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 FOR BUNDESVERBAND DER DEUTSCHEN INDUSTRIE E.V., DEUTSCHER INDUSTRIE- UND HANDELSKAMMERTAG E.V., IBEC CLG, KONFEDERACJA LEWIATAN, AND MOUVEMENT DES ENTERPRISES DE FRANCE AS *AMICI CURIAE* IN SUPPORT OF RESPONDENT

Saad Gul
***Counsel of Record**
Michael E. Slipsky
John M. Durnovich
POYNER SPRUILL LLP
Post Office Box 1801
Raleigh, North Carolina 27602
(919) 783-1170
sgul@poynerspruill.com

Dated January 11, 2018 *Counsel for Amici Curiae*

THE LEX GROUP[DC] ♦ 1825 K Street, N.W. ♦ Suite 103 ♦ Washington, D.C. 20006
(202) 955-0001 ♦ (800) 856-4419 ♦ Fax: (202) 955-0022 ♦ www.thelexgroup.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **Page(s)**

CONSTITUTIONAL PROVISION

FOREIGN CASES

TREATIES & FOREIGN LAW

OTHER AUTHORITIES

INTEREST OF THE AMICI CURIAE

This brief is filed on behalf of Amici Curiae the Federation of German Industries (*Bundesverband der Deutschen Industrie e.V.* or "BDI"), Association of German Chambers of Commerce and Industry (*Deutscher Industrie- und Handelskammertag e.v.* or "DIHK"), Ibec clg ("Ibec"), Polish Confederation Lewiatan (*Konfederacja Lewiatan* or "Lewiatan"), and French Business Federation (*Mouvement des Entreprises de France* or "MEDEF").[1]

Amici are a group of the largest trade organizations from Germany, Ireland, Poland, and France. Together, Amici represent the interests of several million commercial enterprises that span the globe.

BDI is the umbrella organization for all industrial businesses and industry-related service providers in Germany. It represents 36 industrial-sector federations and roughly 100,000 member companies. BDI has offices abroad in Brussels, Beijing, and Washington, D.C.

DIHK is the umbrella organization of Germany's 79 regional Chambers of Commerce and Industry,

---

[1] No counsel for a party authored this brief in whole or in part, and no such counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person, other than Amici Curiae, their members or their counsel, made a monetary contribution that was intended to fund preparing or submitting this brief. This brief is submitted pursuant to blanket consent letters from all parties on file with this Court.

representing more than 3.6 million commercial enterprises in Germany. It also coordinates the German Chamber Network (*Auslandshandel-kammern* or "AHKs") with 130 locations in over 90 countries worldwide, including the United States.

Ibec is the largest organization of Irish businesses, serving as the umbrella group of over 40 industry associations, including Technology Ireland. Ibec's members employ over 70% of the private sector workforce in Ireland.

Lewiatan is the leading national organization of Polish businesses. It is composed of sector and regional associations of private employers as well as individual members. Its membership includes approximately 4,100 companies employing over a million workers in Poland and abroad.

MEDEF is the largest business organization in France, representing more than 173,000 companies. MEDEF's mission is to represent the interests of French companies and develop entrepreneurship in a changing world.

Amici and their members, like all companies operating in the European Union, are ethically and legally obligated to adhere to European privacy laws. Amici and their members also use American technology, products, and services. Amici are concerned that an adverse verdict in this case would (1) force them to choose between violating American or European laws, thereby making it more difficult for them to use American technology, products, and services; and (2) result in data localization and fragmentation, thereby reducing access to

information for both businesses and law enforcement. This brief explains the role of privacy as a fundamental value in European law, as well as how the Justice Department's position creates the potential for conflicting legal requirements and adverse impacts on global business.

SUMMARY OF THE ARGUMENT

This case has global implications that extend far beyond the American technology industry. Endorsing the Justice Department's position would affect virtually every cross-border data transfer, set dangerous international precedent, and have far-reaching consequences for the millions of businesses represented by Amici. The Justice Department's arguments should be rejected for four reasons.

