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 THE COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENT

NOWELL D. BAMBERGER
Counsel of Record
BRANDON N. ADKINS
MELISSA GOHLKE
CLEARY GOTTLIEB STEEN & HAMILTON LLP
2000 Pennsylvania Ave NW
Washington, D.C. 20006
(202) 974-1500
nbamberger@cgsh.com

Counsel for Amicus Curiae

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001

CORPORATE DISCLOSURE STATEMENT

The Council of Bars and Law Societies of Europe is an international non-profit association. It has no corporate parent, and no publicly held company has any ownership interest in it.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND RULE

OTHER AUTHORITIES

INTERESTS OF *AMICUS CURIAE*[1]

Amicus Curiae, the Council of Bars and Law Societies of Europe ("CCBE"), is an international non-profit association which has been, since its creation, at the forefront of advancing the views of European lawyers and defending legal principles upon which democracy and the rule of law are based. Founded in 1960, the CCBE is recognized as the voice of the European legal profession representing, through its member bars and law societies in forty-five member states of the Council of Europe (including twenty-eight member states of the European Union), more than one million European lawyers. The regulation of the profession, the defense of the rule of law, human rights, and democratic values are the most important missions of the CCBE. To that end, the CCBE routinely works with other lawyers' organizations around the world on issues of common interest to the legal profession, such as the independence of the profession and the judiciary, lawyer-client confidentiality, access to justice, rule of law, and the ability of all lawyers to practice their profession freely and without harassment or hindrance.

---

[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.

The CCBE's interest in this case arises from the threat posed by the Government's arguments to the international order under which cross-border law enforcement is routinely conducted. The members of the various national Bars and Law Societies, which are member organizations of the CCBE, practice and represent clients in jurisdictions outside the United States that have their own laws, legal traditions, and law enforcement regimes. Many of those jurisdictions have entered into agreements with the United States that provide clear, efficient, and mutually-agreed mechanisms for obtaining information from their territories in furtherance of U.S. criminal investigations. The Government's approach would upset that order and settled rules of international comity and sovereignty, permitting the United States to execute searches in the territory of other sovereigns, inviting other countries (who may not share a common legal tradition) to do the same and subjecting recipients of such requests to impossibly conflicting legal obligations.

SUMMARY OF THE ARGUMENT

For the CCBE and its members, the central question in this case is where, physically, an electronic search and seizure takes place. The Government's argument that it conducts a purely "domestic" search by executing in the United States a warrant pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. § 2703, to obtain electronic communications located in Ireland would place the SCA in conflict with the laws of countries around the world, would undermine established bilateral and multilateral frameworks for cross-border cooperation in criminal cases, and would

subject foreign parties to competing irreconcilable legal obligations. The Second Circuit rightly held that the search in this case, which the parties agree was intended to yield electronic communications from Ireland, was extraterritorial and therefore outside of the scope of what Section 2703 permits. The Court should affirm.

Around the world, nations are increasingly regulating the way that information, particularly personally identifiable information like electronic communications, is processed, transferred, and disclosed. In Europe, organizations and companies that hold such data are subject to a variety of legal restrictions on how such data may be handled. These include, within the European Union, Directive 95/46/EC of the European Parliament and of the Council, 1995 O.J. (L 281) 31 [hereinafter, "EU Directive 95/46"], shortly to be superseded by the General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1 [hereinafter, "GDPR"], which takes effect in May, as well as existing national laws and regulations. Many European countries – and other countries around the world – regulate the circumstances under which private correspondence may be disclosed to law enforcement, impose professional secrecy obligations on various professions (including lawyers), or recognize the existence of professional privilege, including legal professional privilege, and restrict the ability of private parties to transfer various categories of information abroad.

Just as the United States enacted the SCA to protect the privacy interests of Americans, other countries enact legislation to protect similar interests of their citizens. Persons, including individuals, companies, and organizations, that hold electronic correspondence and various other types of information are subject to the laws of the countries in which they hold that information. In many circumstances, they may be restricted from disclosing information or transferring it to the United States (or other foreign countries) by domestic law. For over 200 years, this Court has recognized the sovereign right of other nations to regulate commerce and the rights of their citizens within their respective territories.

Section 2703 permits the Government to obtain a warrant authorizing the search and seizure of electronic communications. It expressly refers to and incorporates the traditional mechanisms for issuance of warrants – not subpoenas – under U.S. law and the Federal Rules of Criminal Procedure. Those rules have historically been applied to preclude magistrates from issuing warrants with extraterritorial effect. Nothing in the SCA suggests that Congress intended a different outcome when it comes to the search and seizure of electronic communications.

Were this Court to adopt the Government's argument that a search pursuant to a Section 2703 warrant is "domestic" regardless of where the communications seized are physically located, it would invite incessant conflicts between U.S. jurisdiction and foreign law. Companies and organizations and individuals faced with Section 2703 warrants served in this country would be constantly required to choose

between contumacy and violating foreign law. Foreign governments' sovereign authority to protect the privacy interests of their citizens and others to whom they accord protection would be undermined and foreign individuals, companies, and organizations, and their respective lawyers, would be imperiled in their observance of their home countries' laws and standards regarding professional secrecy and privilege. This cannot have been what Congress intended to accomplish; if it were, Congress certainly did not say so clearly in the SCA.

