "the protection of personal data." GDPR art. 1(2). This right originates in Article 8 of the Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 02, as well as Article 8 of the European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms), June 1, 2010, C.E.T.S. No. 005. *See also* European Comm'n Br. 1–2 (identifying other international agreements protecting this right); Cannataci Br. 9–12 (same). The GDPR enforces this fundamental right by imposing comprehensive requirements on the processing of personal data located in the European Union. *See* GDPR arts. 5–6; European Comm'n Br. 8–12.

The European Union's commitment to personal data protection is not shared by all non-EU nations. The United States, for example, provides "more limited safeguards for privacy" than the European Union and imposes "fewer restrictions on how much personal

data may be collected, how such data may be used, and how long that data may be kept." Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & Contemp. Probs. 231, 236–38 (2015). To ensure that the GDPR's provisions cannot be avoided simply by transferring personal data to a country with less protective laws, the GDPR sets forth specific rules for the transfer of personal data from the European Union to a non-EU nation. GDPR, Recital 115.

2. Article 48 of the GDPR provides that, unless otherwise authorized by EU law, a court order requiring the transfer of personal data to a location outside the European Union must be "based on an international agreement, such as a mutual legal assistance treaty." Such MLATs are thus "the preferred option for transfers." European Comm'n Br. 14. Indeed, the influential Article 29 Working Party recently issued a statement asserting that MLATs "must—as a general rule—be obeyed" because "[t]he circumvention of existing MLATs . . . by a third country's law enforcement authority" is "an interference with the territorial sovereignty of an EU member state." Statement of the Article 29 Working Party on Data Protection and Privacy Aspects of Cross-Border Access to Electronic Evidence at 9 (Nov. 29, 2017) [hereinafter WP29 Statement on Data Protection].[3] This statement from the principal advisory body on EU data-protection law confirms

[3] The Article 29 Working Party is the advisory body tasked with advising the European Commission with respect to data privacy. 1995 Directive art. 29. It is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor, and a representative of the European Commission. Electronic Privacy Information Center, *Article 29 Working Party*, https://goo.gl/Xkg7PZ (last visited Jan. 17, 2018).

that the GDPR prohibits Microsoft from transferring the data in this case unless it does so pursuant to an MLAT.

The United States has entered into MLATs with the European Union and Ireland that would authorize Irish authorities to transfer personal data from Microsoft's servers in Ireland to the United States. Agreement on Mutual Assistance, U.S.-European Union, June 25, 2003, T.I.A.S. No. 10-201.1 [hereinafter EU MLAT]; Treaty on Mutual Legal Assistance, U.S.-Ir., art. 1.1, Jan. 18, 2001, T.I.A.S. No. 13,137 [hereinafter Ireland MLAT]. Ireland represents to this Court that it is ready and willing to comply with its MLAT obligations "as expeditiously as possible." Ireland Br. 8. The Government, however, has chosen not to employ the MLAT procedure. *See* U.S. Br. 44–45. Nor does the Government argue that the transfer required by the warrant is authorized by any other EU or Irish law.

3. The GDPR provides no other basis for Microsoft to comply with the SCA warrant. Although Article 48 applies "without prejudice to other grounds for transfer," none of the other grounds recognized in the GDPR applies. *See* European Comm'n Br. 14. Article 45, for example, allows transfers to non-EU countries when the European Commission decides "that the third country . . . ensures an adequate level of protection." GDPR art. 45(1). No such decision has been made here. For its part, Article 46 permits transfer under various "appropriate safeguards," but, again, those do not exist in this case. GDPR art. 46(1)–(2). And Article 47 only applies to transfers within a corporate group, not to transfers to non-EU countries. GDPR art. 47.