First, data privacy is a fundamental right in Europe. Therefore, not only must European businesses comply with data privacy laws, they must respect European privacy norms by meeting users' expectations that their privacy rights will be appropriately protected. This includes ensuring that cross-border data transfers are subject to adequate and consistent safeguards. The Justice Department's position contravenes these long-standing norms.

Second, the Justice Department's position would create a dilemma for European companies doing business in the United States who receive warrants similar to that at issue here: comply with U.S. warrants and violate European law, or abide by European law and be held in contempt in the United States. This untenable position would throw a wrench into the countless routine business

arrangements that comprise "today's highly interdependent commercial world." *F. Hoffmann-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164–65 (2004).

Third, granting the Justice Department unfettered access to extraterritorial data will encourage other nations' law enforcement agencies to make similar demands. Exposing Amici members to global pressure for data access could jeopardize the data privacy of countless individuals, including European and American citizens.

Fourth, unilateral cross-border data requests wreak havoc on comity standards and the established Mutual Legal Assistance Treaty ("MLAT") framework. If that framework is fractured, every party will suffer. The Justice Department will lose existing means of accessing data. Technology companies operating in the United States will lose business to overseas competitors. European industry will lose the benefits of a seamless global economy. Users will be denied choice in providers and optimal data security.

ARGUMENT

I. Privacy Is a Fundamental European Value Factored Into Business Processes and Expectations.

A. Data Privacy Is a Fundamental Right in Europe.

The United States and Europe have different views of data privacy.[2] Perhaps due to its historical struggles with totalitarianism, Europe is highly sensitive to the disclosure of private data to governmental authorities.[3]

Europeans now enshrine the right to the protection of personal data as a fundamental right.[4]

---

[2] *See* U.S. Dep't of Commerce, E.U.-U.S. Privacy Shield Framework Principles (2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg ("While the United States and the European Union share the goal of enhancing privacy protection, the United States takes a different approach to privacy from that taken by the European Union."); *see also, e.g.*, Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev. 877, 877 (2014) ("U.S. and EU privacy law diverge greatly. . . . In the United States, privacy law focuses on redressing consumer harm and balancing privacy with efficient commercial transactions. In the European Union, privacy is hailed as a fundamental right that can trump other interests.").

[3] *See* Michael W. Heydrich, *A Brave New World: Complying with the European Union Directive on Personal Privacy through the Power of Control*, 25 Brook. J. Int'l L. 407, 417 (1999).

[4] *See* Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 10 ("Everyone has the right to the protection of personal data[.]"); Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950,

The United States itself has expressly acknowledged the European Union's heightened concerns over data privacy by treaty. *See* Agreement on Mutual Legal Assistance, E.U.-U.S., June 23, 2003, T.I.A.S. No. 10-201.1.

To safeguard these rights, Europeans have developed a framework of laws designed to ensure uniform standards for data transfers.[5] This framework does not require that European Union data be stored or processed within Europe.[6] It does, however, require that all European data, regardless of location, be processed in accordance with uniform safeguards. After all, privacy laws applicable exclusively within narrow national frontiers would be meaningless in today's era of frictionless global data transfers. Any actor could evade the strictures of national laws by simply processing data abroad. Therefore, European laws are designed to provide

---

213 U.N.T.S. 222; Treaty on the Functioning of the European Union, art. 16, 2012 O.J. (C 326) 55. Of course, privacy is a universal value. *See, e.g.*, Universal Declaration of Human Rights, G.A. Res. 217 (III) A (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy . . . or correspondence[.]"). Europe, however, places a premium on privacy that others may not.

[5] As early as 1970, Germany began enacting laws designed to enhance data security. *See* Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* 56 (2014) (describing *Hessische Datenschutzgesetz*, translated as the "Data Protection Act of Hessen," as providing as series of safeguards on the use of digital information stored by the government).

[6] Notably, many nations, including Russia and Vietnam, do not permit their data to be stored or processed abroad.

legal certainty and uniform protections for handling data within and beyond the European Union.