ARGUMENT

According to the Government's argument, "[b]ecause Section 2703 focuses on the domestic disclosure of information to the government, this case involves a permissible domestic application of the statute." Pet'r's Br. 26. In the decision below, the Second Circuit correctly held that Section 2703 instead focuses on the protection of covered electronic data, and therefore that the relevant search and seizure occurs where the data is located and stored. Microsoft Corp. v. United States, 829 F.3d 197, 220 (2d Cir. 2016). The Second Circuit's interpretation best accords with the language and history of the SCA and most effectively interprets the statute in a way that accomplishes Congressional intent while avoiding conflicts with the laws of other nations and the obligations they impose on the processing, transfer, and disclosure of electronic communications within their respective territories.

I. The Government's Interpretation Of Section 2703 Would Authorize Extraterritorial Searches In Conflict With The Domestic Laws Of Nations Around The World.

While the advancement of technology has rendered the world increasingly interdependent, it nonetheless remains – as Justice Marshall wrote more than two centuries ago – "composed of distinct sovereignties, possessing equal rights and equal independence, whose mutual benefit is promoted by intercourse with each other, and by an interchange of those good offices which humanity dictates and its wants require." The Schooner Exch. v. McFaddon, 11 U.S. (7 Cranch) 116, 136 (1812). In the context of that international order, "[i]t is universally recognized, as a corollary of state sovereignty, that officials of one state may not exercise their functions in the territory of another state without the latter's consent." Restatement (Third) of Foreign Relations Law § 432 cmt. b (1987); see also The Apollon, 22 U.S. (9 Wheat.) 362, 371 (1824) ("It would be monstrous to suppose that our revenue officers were authorized to enter into foreign ports and territories, for the purpose of seizing vessels which had offended against our laws."). This principle rests both on considerations of sovereignty and reciprocity. "It serves to protect against unintended clashes between our laws and those of other nations which could result in international discord." E.E.O.C. v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991); see also The Apollon, 22 U.S. at 371–72 ("[A]n universal right of search . . . has never yet been acknowledged by other nations, and would be resisted by none with more pertinacity than by the American.").

A. The Government's Argument Ignores Increasing Regulation Regarding The Use, Transfer, And Disclosure Of Personal And Other Information In Other Countries.

Within its respective sphere, each sovereign has the authority to prescribe laws governing the protection of the privacy of its citizens, including the circumstances under which those citizens' private papers and effects may be seized and transferred to law enforcement. See, e.g., Laker Airways Ltd. v. Sabena, Belgian World Airlines, 731 F.2d 909, 921 (D.C. Cir. 1984) ("The prerogative of a nation to control and regulate activities within its boundaries is an essential, definitional element of sovereignty. Every country has a right to dictate laws governing the conduct of its inhabitants."); see also The Antelope, 23 U.S. 66, 122 (1825) ("No principle of general law is more universally acknowledged, than the perfect equality of nations. . . . It results from this equality, that no one can rightfully impose a rule on another."); Interamerican Ref. Corp. v. Texaco Maracaibo, Inc., 307 F. Supp. 1291, 1298 (D. Del. 1970) ("It requires no precedent, however, to acknowledge that sovereignty includes the right to regulate commerce within the nation.").[2]

---

[2] In analogous contexts, federal courts have long recognized and given effect to foreign sovereigns' authority to regulate activities within their respective territories. See, e.g., W.S. Kirkpatrick & Co., Inc. v. Environmental Tectonics Corp., Intern., 493 U.S. 400, 405 (1990) (Act of State Doctrine); Mannington Mills, Inc. v. Congoleum Corp., 595 F.2d 1287, 1293 (3d Cir. 1979) (foreign sovereign compulsion doctrine).

Different governments regulate the disclosure of information and personal privacy differently. In the United States, for example, Congress and state legislatures have enacted various provisions protecting certain information and prescribing the circumstances under which disclosure may be compelled. See, e.g., 50 U.S.C. § 1801 et seq. (Foreign Intelligence Surveillance Act, describing conditions for approval of electronic surveillance in the United States); 12 U.S.C. § 3401 et seq. (Right to Financial Privacy Act, defining the circumstances under which individuals' financial records may be searched); Cal. Penal Code § 1546 (California Electronic Communications Privacy Act). Indeed, the SCA itself is an example of how Congress chose to strike the balance between privacy and law enforcement interests within the United States. See S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557.