Nor would Article 49 of the GDPR, which sets forth "derogations for specific situations," authorize the transfer here. The European Commission suggests that two derogations may be relevant to this action, but it does not argue that either derogation would allow Microsoft to comply with the SCA warrant. European Comm'n Br. 15–16. In fact, neither derogation could apply here without swallowing the privacy regime that the MLAT requirement is meant to protect.

a. As an initial matter, Article 49's derogations must "be interpreted strictly," so as not to defeat the GDPR's protections. European Comm'n Br. 16. The GDPR requires that its provisions "be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined." GDPR art. 44. The Article 29 Working Party confirms that "[l]aw enforcement access to personal data" interferes with the "right to protection of personal data" under the EU Charter on Fundamental Rights, so the GDPR's "limitation[s] on the exercise of the rights and freedoms recognised by the Charter . . . must respect the essence of these rights and freedoms." WP29 Statement on Data Protection at 1.

These principles guide *Amici*'s reading of the Article 49 derogations. To interpret the derogations to cover the SCA warrant in this case would undermine the GDPR and the protection for personal privacy it recognizes.

b. The first potentially relevant derogation permits data transfers where "the transfer is necessary for important reasons of public interest." GDPR art. 49(1)(d). Although *Amici* recognize the United States' strong interest in criminal law enforcement, that is not an interest protected by this derogation.

First, the "public interest" must be one "recognised in Union law or in the law of the Member State to which the controller is subject." GDPR art. 49(4). *Amici* read this requirement to limit the "public interest" derogation to public interests of the European Union or its member states, not those of non-EU countries. So does Ireland's Data Protection Commissioner. *See Transfers Abroad*, Office of the Data Protection Commissioner (Ir.), https://goo.gl/ezLigF (last visited Jan. 17, 2018) ("[The public interest derogation] is only likely to be relevant to public sector data controllers and only in circumstances where they can show that there is a substantial *Irish public interest* in the transfer of personal data." (emphasis added)).

*Amici*'s reading of Article 49(4) comports with other provisions of the GDPR, which recognize a "legal obligation" to process personal data only when that obligation is imposed by the European Union or its member states. GDPR art. 6(1)(c), (3). And *Amici*'s reading mirrors the Article 29 Working Party's interpretation of a similar derogation in the 1995 Directive, which could "only be used if the transfer is of interest to the *authorities of an EU Member State themselves*, and not only to one or more public authorities in [a] third country." Article 29 Working Party, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 at 15 (Nov. 25, 2005) (emphasis added).

Second, a broad reading of the "public interest" derogation would supplant the GDPR's detailed limitations on transfers of personal data. As noted, the GDPR provides for transfers to non-EU countries only under specific circumstances, with MLATs providing the primary means for such transfers. GDPR arts. 45–48. The entire purpose of MLATs is to facilitate cooperation between countries in transnational criminal

matters while ensuring that the laws of both countries are not violated. *See* EU MLAT at 4 (stating parties' purpose to "combat crime in a more effective way" and provide "mutual legal assistance in criminal matters"); Ireland MLAT art. 1.1 (providing for "mutual assistance . . . in connection with the investigation, prosecution, and prevention of offenses, and in proceedings related to criminal matters"). If a non-EU country could bypass the MLAT process any time protected personal data could aid a criminal prosecution, Article 48's MLAT requirement would have essentially no effect.

c. The second potentially relevant derogation is irrelevant for much the same reasons. It permits transfers that are "necessary for the purposes of compelling legitimate interests pursued by the data controller which are not overridden by the interests or rights and freedoms of the data subject." GDPR art. 49(1). The European Commission raises the possibility (though does not analyze it) that a "compelling legitimate interest" could be the controller's (here, Microsoft's) interest in complying with non-EU law. European Comm'n Br. 15.

But a data controller's interest in complying with non-EU law is identical to an interest in *not* complying with the GDPR. Moreover, Article 48 addresses precisely those situations in which a non-EU country seeks data stored in the European Union, so the data controller will always have an interest in complying with such a request. It makes no sense to read Article 49's "compelling legitimate interest" derogation to swallow Article 48. *See* GDPR art. 49 (requiring a data controller's interests to be balanced with those of the person who owns the data, requiring an assessment of whether "suitable safeguards" exist in the foreign country prior to the transfer of data, and mandating

that notice be given to the person whose data is transferred). The GDPR is not so self-defeating.