For example, nations within the European Economic Area ("EEA"), such as Norway and Iceland, agree to conform to E.U. data processing standards even though they are not E.U. members. *See* 2000 O.J. (L 1) 8. Likewise, all nations within the jurisdiction of the European Court of Human Rights, such as Turkey, are bound by that Court's recognition of the fundamental right to data privacy.[7]

The recently adopted omnibus E.U. data law, the General Data Protection Regulation ("GDPR"),[8] begins by reemphasizing that "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right." GDPR, pmbl. 1, 2016 O.J. (L 119) 1. This embodies Europe's values regarding data processing and privacy. Moreover, the GDPR reflects the European Union's determination that meaningful protection of this fundamental right requires a *uniform* standard for data protection—within member states, within Europe, and within other nations processing E.U. data. To that end, European governments not only constrain data

---

[7] *See* Convention for the Protection of Human Rights and Fundamental Freedoms, *supra* n. 4, art. 32.

[8] The GDPR goes into effect in May 2018. Commission Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter GDPR]. The current law, the E.U. Data Protection Directive, similarly provides strict guidelines for the transfer of data across borders. *See* E.U. Directive 95/46, art. 7, 1995 O.J. (L 281) 40 (restricting processing of personal data, including disclosures to third parties); *id.* at 45–46 (restricting transfers of personal data outside the European Economic Area).

processing within their borders, but also provide safeguards regarding foreign[9] processing of E.U. data.[10] The GDPR recognizes that uniformity of data regulation is critical to fostering simultaneous economic and social progress.[11]

Critically, the European Union's recognition of data privacy as a fundamental right extends to data

---

[9] *See* E.U. Directive 95/46, art. 4, 1995 O.J. (L 281) 39.

[10] For example, the Article 29 Working Party directed that foreign governments' requests for data must be routed through appropriate governmental authorities and should not be sent directly to European companies. *See* Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, at 3, 14/EN WP 227 adopted (Nov. 26, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf. The Article 29 Working Party is the European Union advisory body on Data Protection and Privacy issues. *See* Article 29 Working Party, European Commission, http://ec.europa.eu/newsroom/article29/news-overview.cfm (last visited Jan. 3, 2018).

[11] The Preamble to the GDPR provides:

> The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, *whatever their nationality or residence*, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

GDPR, pmbl. 2, 2016 O.J. (L 119) 1 (emphasis added).

held by a *business*. *See Wieser v. Austria*, 46 Eur. H.R. Rep. 54 (2008) (finding "no reason to distinguish between" the data privacy rights of a natural person and a business).[12] Companies must maintain enormous amounts of confidential information—such as private customer data, legal advice, proprietary technology, and strategic plans. This sensitive content is increasingly maintained in electronic form and routinely transferred across borders.

The GDPR, therefore, regulates the transfer or processing of certain European data regardless of its location. To illustrate, if BNP Paribas is processing data between its New York City office and its French headquarters, that processing will be subject to the GDPR.[13] This breadth is meaningful, particularly in light of the GDPR's enforcement mechanisms.

The GDPR imposes significant penalties for infringing upon data privacy rights. First, it allows for the recovery of private damages for violations. *See*

---

[12] *Wieser* is a decision of the European Court of Human Rights, whose jurisprudence applies to all European Union member states.

[13] Merely viewing protected data remotely—for example, using a computer in the United States to view data stored on a server in Ireland—would trigger GDPR safeguards. This is because the GDPR governs data "processing", which is broadly defined to include "any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[.]" GDPR, 2016 O.J. (L 119) 33.

GDPR, art. 82(1). Second, it authorizes the assessment of administrative fines of up to €20,000,000 or 4% of the "total worldwide annual turnover of the preceding financial year, whichever is higher[.]" GDPR, art. 82(5).

For perspective, consider the 2016 cybersecurity attack on the British retail bank Tesco, where roughly 40,000 bank accounts were compromised. Under current British law, Tesco could have faced a maximum fine of £500,000.[14] Starting in May 2018, fines under the GDPR for a similar breach could exceed £32,000,000.

Given the potential for significant legal, financial, and reputational harm, European companies must be highly vigilant regarding their obligations to safeguard data within the strictures of the GDPR and other privacy laws.