In Ireland, no fewer than three separate sources of law regulate the protection of privacy interests of persons and the circumstances under which those interests may be infringed. These include (i) Irish national law, see, e.g., In re Ward of Court (withholding medical treatment) (No. 2), [1995] 2 I.R. 79, 125 (Ir.) ("[T]he right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State." (internal quotation marks omitted)); CRH Plc. v. Competition & Consumer Prot. Comm'n, [2017] I.E.S.C. 34, at ¶ 54 (Ir.) (MacMenamin, J.) ("The right to privacy is an increasingly important constitutional value in an age where privacy is challenged."), (ii) European Union law, see, e.g., EU Directive 95/46, as implemented in Ireland by the Irish Data Protection

Act 1988, as amended, and (iii) the European Convention on Human Rights ("ECHR"), see, e.g., ECHR art. 8, Nov. 4, 1950, E.T.S. No. 5 ("Everyone has the right to respect for his private and family life, his home and his correspondence. . . . There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society . . . ."). [3] Both the Irish courts and the European Court of Justice have recognized the transfer of personal information by a private company to the United States outside an appropriate framework ensuring adequate protection thereof, is a violation of these requirements. See Schrems v Data Protection Comm'r, Case C-362/14, EU:C:2015:650; Data Protection Comm'r v Facebook Ireland Limited, [2017] IEHC 545.

Other countries have adopted laws providing additional or different protections against the disclosure of different types of information, and in some cases even domestic courts of those countries would lack the authority to compel disclosure. See, e.g., Code Monétaire et Financier du France art. L511-33 (Fr.) (authorizing disclosure of professional secrets by a financial institution in criminal, but not civil, cases); U.K. Investigatory Powers Act 2016, c. 25 (prescribing mechanisms for obtaining warrants for electronic

---

[3] The ECHR accords Human Rights to both natural and legal persons. Signatories to the ECHR have undertaken not only a negative obligation against conducting unlawful searches, but an affirmative obligation to "secure to everyone within their jurisdiction the rights and freedoms defined" in the Convention, ECHR art. 1, an obligation that is enforceable in direct claims by their citizens and others within the jurisdiction, see id. art. 34.

surveillance in the U.K.); Bundesverwaltungsgericht [BVerwG] [Federal Constitutional Court] Feb. 27, 2008, BVerfG ¶ 247 (Ger.) (Statutory authorizations of secret access to information technology systems must be "contingent on the existence of factual indications of a concrete danger to a predominantly important legal interest . . . [such as] . . . life, limb and freedom of the individual.").

European laws concerning the protection of personal data are of particular relevance. The approach European nations (and many other nations around the world) have taken to the protection of personally identifiable information is different from the approach taken by the United States. Under EU Directive 95/46, which is currently in force and was at the relevant time, and relevant Irish national law enacted pursuant thereto, an entity that processes data – for example, by storing data or retrieving it – using equipment within the territory of a European Union Member State must do so in accordance with European data protection and privacy laws. See Data Protection (Amendment) Act 2003 § 2(b) (Act No. 6/2003) (Ir.) (amending Data Protection Act 1988 § 1 (Act No. 25/1988)), http://www.irishstatutebook.ie/eli/2003/act (data protection law applies to a data controller that "makes use of equipment in the State for processing the data"). Among the requirements of that legislation is a prohibition on cross-border transfers to countries that do not afford similar legal protection to personal data (including the United States), and that prohibition is subject to very limited exceptions. See id. § 12 (amending Data Protection Act 1988 § 11). While those exceptions may apply in certain cases, they will not apply in all (or even most) cases. And while the

purpose of the transfer is very much relevant under this approach, the recipient of a Section 2703 warrant will seldom know the purpose for which the Government seeks information or be in a position to evaluate whether that purpose comports with relevant law. Indeed, historically, compliance with a foreign judicial request has not been viewed as such a proper purpose by itself.[4]

Around the world, different countries' approaches to balancing their citizens privacy interests and law enforcement's access to records differ even more dramatically. Some countries afford citizens relatively little, if any, protection against government intrusion into their private correspondence. For example, recently-enacted legislation in Russia, which takes effect in July 2018, includes a provision requiring the content of transmitted messages and other communications and records of telephone communications to be preserved for six months and forwarded to the security services upon request. See Federal Law No. 374 On Amending the Federal Law on Counterterrorism and Select Legislative Acts Concerning the Creation of Additional Measures Aimed at Countering Terrorism and Protecting Public Safety,

---

[4] This position has been confirmed by the Article 29 Working Party, a body comprised of representatives from national data protection authorities and the European Commission, which emphasized in 2009 guidance on EU Directive 95/46 that "[a]n obligation imposed by a foreign legal statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate." Working Document 1/2009 on Pretrial Discovery for Cross Border Civil Litigation, Feb. 11, 2009 (WP 958) 9.

art. 19.[5] Likewise, while the constitution of the People's Republic of China protects the "[f]reedom and privacy of correspondence," that protection is qualified by the rights of the State in cases involving security or criminal investigation. Chinese Const. art. 40, http://www.npc.gov.cn/englishnpc/Constitution/node_2825.htm; see also Telecommunications Regulations of the People's Republic of China (promulgated by the State Council), Sept. 25, 2000, art. 66, (providing for the privacy of telecommunications, subject to exemptions for examination by State security organs and prosecutorates).

