No. 17-2

IN THE
Supreme Court of the United States

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL 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 THE EUROPEAN COMMISSION ON BEHALF OF THE EUROPEAN UNION AS *AMICUS CURIAE* IN SUPPORT OF NEITHER PARTY

PATRICK W. PEARSALL
ADAM G. UNIKOWSKY
Counsel of Record
ZACHARY C. SCHAUF
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
aunikowsky@jenner.com

QUESTION PRESENTED

Whether 18 U.S.C. § 2703 authorizes a court in the United States to issue a warrant that compels a U.S.-based provider of email services to disclose data stored outside of the United States.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

TREATIES AND AGREEMENTS

INTEREST OF *AMICUS CURIAE*[1]

The European Commission is the executive body of the European Union. The European Union is composed of twenty-eight Member States.[2] It is a treaty-based international organization[3] with the competence to develop and enforce Union-wide legislation in specified areas of policy, conferred upon the Union by its Member States.

In the European Union, the protection of personal data is a fundamental right protected by Article 8 of the

---

[1] Pursuant to this Court's Rule 37.3(a), counsel for all parties consented to the filing of this brief. Pursuant to this Court's Rule 37.6, *amicus* states that this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than *amicus*, its members, or its counsel made a monetary contribution intended to fund the preparation or submission of this brief.

[2] These Member States are Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

[3] The European Union (EU) is currently based on two treaties setting out its primary law: the Treaty on the European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). Consolidated versions of the TEU and TFEU are published in the Official Journal of the European Union, which was named Official Journal of the European Communities until February 1, 2003. *See Consolidated Versions of the Treaty on European Union & Treaty on the Functioning of the European Union*, June 7, 2016, 2016 O.J. (C 202) 13, 47 (EU).

Charter of Fundamental Rights of the European Union[4] and Article 16(1) of the TFEU. In accordance with Article 16(2) of the TFEU, the European Union has competence to lay down rules relating to the protection of personal data, and rules relating to the free movement of such data.

The European Union has promulgated regulations to protect the privacy of personal data. These regulations implement, and build on, the fundamental rights to privacy and data protection recognized in the European Union's Charter of Fundamental Rights, Dec. 7, 2000, 2000 O.J. (C364) 1, and in international agreements to which EU states are parties, including the European Convention on Human Rights, Nov. 4, 1950, E.T.S. No. 5, and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108. Especially relevant here is Regulation (EU) 2016/679, Apr. 27, 2016, 2016 O.J. (L119) 1—known as the General Data Protection Regulation (or "GDPR")—which was adopted in 2016 and will become effective in May 2018.[5] At the certiorari stage, both

---

[4] The Charter of Fundamental Rights of the European Union has the same legal status as the TEU and the TFEU. *See* TEU art. 6.

[5] Until May 2018, protection of personal data in the European Union is governed by EU Directive 95/46, Oct. 24, 1995, 1995 O.J. (L281) 31. But because any warrant in this case would likely be enforced after May 2018, this brief focuses on the GDPR's rules. In substance, the provisions of the GDPR on transfer of personal data to a non-EU state are largely similar to those in EU Directive 95/46.

parties made claims about Article 48 of the GDPR and whether, if Microsoft Corp. ("Microsoft") complies with the warrant issued in this case, Microsoft would be at risk of violating the GDPR. *Compare* Pet. 32-33 n.7, *with* Br. in Opp. at 17.

The European Union has significant interests in this case. First, the European Union has an interest in ensuring that the Court proceeds based on a correct understanding of EU law.[6] This case concerns personal data stored in a datacenter in the European Union that is operated by an EU-based subsidiary of Microsoft. Storing such data and transferring it from the European Union to the United States constitutes data "processing" to which the EU data protection rules apply.

Second, the European Union submits this brief to reaffirm its commitment to international law enforcement cooperation between it and the United States. The European Union and its Member States are party to numerous treaties and international agreements providing for law enforcement cooperation with the United States, including the Mutual Legal Assistance Agreements with the United States of

---

Where relevant, this brief will identify the corresponding provisions currently applicable under Directive 95/46.

[6] The European Union provides its views in this brief without prejudice to any interpretation that the European Court of Justice may give in a subsequent case.

America.[7] These agreements reflect the value that the European Union attaches to law enforcement cooperation. The European Union has an interest in ensuring that such law enforcement cooperation continues to take place within a legal framework that avoids conflicts of law, and is based on ongoing dialogue, voluntary cooperation, and respect for each others' fundamental interests in both privacy and law enforcement.