B. Dismissing Privacy Norms Harms European Business.

In light of this background, it is difficult to envision a more flagrant violation of European privacy norms than a foreign law enforcement agency's unilateral demand for personal data that bypasses existing, carefully negotiated, and delicately balanced bilateral procedures.[15] The shock of the

---

[14] Ben Martin & James Titcomb, *Regulators could fine Tesco Bank over cyber attack*, The Telegraph (Nov. 7, 2016), http://www.telegraph.co.uk/business/2016/11/07/tesco-bank-to-freeze-customer-transactions-after-hacking-attack/.

[15] As discussed *infra* at Part II.A., the United States has entered into bilateral treaties that provide a mechanism for

intrusion is magnified by technological advances that readily permit fluid data transfers across the globe. As technology advances, the impact of such intrusions will be compounded.

For example, cloud technology is currently one popular mechanism for data access, storage, processing, and transfer. While its infinite capacity and ubiquitous application are among the cloud's most desirable characteristics, those same characteristics trigger privacy concerns regarding data retention and transfer. As this Court recognized in *Riley v. California*, 134 S. Ct. 2473, 2494–95 (2014), accessing the "immense storage capacity" of an individual's cell phone would permit "[t]he sum of an individual's private life [to be] reconstructed[.]" Yet, a cell phone's storage capacity is infinitesimal relative to the storage capacity of the cloud.[16]

Moreover, Amici members routinely transfer sensitive data—valuable algorithms, proprietary technologies, intellectual property, business plans, employee information, and personal customer data—across borders. These transfers, which are an integral part of doing business in a globally interconnected economy, are possible only because

---

accessing the data at issue in this case. However, the Justice Department chose to bypass that procedure in the instant case.

[16] For context, even a relatively small document like this brief could not have been transmitted as an e-mail attachment when the Electronic Communications Privacy Act was enacted in 1986. Today, unfathomable volumes of data cross countless borders in the blink of an eye.

businesses and consumers alike expect a uniform level of data protection regardless of locale.

But exposing this data to unilateral governmental searches raises concerns over the protection of individuals' fundamental rights. It greatly increases the potential for compromise of sensitive data, such as customers' personal information or employees' human resources data. Exposure of that data, even in the absence of the discloser's malign intent,[17] could spell disaster for competitive businesses—for example, through the leaking of proprietary software information or confidential merger plans. Thus, while modern technological advances like the cloud offer unprecedented conveniences and efficiencies, those same advantages accentuate the risks associated with unfettered access to those data transfers.

For this reason, European businesses are heavily reliant on consistent safeguards to protect both their own data and that of their customers. With respect to data transfers outside of the EEA, those safeguards typically represent either carefully considered "adequacy" determinations or meticulously negotiated bilateral arrangements.

To be clear, respecting these privacy norms and safeguards would not eliminate the Justice

---

[17] The argument that "'the innocent have nothing to fear' is cold comfort and poor constitutional argument. The very principle that imprisons the guilty can be used to seize the innocent." Gene Healy, *Can the President Imprison Anyone, Forever?*, Cato Institute (Apr. 28, 2004), https://www.cato.org/publications/commentary/can-president-imprison-anyone-forever.

Department's access to the data it seeks.[18] It only requires that such requests flow through the appropriate channels: the carefully negotiated MLATs that balance both competing interests.[19]

The Justice Department's position, however, dismisses fundamental Amici concerns along with Amici members' corresponding legal and contractual commitments. This position threatens to upset a delicate balance between European privacy rules and international arrangements.

II. The Justice Department's Position Forces Companies Into the Untenable Position of Deciding Which Legal Obligation to Disregard.

A. Authorizing the Warrant Would Create an Actual Conflict of Laws.

The warrant at issue in this case placed Microsoft Ireland in a dilemma: comply with the warrant and violate both Irish and E.U. law, or comply with those local laws and be held in contempt in the United States.

Microsoft Ireland's compliance with the warrant would directly contravene Irish law. The U.S.-Ireland MLAT explicitly requires that searches be executed in

---

[18] Article 9 of the E.U.-U.S. MLAT provides that a party cannot refuse a lawful request based upon "generic restrictions" on the processing of personal data. *See* Agreement on Mutual Legal Assistance, E.U.-U.S., at 18, June 25, 2003, T.I.A.S. 10-201.1.