Other countries have expressly legislated that the collection of certain types of information from within their territories – whether by public officials or private parties acting at their direction – is prohibited, often at the risk of criminal sanctions. In a number of cases, such legislation was overtly or implicitly adopted out of concern regarding the extraterritorial reach of U.S. legal process. French law, for example, prohibits the transfer of certain categories of information abroad for use as evidence in legal proceedings. Loi 68-678 du 26 Juillet 1968 relative à communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personne physiques ou morales étrangères [Law No. 68-678 of July 26, 1968 relative to communication documents and information of an Economic, commercial or technical nature to foreign natural or legal persons]; see Société Nationale Industrielle Aérospatiale v. U.S.

---

[5] The Library of Congress Global Legal Monitor published a summary of the new law at http://www.loc.gov/law/foreign-news/article/russia-new-electronic-surveillance-rules/.

Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 526 & n.29 (1987). Legislation in the United Kingdom likewise prohibits the cross-border transfer of certain types of information in certain circumstances, subject to criminal penalties. See Protection of Trading Interests Act (1980), c. 2, § 2. Under Swiss law, any person who obtains a manufacturing or trade secret in Switzerland with a view to its transmission to a foreign agent is guilty of industrial espionage. Schwizerisches Strafgesetzbugh [StGB] [Criminal Code] Dec. 21, 1937, SR 757 (1938), Dec. 21, 1937, SR 757, art. 273. The European Union's GDPR, which takes effect in May 2018, both prohibits the transfer of personal information to countries (including the United States) that have not been found to afford a similar type of protection to personal information and also expressly provides that a judgment of a foreign court requiring transfer of data "may *only* be recognized or enforceable in any manner if based on an international agreement," thus making mutual legal assistance treaties the preferred option for transfers. GDPR art. 48 (emphasis added). Though article 49 of the GDPR might appear to admit in limited circumstances of the possibility of a data transfer otherwise than by international agreement, Br. of European Commission 14–16, the derogations are narrow and to be construed strictly. Similarly, Brazilian law requires a Brazilian court order before an internet provider may produce data stored in Brazil or communications to or from a party in Brazil. See Marco Civil da Internet, Lei No. 12.965 de 23 Abril de 2014, https://www.publicknowledge.org/documents/marco-civil-english-version. China's recently-enacted cybersecurity law also requires that certain types of data be held within China, presumably achieving the dual objectives of preventing access by

foreign governments and ensuring a right of access by the Chinese government. See People's Republic of China Network Security Law (Nov. 7, 2016), http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm.

What these different approaches collectively demonstrate is that when the power to issue warrants under Section 2703 is interpreted to permit orders compelling service providers to seize data stored abroad and turn it over to U.S. law enforcement, that power will *inevitably* come in direct conflict with the legislation of foreign governments, and that conflict will relate to how data is stored, processed and transferred *in foreign countries*. Whether such a conflict exists in any particular case is less relevant than the observation that Congress cannot be assumed to have intended to embark on a policy of such expansive extraterritorial seizures without saying so expressly. But the Government's position not only assumes this, it goes a step forward and assumes that in issuing Section 2703 warrants, courts are not obligated to consider the interests of foreign governments, their citizens, others who are protected by the privacy laws of foreign sovereigns, or the legitimate regulation by foreign governments of the conduct of data-processing operations within their jurisdictions.

B. The Government's Position Affords No Meaningful Consideration To Foreign Law Concerning Legal Privilege And Professional Secrecy.

As an association of bars and law societies, CCBE also has a particular concern regarding the implications of the Government's position on the rights of lawyers and their clients to engage in confidential communications. The Government's argument raises particular concerns regarding the ability of lawyers and their clients to preserve privileges and rights to confidentiality when material is seized from their home country and transferred to the United States. Across Europe, different countries take different approaches to the law of privilege. See, e.g., AM&S Europe Ltd. v. Comm'n of the European Communities, 1982 E.C.R. 1577, 1610 (E.C.J. 1982) ("[I]t is apparent from the legal systems of the Member States that, although the principle of such protection is generally recognized, its scope and the criteria for applying it vary . . . ."). In the United Kingdom and Ireland, principles of legal professional privilege – comprised of the privilege attaching to legal advice and to a lawyer's preparations for litigation – are broadly analogous to legal privileges recognized in the United States. See, e.g., Balabel v Air India [1988] Ch. 317 (EWCA); McMullen v Kennedy [2007] IEHC 263. In many civil law countries, the obligation of professional secrecy is imposed on the lawyer by the state, may be subject to criminal sanctions, and in many cases may not be waived even by the client. See, e.g., Art. 66-5 de Loi 71-1130 du 31 décembre 1971 portant réforme de certaines professions judiciaires et juridiques [Art. 66-5 of Law 71-1130 of December 31, 1971 regarding the reform of

certain judicial and legal professions] ("[G]enerally all documents held in a file are covered by professional secrecy."); Code Pénal [Penal Code] art. 226-13 (Fr.) (imposing criminal sanctions for violation of professional secrecy); Codice di condotta professionale 13 & 28 [Code of Professional Conduct Art. 13 & 28] (It.) (requiring lawyers to maintain professional secrecy); Strafgesetzbugh [StGB] [Criminal Code], § 203(1) para. 3 (Ger.) (failure to observe professional secrecy constitutes a criminal misdemeanor).