---

[7] The Member States are also parties to the Council of Europe Convention on Cybercrime. *See* Council of Europe Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185; *cf. id.* art. 18.1(a). Furthermore, the European Union is party to the Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, Aug. 8, 2012, 2012 O.J. (L215) 5 ("PNR Agreement"); the Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, July 27, 2010, 2010 O.J. (L195) 5; and the European Union-United States Agreement on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, June 2, 2016, 2016 O.J. (L336) 3 ("Umbrella Agreement"), which complements existing cooperation agreements in the area of criminal law enforcement with the necessary data protection safeguards. It covers data transfers between law enforcement authorities, but also transfers from private entities in the European Union to law enforcement authorities in the United States if those transfers are based on an international agreement, such as the PNR Agreement.

SUMMARY OF ARGUMENT

I. This case concerns whether a U.S. court may issue a warrant requiring Microsoft to produce data stored in the European Union, subject to EU data protection laws. In the European Union's view, any domestic law that creates cross-border obligations should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. The European Union understands this Court's precedents to embody similar principles. Insofar as these precedents aim to avoid risks of conflict with foreign law, they may invite an inquiry into the content of foreign law.

II. The relevant foreign law here is the GDPR, a comprehensive EU framework for regulating privacy of personal data. The GDPR contains specific rules to ensure that the high level of data protection within the European Union is ensured where personal data is transferred to a non-EU state. Article 48 specifically contemplates transfers ordered by courts in "third countr[ies]" like the United States. GDPR art. 48. The GDPR provides that such orders "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," but "without prejudice to other grounds for transfer" pursuant to the GDPR. *Id.*

III. There is thus no doubt that the European Union is actively regulating the issues at this case's heart, including how data stored in the European Union must

be protected, and when such data may be transmitted abroad.

ARGUMENT

In this case, a U.S. court issued a warrant requiring Microsoft to produce data stored in the European Union, subject to EU data protection laws. This Court has long recognized that application of domestic law to foreign conduct may cause friction with foreign countries and result in violations of international law, and it has developed doctrines designed to mitigate those risks. The European Union submits this brief to aid this Court's consideration of those doctrines. In particular, the brief lays out the GDPR's comprehensive framework for regulating the protection of EU personal data.

I. It Is Appropriate For The Court To Consider EU Domestic Law As It Pertains To Searches Of Data Stored In The European Union

While the European Union takes no position on the ultimate question of the Stored Communication Act's proper construction under U.S. law, the European Union submits that it would be appropriate for the Court to consider EU domestic law as it pertains to searches of data stored in the European Union.

In the European Union's view, from the perspective of public international law, when a public authority requires a company established in its own jurisdiction to produce electronic data stored on a server in a foreign jurisdiction, the principles of territoriality and comity under public international law are engaged, and the

interests and laws of that foreign jurisdiction must be taken into account.

Any domestic law that creates cross-border obligations—whether enacted by the United States, the European Union, or another state—should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity. The European Union's foundational treaties and case law enshrine the principles of "mutual regard to the spheres of jurisdiction" of sovereign states and of the need to interpret and apply EU legislation in a manner that is consistent with international law. *See* TEU arts. 3(5), 21(1); Case 52/69, *Geigy v. Commission*, ¶ 11, ECLI:EU:C:1972:73; Case C-366/10, *Air Transport Ass'n of America v. Sec'y of State for Energy and Climate Change*, ¶ 123, ECLI:EU:C:2011:864.

The European Union understands this Court's precedents to embody similar principles via two canons of construction—the presumption against extraterritoriality, and the *Charming Betsy* canon—which each serve to mitigate the risk of conflict with foreign law and advance international comity. *See RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2100, 2107 (2016) (extraterritoriality canon "avoid[s] the international discord that can result when U.S. law is applied to conduct in foreign countries," and "the need to enforce the presumption is at its apex" when there is a "risk of conflict between [an] American statute and … foreign law" (quotation marks omitted)); *F. Hoffmann-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164 (2004) (Under *Charming Betsy* canon, a statute "ought

never to be construed to violate the law of nations if any possible construction remains," and must be interpreted in light of "principles of prescriptive comity" that prohibit "unreasonable interference with the sovereign authority of other nations" (internal quotation marks omitted)).

Insofar as these canons aim to avoid risks of conflict with foreign law, they may invite an inquiry into the content of foreign law.

II. Production Of Data Stored In The European Union Is Addressed By EU Privacy Law.

In this case, the United States demands that Microsoft produce personal data stored in Ireland. The "processing" of personal data—which includes collection, storage, and transfer of personal data[8]—in the European Union is regulated by EU privacy law under the GDPR. The GDPR is a comprehensive framework, providing both general rules for the processing of personal data and specific rules for transfer of personal data to non-EU states.

A. The GDPR's General Rules For Processing Of Personal Data.

The GDPR "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." GDPR art. 1(2).