In short, Article 48's limitations on transfers of personal data apply, so the GDPR prohibits Microsoft from complying with the SCA warrant in this case. Instead, unless the Government seeks the data through the recognized MLAT procedure, complying with the SCA warrant would likely require Microsoft to violate EU law.

### B. The Budapest Convention Does Not Authorize The SCA Warrant.

Although the Government's brief does not address the GDPR, the Government does argue that construing the SCA not to apply to data stored abroad would "undermine the United States' compliance with Article 18 of the Budapest Convention." U.S. Br. at 47, 49. With respect, the Government misunderstands the Budapest Convention.

Article 18 of the Budapest Convention requires signatories to "empower [their] competent authorities to order . . . a person in [their] territory to submit specified computer data in that person's possession or control." Budapest Convention art. 18(1)(a). This text is ambiguous as to whether it covers all data wherever it is stored, or just data stored within a signatory's borders. It does not clearly require what the Government seeks in this case, which is unilateral law-enforcement access to personal data stored abroad.

Context resolves the question, however, for the Budapest Convention's other provisions strongly suggest that Article 18 is limited to domestic data. The Convention's preamble recognizes the importance of protecting the "fundamental human right[]" to data privacy. Budapest Convention, preamble

¶¶ 10–11. Article 19, which expressly applies to law-enforcement "[s]earch and seizure of stored computer data," limits a signatory's law-enforcement access to data "stored in its territory." And Article 32 permits unilateral "trans-border" access to data only if the data are "publicly available" or the party who "has the lawful authority to disclose the data" consents.

The Guidance Note to Article 32 makes clear that it—not Article 18—applies when a country tries to "'unilaterally access computer data stored in another [country] without seeking mutual assistance.'" Cybercrime Convention Comm., Council of Europe, *T-CY Guidance Note #3: Transborder Access to Data (Article 32*), at 5–6 (Nov. 5, 2013). None of Article 32's requirements are satisfied in this case. The Government's reading of Article 18 would render superfluous Article 32's limitations on "unilateral transborder access without the need for mutual assistance." *Id.* at 3.

Finally, the Guidance Note to Article 18 contemplates that signatories "may require that subscriber information be requested through mutual legal assistance." Cybercrime Convention Comm., Council of Europe, *T-CY Guidance Note #10: Production Orders for Subscriber Information (Article 18 Budapest Convention)*, at 3 (Mar. 1, 2017). The MLAT between the United States and Germany (both signatories to the Budapest Convention) contains such a requirement. Treaty Between the United States of America and the Federal Republic of Germany on Mutual Legal Assistance in Criminal Matters, art. 1(5), Oct. 14, 2003, T.I.A.S. No. 09-1018. This fact further belies the Government's reading of the Convention.

The Budapest Convention thus does not authorize the SCA warrant in this case or remedy the likely con-

flict between the warrant and the GDPR. To the contrary, the Budapest Convention, as does the GDPR, reflects a strong default rule that countries must seek computer data from other countries through MLATs or other international agreements.

### III. To Avoid Conflicts Between U.S. And Foreign Law, The Court Should Limit The SCA To Data Stored In The United States.

Because requiring Microsoft to comply with the SCA warrant here would likely conflict with the GDPR, the presumption against territoriality is "at its apex." *RJR Nabisco*, 136 S. Ct. at 2107. It is implausible that an application of the SCA that so clearly implicates a foreign data-protection regime could be described as "domestic."

Indeed, the risk of "international discord," *id.* at 2100, is especially high with respect to data. Most of the world's data centers are located outside of the United States. Yevgeniy Sverdlik, *Research: There are Now Close to 400 Hyper-Scale Data Centers in the World*, Data Cntr. Knowledge (Dec. 21, 2017), https://goo.gl/Vxg2sa. The countries in which those data centers are located have their own, often complex data-protection laws. Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 682–713 (2015). If the SCA permits the service of a warrant for data stored anywhere in the world, courts will have to confront conflicts with such laws all the time, if nothing else as a matter of comity. *Cf. Hartford Fire Ins.*, 509 U.S. at 814–18 (Scalia, J., dissenting) (explaining that even if a statute applies extraterritorially, its scope can be limited by international comity). Analyzing such conflicts would plunge district courts into difficult questions of foreign law and expose them to the risk of "erroneously adopt[ing] an interpretation of

U.S. law that carries foreign policy consequences not clearly intended by the political branches." *Kiobel*, 569 U.S. at 116.