Across Europe, the ECHR requires signatories (which include EU members, but also all forty-seven countries of the Council of Europe) to ensure the sanctity of the legal professional privilege or professional secrecy within their territories. Specifically, these obligations have been found to adhere in Article 6 (which protects the right "to a fair and public hearing") and Article 8 (concerning the right to privacy). The protection afforded by Article 6 is absolute (which is to say it cannot be derogated from for any reason whatever). In relation to Article 8, the European Court of Human Rights has asserted that "while Article 8 protects the confidentiality of all 'correspondence' between individuals, it affords strengthened protection to exchanges between lawyers and their clients." Michaud v. France, 2012-VI Eur. Ct. H.R. 89, 132 ¶118; see also Council of Bars & Law Societies of Europe, CCBE Recommendations: On the protection of client confidentiality within the context of surveillance activities 13–16, http://www.ccbe.eu/documents/publications/ (summarizing judgments of the European Court of Human Rights recognizing a right to confidentiality of lawyer-client communications in the context of law enforcement

surveillance). By enacting legislation enforcing the ECHR, countries that are parties to it – like Ireland – have incorporated these protections into their national laws. See, e.g., European Convention on Human Rights Act (Act No. 20/2003) (Ir.).

The Government's position fails to acknowledge the particular concerns that foreign lawyers have regarding the seizure by the United States of potentially privileged material held on email and data servers throughout Europe. European courts are obligated, in the discharge of their own legal process, to afford due respect to considerations of privilege. See, e.g., Vinci Construction and GTM Génie Civil et Services v. France, App. Nos. 63629/10 and 60567/10, 2 April 2015 (Eur. Ct. of H. R.) (holding that a broad undifferentiated seizure of email correspondence, including correspondence between a lawyer and client, pursuant to a French court order violated the fundamental rights guaranteed under article 8). But a client (or, in relevant cases, a lawyer) whose privileged correspondence stored on a European server is seized by the Government pursuant to a Section 2703 warrant would have no redress – she would likely not have an opportunity to intervene because the Government would not be required to provide notice of the seizure, see 18 U.S.C. § 2703(b)(A), and the procedure would not be supervised by a judicial authority that is obligated to respect the privileges or professional secrecy obligations that may attach to the materials seized.

C. The Presumption Against Extraterritoriality And The "Charming Betsy Doctrine" Favor An Interpretation of Section 2703 That Does Not Conflict With Sovereign Rights and Foreign Law.

The variety of approaches taken by different governments to regulating similar concerns leads to two related foundational principles of law, which together suggest that Section 2703 should be read not to reach data stored outside the United States. The first is that "[a]bsent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090, 2100 (2016); Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1664 (2013); Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247, 255 (2010). The second is that "[a]n act of congress ought never to be construed to violate the law of nations if any other possible construction remains." F. Hoffman-LaRoche Ltd. v. Empagran S.A., 542 U.S. 155, 164 (2004) (quoting Murray v. Schooner Charming Betsy, 6 U.S. (2 Cranch) 64, 118 (1804)) (internal quotation marks omitted).

The Government's position that the focus of Section 2703 is on the disclosure of information, which here would occur within the United States, Pet'r's Br. 13–14, 25–26, ignores that the only communications the Government now seeks are records that are stored in Ireland and that are not in this country. Where the information sought is abroad, and would remain abroad but for the Government's compulsory intervention, the search and seizure is quintessentially extraterritorial.

The Government places far too much emphasis on the fact that it would be Microsoft employees and not government agents physically retrieving the relevant communications from Ireland and transferring them to the United States. From the standpoint of the person whose communications are seized, and from the standpoint of the foreign government whose laws are infringed, this is a distinction without a difference. See Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement to data stored in other jurisdiction, December 5, 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf ("[L]aw enforcement access to a specific computer system to access data stored in another computer system even if the latter is not within the jurisdiction of the requested Party…would breach the principle of territoriality and sovereign jurisdiction of the requested Party[.]"); Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, November 26, 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf ("As a rule, a public authority in a non-EU country should not have unrestricted direct access to the data of individuals processed under EU jurisdiction."); EU Directive 95/46, pmbl. ¶ 10 ("[T]he objective of the national laws on the processing of personal data is to protect fundamental rights and freedoms."); see also United States v. Feffer, 831 F.2d 734, 737 (7th Cir. 1987) ("The government may not do, through a private individual, that which it is otherwise forbidden to do."). The Government proposes no substantive distinction attached to whether the machinery by which records

are transferred from abroad is operated by its agents or by private parties acting at its direction and pursuant to its compulsion. This is not a case in which Microsoft might have extracted data from its server in Ireland for its own purposes, and the Government merely took advantage of that. Cf. Burdeau v. McDowell, 256 U.S. 465, 475 (1921). Rather, the *only* reason for the transfer in this case was Government compulsion, and the search in Ireland was therefore conducted by the Government. See, e.g., Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 614 (1989); Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

Any ambiguity about the "focus" of the relevant legislation in this case should be resolved by reference to the canon of interpretation, commonly known as the "Charming Betsy Doctrine," that "this Court ordinarily construes ambiguous statutes to avoid unreasonable interference with the sovereign authority of other nations." F. Hoffman-La Roche, 542 U.S. at 164. This venerable canon is also highly practical as an expedient to avoid this nation's courts from entering into conflicts with other nations in the absence of direction from the political branches.