---

[8] The list of activities that qualify as "processing" is contained in Article 4(2).

The key principles for the processing of personal data are laid down in Article 5.[9] That article requires, among other things, that personal data be "processed lawfully, fairly and in a transparent manner in relation to the data subject" and "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." *Id.* art. 5(1)(a), (b). Moreover, personal data must be "adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed"; "accurate and, where necessary, kept up to date"; and processed "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing." *Id.* art. 5(1)(c), (d), (f). The "controller" of the data is "responsible for, and [must] be able to demonstrate compliance with" the GDPR's requirements. *Id.* arts. 4(7), 5(2).

Every "processing" of personal data must meet the requirements of Article 6 (which concerns the "[l]awfulness of processing" generally) or Article 9 (which imposes additional restrictions on processing of "special categories of personal data" that are especially sensitive).[10] In addition, if such processing involves a transfer of personal data to a non-EU state, the

---

[9] These key principles can already be found in Article 6 of Directive 95/46.

[10] See also the equivalent provisions in Articles 7 and 8 of Directive 95/46.

controller must also satisfy the requirements for transfers in Chapter 5, as discussed in the next section.

Under Article 6, processing is "lawful only if and to the extent that at least one of" six enumerated grounds "applies." *Id.* art. 6(1). In the present case, in the absence of a European Union or Member State law requiring Microsoft's "processing," either as a legal obligation or as a task carried out in the public interest of the European Union or a Member State, *id.* art. 6(1)(c), (e), the transfer could potentially qualify as "necessary for the purposes of the legitimate interests pursued by the controller"—namely, the interest in not being subject to legal action in a non-EU state. *Id.* art. 6(1)(f). This provision, however, only allows processing "where such interests are [not] overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." *Id.* The provision thus contemplates a balancing exercise, taking into account all relevant circumstances of the situation.

The GDPR grants persons whose personal data are processed a number of specific rights, such as rights to access data, to rectify errors, to erase data, and to object. *Id.* arts. 15, 16, 17, 21. The GDPR also imposes obligations on the persons processing personal data.[11] These include requirements to keep records of data processing, to ensure the security of the data processing, and, under certain conditions, to give notice of data

[11] See the equivalent provisions in Articles 12 and 14 of Directive 95/46.

breaches and to perform data protection impact assessments. *Id.* arts. 30, 32, 33, 34.[12]

Monitoring application of the GDPR's provisions lies in the first instance with national "supervisory authorities." *Id.* art. 51(1).[13] These authorities "act with complete independence in performing [their] tasks" under the GDPR. *Id.* art. 52(1). These supervisory authorities receive complaints, *id.* art. 57(1)(f), and initiate investigations, *id.* art. 57(1)(h). They have several remedial powers, including power to order the suspension of data flows to a recipient outside the European Union. *Id.* art. 58(2)(j). They can also assess administrative fines against violators, subject to review in national courts, in amounts that vary with the severity of the violation. *Id.* art. 83(1). More severe violations, including violations of the rules governing "transfers of personal data to a recipient in a third

---

[12] These obligations replace or further elaborate requirements in Directive 95/46.

[13] The European Commission, as the "guardian of the EU treaties," has authority to ensure that Member States comply with EU laws, including the GDPR. Typically, the Commission acts only if there are structural shortcomings in how Member States apply EU laws, not in individual cases. As explained in footnote 6, the European Court of Justice has the final authority to interpret EU law. The independent supervisory authorities were already established under Article 28 of Directive 95/46. These authorities have a special status that stems directly from the EU Charter of Fundamental Rights and the TFEU. *See* EU Charter of Fundamental Rights, art. 8(3); TFEU art. 16(2). On the importance of independent supervision in the context of international transfers, see Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications*, ¶ 68, ECLI:EU:C:2014:238.

country," are subject to fines of up to €20 million or 4% of total worldwide annual turnover, whichever is higher. *Id.* art. 83(5).

B. The GDPR's Specific Rules For Transfer Of Personal Data To Non-EU States.

The GDPR, in Chapter 5, contains specific, additional rules for transfer of personal data from the European Union to a non-EU state. These specific rules implement the express obligation laid down in the EU Charter of Fundamental Rights to protect personal data and are "intended to ensure that the high level of that protection continues where personal data is transferred to a [non-EU state]." Case C-362/14, *Schrems v. Data Protection Commissioner*, ¶ 72, ECLI:EU:C:2015:650; Opinion 1/15, ¶ 214, ECLI:EU:C:2017:592. Transfer can be lawful under these rules only if the data processing is lawful under the GDPR's other rules. *See also* GDPR art. 44.