[19] *See* discussion *infra* Part IV.C.

accordance with the laws of the requested jurisdiction.[20] In this case, Irish laws require the pre-search authorization of an Irish court after consideration of multiple, enumerated factors.[21] The Irish judge may authorize data extraction if the court is satisfied by information provided under oath that (1) the provider has possession of the materials, (2) the materials are relevant to the investigation of the applicable offense, (3) the materials may be evidence related to the commission of the offense, and (4) there are reasonable grounds to require production.[22]

Here, nothing in the Record indicates that the Justice Department even attempted to obtain judicial authorization under Irish law. Therefore, Microsoft Ireland could not produce the data without violating Irish law.

In addition to violating Irish law, production of the materials outside the MLAT framework would have forced Microsoft Ireland to violate European Union law. *See, e.g.*, GDPR, art. 48 (providing that foreign demands for data are not recognizable in the EU unless domesticated through an MLAT or other agreed-upon framework); E.U. Directive 95/46, art. 7, 1995 O.J. (L 281) 38 (restricting processing of personal data, including disclosures to third parties); *id.* at 45–46 (restricting transfers of personal data

---

[20] Agreement on Mutual Legal Assistance, Ir.-U.S., at 8, Jan. 18, 2001, T.I.A.S. No. 13137.

[21] *See* Criminal Justice Act 2011, § 15 (Act No. 22/2011) (Ir.).

[22] *Id.*

outside the European Economic Area).[23] Violating these laws could result in substantial liability.[24]

Notably, both the European Commission[25] and the Article 29 Working Party[26] have taken issue with the Justice Department's broad position in this case. The Article 29 Working Party cited the present dispute in stressing that E.U. law requires that international agreements like MLATs be followed when law enforcement authorities request data access from E.U. data controllers.[27]

Microsoft Ireland's dilemma—being trapped between two contradictory legal mandates—would

---

[23] Further, many European companies must consider whether compliance with a foreign demand would violate existing contractual commitments (whether business-to-business, business-to-government, or business-to-consumer) governing their treatment of data. This also makes it difficult to adopt and implement coherent compliance policies in the face of conflicting requirements.

[24] *See supra* at 11–12 (discussing civil liability and administrative penalties available under the GDPR).

[25] *See* Věra Jourová, *Answer given by Ms. Jourová on behalf of the Commission E-010602/2014,* European Parliament (Mar. 4, 2015), http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-010602&language=EN.

[26] *See* Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, at 3, 14/EN WP 227 adopted (Nov. 26, 2014) (emphasis omitted).

[27] Statement of the Article 29 Working Party, Data protection and privacy aspects of cross-border access to electronic evidence (Nov. 29, 2017), *available at* http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801.

not be a one-off aberration if the Justice Department prevails in this case. It would not matter whether the data was located in Germany, Ireland, Poland, or France. The United States has entered into MLATs with each of Amici's nations.[28] Each MLAT requires the execution of warrants in accordance with local law.[29] If those MLATs can be ignored at the Justice Department's whim, countless businesses will undoubtedly face the same dilemma in the future.

Thus, any European business in receipt of a similar Justice Department request would face an impossible decision: determining which nation's laws to flout. Such an environment is conducive neither to business nor the orderly collection of data for civil or criminal matters.

---

[28] *See* Agreement on Mutual Legal Assistance, Ger.-U.S., at 11, Oct. 14, 2003, T.I.A.S. No. 09-1018 (providing that the "Requesting State" must provide "information justifying such action under the laws of the Requested State"); Ir.-U.S. MLAT, *supra* n. 20; Agreement on Mutual Legal Assistance, Pol.-U.S., at 8, Jul. 10, 1996, T.I.A.S. No. 99-917.1 ("Requests shall be executed in accordance with the laws of the Requested State except to the extent that this Treaty provides otherwise. However, the method of execution specified in the request shall be followed except insofar as it is prohibited by the laws of the Requested State."); Agreement on Mutual Legal Assistance, Fr.-U.S., at 5, Dec. 10, 1998, T.I.A.S. No. 13110 ("Requests shall be executed in accordance with the provisions of this Treaty and the laws of the Requested State.").