Whether or not the requirements of a Section 2703 warrant would conflict with foreign or international law will necessarily depend on the facts and circumstances of a particular case – by way of example, whether there may exist the strict conditions permitting a derogation under article 49 of the GDPR. However, the SCA that Congress enacted leaves no room for such considerations. Section 2703's warrant provision refers to the Federal Rules of Criminal Procedure, which *require* the issuance of a warrant

when probable cause is shown. Fed. R. Cr. P. 41(d)(1) ("[A] magistrate judge . . . must issue the warrant if there is probable cause . . . .").[6] By construing that provision to extend the warrant power to records and communications held abroad, the Government advocates a construct in which no consideration whatsoever need be given to the interests of foreign governments, their laws, or their citizens prior to the issuance of a Section 2703 warrant, provided that the warrant in question can be served on a domestic office or officer.

II. Construing The Warrant In This Case As "Domestic" Would Dramatically Expand The Scope Of Information Held Abroad That Is Subject To Domestic Process And Undermine Internationally Agreed Means of Cooperation.

A. The Government's Interpretation Would Make The United States The Information Clearinghouse Of The World.

Adopting the Government's position that the search and seizure in this case were purely "domestic" would have far-reaching effects beyond the specific facts of

---

[6] This Court has long recognized that American magistrates have no power to authorize searches abroad. See, e.g., United States v. Verdugo-Urquidez, 494 U.S. 259, 274 (1990) (a "warrant . . . from a magistrate in this country" "would be a dead letter outside the United States"); id. at 279 (Stevens, J., concurring) ("I do not believe the Warrant Clause has any application to searches of noncitizens' homes in foreign jurisdictions because American magistrates have no power to authorize such searches.").

this case. Under the Government's proposed rule, so long as the last step in the chain of the search or seizure occurred within the United States, it would be considered "domestic," notwithstanding that the object of the search and the materials to be seized were located abroad.

At its most focused point, the Government's position would permit, without regard to the interests or laws of foreign countries, the use of Section 2703 warrants to obtain information anywhere in the world that can be accessed from within the United States. Such a rule would essentially deputize American telecommunications firms and other service providers to conduct global searches for data on behalf of the U.S. Government. To comply with U.S. warrants, this approach would require – if not in every case, then in many – that U.S. companies violate the laws of the foreign countries in which they operate, and would encourage those abroad to avoid using U.S. companies to conduct business. What is more, the Government's proposed rule would introduce a strong disincentive for investment in the United States by foreign firms not wishing to violate the information security requirements in their home countries.

The Government's interpretation of Section 2703 would also cast doubt on the territorial limitations and comity analyses attaching to other types of compulsory process. If service of a warrant in the United States for records held abroad is a "domestic" search, then it may be argued that other types of searches of materials outside the United States that can be initiated from within the United States are similarly "domestic." For example, service of a subpoena on the U.S. branch

office of a foreign bank does not confer jurisdiction to compel that bank to conduct a world-wide search of accounts held at foreign branches. See Leibovitch v. Islamic Republic of Iran, 852 F.3d 687, 689–90 (7th Cir. 2017); Gucci Am., Inc. v. Weixing Li, 768 F.3d 122, 135 (2d Cir. 2014). The rule arises from the settled law that a foreign bank is not subject to general jurisdiction in the United States and therefore cannot be compelled to answer a subpoena unrelated to its forum-related activities. But under the rule the Government advocates, such questions of jurisdiction would seem irrelevant; so long as the domestic branch has the technical ability to obtain and transfer records from abroad, any search would be purely "domestic" and within the jurisdiction of the issuing court.

The Government's proposed rule could also undermine the Court's jurisprudence with respect to the comity analysis that is to be undertaken in pre-trial discovery proceedings, in consideration of the "special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state." Aérospatiale, 482 U.S. at 546. Aérospatiale recognized that parties subject to personal jurisdiction in the United States may nonetheless confront particular challenges when required pursuant to the Federal Rules of Civil Procedure to transfer data and information from abroad for production in a U.S. court. It recognized the need for "particularly close[]" judicial supervision in cases where "it is necessary to seek evidence abroad." Id. Courts applying Aérospatiale have considered and weighed a variety of factors, including whether "compliance with the request would undermine important interests of the state where the

information is located." See, e.g., In re Air Cargo Shipping Services Antitrust Litig., 278 F.R.D. 51, 52 (E.D.N.Y. 2010) (quoting Restatement (Third) of Foreign Relations Law § 442(1)(c) (1987)); Strauss v. Credit Lyonnais, S.A., 249 F.R.D. 429, 439 (E.D.N.Y. 2008). Were this Court to adopt the Government's position, however, any party who seeks evidence located abroad would be free to argue that, so long as the discovery is ordered by a court in the United States and production is to be made here, it is irrelevant where the material to be produced was stored or originated.