The Court should avoid this risk by interpreting the SCA to apply only to data stored within the United States. Such a holding will provide a clear rule for courts considering SCA warrants. It will also let Congress make the policy decision whether to authorize unilateral law-enforcement collection of data stored abroad. Congress, after considering the international implications, may decide to do so, just as other countries have enacted legislation to permit such collection. *See* U.S. Br. 46–47; U.K. Br. 5–6. Or Congress may settle on a different approach, perhaps by specifying the situations in which extraterritorial warrants are appropriate and those in which they are not. Indeed, as recently as 2016 the Government proposed legislation to amend the Electronic Communications Privacy Act, of which the SCA is a part, to authorize access to data stored abroad. Letter from Peter J. Kadzik, Assistant Attorney Gen., to Joseph R. Biden (July 15, 2016).

Whatever Congress decides, however, the Court's decisions recognize that the choice should be Congress's to make. *Kiobel*, 569 U.S. at 116. In the meantime, the Government's MLATs with the European Union and Ireland provide an adequate, legal method for it to get the data it seeks from Microsoft.

## CONCLUSION

The Court should affirm the judgment of the Court of Appeals.

Respectfully submitted,

VINCENT LEVY
DANIEL M. SULLIVAN*
*Counsel of Record
MATTHEW V.H. NOLLER
KEVIN D. BENISH
HOLWELL SHUSTER & GOLDBERG LLP
750 Seventh Avenue
New York, NY 10019
(646) 837-5151
dsullivan@hsgllp.com

*Counsel for Amici Curiae*

January 18, 2018

## APPENDIX

*Amici* consist of the following scholars:

1. Dr. Maja Brkan, Maastricht University Faculty of Law
2. Professor Céline Castets-Renard, Institute of European International and Comparative Law at the University of Toulouse
3. Professor Dr. Mark D. Cole, Faculty of Law, Economics and Finance at the University of Luxembourg
4. Professor Egbert Dommering, Institute for Information Law at the University of Amsterdam
5. Professor Dr. Nikolaus Forgó, Department of Innovation and Digitalisation in Law at the University of Vienna
6. Professor em. Douwe Korff, London Metropolitan University
7. Professor Dr. Eleni Kosta, Tilburg Institute for Law, Technology and Society (TILT) at Tilburg University
8. Professor Katalin Ligeti, University of Luxembourg
9. Dr. Cristina M. Mariottini, Max Planck Institute for Procedural Law
10. Dr. Sylvain Métille, Lecturer in the Faculty of Law, Criminal Justice and Public Administration at the University of Lausanne
11. Professor Dr. Lilian Mitrou, INFOSEC Lab at the University of the Aegean – Greece
12. Professor Oreste Pollicino, Bocconi University
13. Professor Dr. Alexander Pretschner, Technical University of Munich

14. Dr. Gavin Robinson, University of Luxembourg
15. Professor Dr. Cedric Ryngaert, Faculty of Law at Utrecht University
16. Dr. Gerald Spindler, Department of Commercial Law, Multimedia and Telecommunication Law at the University of Goettingen Platz der Goettinger Sieben
17. Professor Peggy Valcke, Faculty of Law at KU Leuven
18. Professor Geert Van Calster, KU Leuven, King's College (London), and Monash University (Australia)
19. Professor Dr. Nico van Eijk, Institute for Information Law at the University of Amsterdam
20. Professor em. Dr. Rolf H. Weber, Faculty of Law at the University of Zurich
21. Dr. Frederik Zuiderveen Borgesius, Vrije Universiteit Brussel and Institute for Information Law Fellow at the University of Amsterdam