Article 45 allows for transfers when the European Commission has made an "adequacy decision"; Article 46 allows for transfers if "the controller or processor has provided appropriate safeguards," based on an enumerated list of safeguards, "and on condition that enforceable data subject rights and effective legal remedies for data subjects are available." GDPR arts. 45(3), 46(1)-(3). Among others, Article 46 covers international agreements (providing appropriate safeguards), contractual tools and legally binding rules for transfers within a corporate group ("binding corporate rules," governed by Article 47). If none of these grounds apply, a transfer to a third country may still proceed if one of the "Derogations for specific

situations" pursuant to Article 49 applies, as discussed further below. *Id.* art. 49.[14]

Article 48 concerns "[t]ransfers or disclosures not authorized by Union law." This article was adopted specifically to address disclosures compelled by non-EU states, as is evident from the Recital that accompanies Article 48.[15] Recital 115 observes that "[s]ome third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States," including "judgments of courts … requiring a controller or processor to transfer or disclose personal data, and which are not 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." GDPR, Recital 115. The GDPR warns that "extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation." *Id.* And it emphasizes that transfers "should only be allowed where the conditions of this Regulation for a transfer to third countries are met." *Id.*

---

[14] To a large extent, the grounds for transfer in Articles 45-47 and 49 already exist under Directive 95/46. *See* Directive 95/46 arts. 25, 26.

[15] The GDPR's recitals provide "the … reasons the articles of the GDPR have been adopted." *See* GDPR Recitals. The recitals stem from the general obligation to state the reasons on which EU legal acts are based. *See* TFEU art. 296.

Article 48 makes clear that a foreign court order does not, as such, make a transfer lawful under the GDPR. It provides that "[a]ny judgment of a court or tribunal and any decision of an administrative authority 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." *Id.* art. 48. The GDPR thus makes "mutual legal assistance treaties," or "MLATs," the preferred option for transfers. Such treaties provide for collection of evidence by consent, and embody a carefully negotiated balance between the interests of different states that is designed to mitigate jurisdictional conflicts that can otherwise arise. As relevant here, the United States has ratified MLATs with both the European Union and Ireland,[16] and Article 48 by its terms contemplates those two governing MLATs.

As just described, however, Article 48 provides that its requirements are "without prejudice to other grounds for transfer" in Chapter 5. If none of the grounds in Article 45 to 47 apply—as would likely be true in the present situation—a transfer to a third country thus could proceed only if it qualified under

---

[16] *See* Agreement on Mutual Legal Assistance Between the United States of America and the European Union, June 25, 2003, 2003 O.J. (L181) 34; Treaty Between the United States of America and Ireland on Mutual Legal Assistance in Criminal Matters, Jan. 18, 2001, S. Treaty Doc. No. 107-9 (2002).

Article 49. In the present situation, depending on the precise circumstances, the two following provisions seem most relevant:

- A transfer "necessary for important reasons of public interest." GDPR art. 49(1)(d). Notably, to qualify, this "public interest" must be one "recognised in Union law or in the law of the Member State to which the controller is subject." *Id.* art. 49(4). In general, Union as well as Member State law recognize the importance of the fight against serious crime—and thus criminal law enforcement and international cooperation in that respect—as an objective of general interest. Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications*, ¶ 42, ECLI:EU:C:2014:238; Opinion 1/15, ¶ 148, ECLI:EU:C:2017:592. Article 83 of the TFEU identifies several areas of crime that are particularly serious and have cross-border dimensions, such as illicit drug trafficking.

- A transfer "necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject." GDPR art. 49(1). The legitimate interest could, again, be the interest of the controller in not being subject to legal action in a non-EU state. Such transfers are permissible "only if the transfer is not repetitive," only if it "concerns only a limited number of data subjects," and only if "the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data." *Id.*

> Relevant circumstances might include procedural guarantees under which the foreign court order was adopted, as well as applicable data protection rules in place in the third country. The controller must also "inform the supervisory authority of the transfer." *Id.*

It should also be noted, however, that Article 49 is entitled "Derogations for specific situations." Therefore, these grounds are to be interpreted strictly. *Cf.* Case C-119/12, *Probst v. mr.nexnet GmbH*, ¶ 23, ECLI:EU:C:2012:748.

CONCLUSION

The European Union takes no position on the ultimate question of the SCA's proper construction under U.S. law. The European Union respectfully offers the explanation set forth in this brief of the EU data protection rules in order to facilitate this Court's inquiry under U.S. law.

Respectfully submitted,

PATRICK W. PEARSALL
ADAM G. UNIKOWSKY
Counsel of Record
ZACHARY C. SCHAUF
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
aunikowsky@jenner.com