The scope of the Government's proposed rule is also not easily confined to Section 2703 warrants. A rule that disregards the physical location of data – such as the Government now advocates – could readily be applied to any run-of-the-mill warrant issued pursuant to Federal Rule of Criminal Procedure against a company or individual that is not a "provider of electronic communication service" and that therefore falls outside the scope of Section 2703. Federal Courts routinely uphold broad warrants for the search and seizure of electronic communications. See, e.g., United States v. Galpin, 720 F.3d 436, 451 (2d Cir. 2013); United States v. Bansal, 663 F.3d 634, 662 (3d Cir. 2011); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999). Accepting the Government's argument regarding Section 2703 warrants is also to accept that the Government could obtain ordinary warrants to search computers in a home or business in the United States and, through that access, could conduct a global search of records located anywhere in the world – to include data that were never transferred to the United States and that were never contemplated to be

transferred to the United States, without regard to any foreign legal restrictions that might govern such data. This would be an exceptionally broad interpretation of a "domestic" search warrant. The Government's interpretation of Section 2703 does not admit of limiting principles.

Finally, the Government's proposed interpretation of Section 2703 would invite extension to other types of searches that, although initiated within the United States, are in purpose and effect searches of information and correspondence held abroad. For example, this Court has long recognized the relative freedom of border officers to conduct searches of travelers presenting themselves at the border without any requirement for reasonable suspicion. See, e.g., United States v. Ramsey, 431 U.S. 606, 615 (1977). Recently, Circuit Courts have upheld searches in circumstances where customs agents required travelers to boot up their electronic devices in order to allow agents to review their contents. See, e.g., United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 506–07 (4th Cir. 2005). In an age where virtually every device enjoys wireless internet connectivity, the Government's proposed rule would invite customs officers to review not only the contents of the device but any information (including information held abroad) that might be accessed on it. Cf. Riley v. California, 134 S. Ct. 2473, 2491 (2014). After all, such a search – like the search of Microsoft's records – is conducted by law enforcement solely "domestically" at a port of entry.

B. Characterizing Cross-Border Searches and Seizures As "Domestic" Would Dramatically Undermine The International Mutual Legal Assistance Framework.

The Government's position in this case also affords little respect to the extensive network of international agreements that the United States has negotiated with nations around the world governing the disclosure of evidence from their territories to U.S. law enforcement. The Republic of Ireland is on record that, were the Government to make an appropriate request pursuant to the Treaty Between the Government of Ireland and the Government of the United States of America on Mutual Legal Assistance done on January 18, 2001 (the "Irish MLAT"), its government would act expeditiously on that request. Br. of Ireland 3. According to the State Department, mutual legal assistance treaties (MLATs), which establish, inter alia, a process for collecting evidence across borders, are currently in force between the United States and 57 different countries, including virtually all European countries. U.S. Dep't of State, Treaties & Agreements, https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm.

In addition, in June 2016, the United States and the European Union signed a framework agreement for mutual legal assistance that defines procedures and safeguards with respect to the cross-border transfer of data and information from E.U. Members States to the United States. See Agreement between the United States of America and the European Union on the protection of personal information relating to the

prevention, investigation, detection, and prosecution of criminal offences, 2016 O.J. (L 336) 3. Such bilateral and multilateral agreements reflect political agreements by the Executive and Legislative branches with foreign powers regarding the manner in which information is to be collected from their territories for law enforcement purposes. While proceeding through the MLAT process may be less convenient for U.S. law enforcement than simply compelling the disclosure of foreign records through domestic process, the process serves an important function in affording procedural protections *both* to foreign nationals and governments and to the United States and its citizens when the shoe is on the other foot. Available evidence strongly supports the view that MLATs work. See Sergio Carrera et. al, Centre for European Policy Studies, Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights 69 (2015) ("[T]here is no evidence substantiating the argument that [MLATs] [are] ineffective, which would properly justify bypassing its application."). They also ensure that information sought is produced in accordance with the substantive and procedural laws of both the requesting and the requested States.

Despite having negotiated them with dozens of nations, the Government argues here that MLATs are not an "effective alternative to requiring disclosure of emails under the SCA." Pet'r's Br. 44. The Government's objection to the MLAT procedure, however, is largely that it takes time and the outcome is uncertain. Id. at 44–45. Granted that requesting the assistance of another sovereign government to collect evidence within its territory provides less

"certainty" than simply seizing the requested correspondence oneself, any delay and uncertainty reflects the nature of the agreements that both the United States and foreign governments have subscribed to as a precondition to agreeing to provide mutual legal assistance. The very agreement of those mechanisms of cooperation between friendly nations strongly suggests that they did not intend to reserve unto themselves a right for their domestic courts to sanction searches in each other's territory without complying with the agreed treaty terms. See United States v. Rauscher, 119 U.S. 407, 422 (1886) ("No such view of solemn public treaties between the great nations of the earth can be sustained by a tribunal called upon to give judicial construction to them."); see also United States v. Alvarez-Machain, 504 U.S. 655, 678–79 (1992) (Stevens, J., dissenting) ("It is shocking that a party to an extradition treaty might believe that it has secretly reserved the right to make seizures of citizens in the other party's territory.").

III. A Modern Interpretation Of Search and Seizure Law Requires That The Focus Be On The Location Of The Electronic Records Seized.

A century ago, this Court construed a "search or seizure" within the meaning of the Fourth Amendment to relate solely to a physical trespass. See Olmstead v. United States, 277 U.S. 438, 464–65 (1928) ("The amendment itself shows that the search is to be of material things . . . ."). At the time, the Court struggled to comprehend how the concept of a "search" could possibly be "extended and expanded to include telephone wires, reaching to the whole world from the

defendant's house or office," and on that basis held that "wire tapping . . . did not amount to a search or seizure within the meaning of the Fourth Amendment." Id. at 466. With the passage of time and the ubiquity of telecommunications, it became clear that citizens did indeed have a reasonable expectation in the privacy of their telephone conversations, and that the Fourth Amendment's protections did not recede with the advent of technology making possible a search without the need for a physical invasion. Thus, fifty years ago in Katz v. United States, 389 U.S. 347, 352 (1967), the Court rejected Olmstead, holding instead that "the Fourth Amendment protects people – and not simply 'areas' – against unreasonable searches and seizures." Id. at 353. Concurring in the judgment, Justice Harlan stressed that "reasonable expectations of privacy may be defeated by electronic as well as physical invasion." Id. at 362 (Harlan, J., concurring).

The passage of another fifty years and the corresponding advancements in technology require the Court to once again consider what it means to conduct a "search" in an electronic age when virtually all communications exist in electronic form and government agents sitting in one country have the ability to execute searches on the far side of the world. See Olmstead, 277 U.S. at 474 (Brandeis, J., dissenting) ("Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."). That it is the SCA and not the Fourth Amendment that the Court is asked to interpret is reflective of the Congressional view at the time of enactment that a digital age required

greater protection for the individual's electronic communications than the Constitution itself might otherwise have provided. Indeed, Congress was mindful of this Court's jurisprudence under Olmstead and Katz when it enacted the SCA. See S. Rep. No. 99-541, at 2–3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555–57.

The question then is, in this modern era, where does a search and seizure of electronic communications actually take place? The Government urges that the answer is one of practical expediency: if the communications can be accessed from within the United States, even if they are not physically within this country, then the Government can seize them here. In an interconnected world, the Government's argument proves too much. Although it was not true at the time the SCA was enacted, data and correspondence held on remote computers is now often accessible from multiple countries. Nigel Cory, Info. Tech. & Innovation Found., Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? 1, 6 (2017), http://www2.itif.org/2017-cross-border-data-flows.pdf ("[I]n the United States, digitally enabled services grew from $282.1 billion in 2007 to $356.1 billion in 2011. Globally, . . . over the past decade, data flows have increased world GDP by 10.1 percent."). Americans, Europeans, and others conduct businesses around the world from offices in many different countries and often have a technical ability to obtain from those offices records held on remote computer systems around the world. Relying on the same reasoning the Government uses here, it would not be difficult for the Chinese, Russian, or some other government to assert a right to access, through a

branch office in its territory, the worldwide records of such companies, including sensitive or personal data held on servers located in the United States. It is not a far reach to imagine such a government using a "domestic" search of offices within its territory to access trade secrets, personal information, or intellectual property from data sources in the United States.

This Court has observed that courts should "assume that legislators take account of the legitimate sovereign interests of other nations when they write American laws." F-Hoffmann-LaRoche, 542 U.S. at 164. This assumption respects the rights of foreign governments to legislate within their respective realms, as well as the Realpolitik nature of international relations – that actions by this country directed abroad may invite reciprocal actions by foreign governments. If the United States is to adopt a broad view of its jurisdiction to search and seize electronic records located in the territory of foreign sovereign governments contrary to their laws and customs, then Congress and the Executive should say so expressly. In the absence of such a manifest expression, Section 2703 should be interpreted consistent with a traditional understanding of the warrant power. The Second Circuit's conclusion that Congress would not *sub silentio* enact the alternative is sound judgment that "helps the potentially conflicting laws of different nations work together in harmony – a harmony particularly needed in today's highly interdependent commercial world." Id. at 164–65.

CONCLUSION

For the reasons set out above, CCBE respectfully submits that the judgement of the United States Court of Appeals for the Second Circuit should be affirmed.

Respectfully submitted,

Nowell D. Bamberger
Counsel of Record
Brandon N. Adkins
Melissa Gohlke
CLEARY GOTTLIEB STEEN & HAMILTON LLP
2000 Pennsylvania Ave NW
Washington D.C., 20006
T: (202) 974-1500
F: (202) 974-1999
nbamberger@cgsh.com

Attorneys for Amicus Curiae the Council of Bars and Law Societies of Europe

January 18, 2018