[29] *See id.* Indeed, once the United States ratifies a treaty, its provisions must be respected as the "law of the land." *See* U.S. Const. art. VI, cl. 2. Of course, the United States is limited by the Constitution in the extraterritorial powers it awards itself by treaty. *See Reid v. Covert*, 354 U.S. 1, 16 (1957).

B. The Dilemma Will Drive the Localization and Fragmentation of Global Business.

Actors respond to incentives. Faced with the prospect of inevitable legal landmines, economic theory and history teach that businesses will respond by resorting to localization, thereby fragmenting global commerce. This is not mere speculation.

In one recent example, SWIFT, the Belgian banking consortium, faced significant backlash for complying with a United States administrative subpoena.[30] Because permitting American access to these records violated Belgian and E.U. privacy laws, European regulators subjected SWIFT to lengthy investigations, issued a harsh reprimand, and ultimately directed the banking consortium to cease compliance with the U.S. subpoenas.[31] Much like

---

[30] *See* Royaume de Belgique, Commission de la Protection de la Vie Privee, *Opinion on the Transfer of Personal Data by the CSLR SWIFT by Virtue of UST (OFAC) subpoenas*, Opinion No. 37/2006, at 26 (Sep. 27, 2006) [hereinafter Belgian Opinion] (nonofficial and temporary translation), *available at* https://www.steptoe.com/assets/attachments/2644.pdf (detailing SWIFT's violations of Belgian and E.U. law).

[31] *See* Press Release, Article 29 Working Party, Press Release on the SWIFT Case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 06/EN (Nov. 23, 2006) (detailing SWIFT's violations of Belgian and E.U. law).

Microsoft Ireland, SWIFT found itself trapped between contradictory legal demands.[32]

SWIFT's response to this dilemma is revealing: Even after the United States and the European Union negotiated a political resolution to the dispute, a chastened SWIFT announced that it would reconfigure its computer systems and business processes to ensure that intra-European data was thereafter stored solely in Europe.[33]

SWIFT's decision to shield data through localization, which generated no technical or business dividends, was the rational response to a difficult position. Should the Justice Department prevail in this matter, the SWIFT situation would be reenacted endlessly—that is, the same pressures and incentives would be repeatedly brought to bear on Amici's member businesses. For that reason, the SWIFT episode warns against acceding to the Justice Department's demands.

SWIFT is not the only entity caught between legal crosswinds. In another instance, Brazil imposed fines on Microsoft Brazil and ordered the arrest of a Brazilian Microsoft executive because of the company's refusal to turn over material in

---

[32] *See* Press Release, European Commission, USA to Take Account of EU Data Protection Principles to Process Data Received from Swift, IP/07/968 (June 28, 2007).

[33] Ingrid Melander, *E.U. Approves Deal for U.S. Use of Banking Data in Anti-Terrorism Probes*, Wash. Post, June 28, 2007, at A21.

contravention of U.S. law.[34] Similarly, an Antwerp court fined Skype for its failure to turn over certain communications despite the fact that such turnover would have caused legal issues in Luxembourg, where Skype and its servers were located.[35]

As these examples reveal, the potential for conflict is not merely speculative. The gravity of the Justice Department's position is further underscored by the fact that several E.U. member states have enacted blocking statutes designed to thwart compliance with extra-MLAT demands. Some blocking statutes carry criminal penalties. For example, the French Supreme Court affirmed the conviction of a French attorney for attempting to procure evidence in contravention of a blocking statute. *See* Cour de cassation [Cass.] [supreme court for judicial matters] Paris, Dec. 12, 2007, No. 2007-83228 (Fr.).

Even in the present matter, the underlying decision raised sufficient concerns among European customers to prompt responses from both American technology companies and European regulators. Microsoft Germany, for instance, recently announced plans to offer data storage services where access to

---

[34] *International Conflicts of Law and Their Implications for Cross Border Data Requests by Law Enforcement: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 62 (2016) (statement of Brad Smith, President and Chief Legal Officer, Microsoft Corp.).

[35] Robert-Jan Bartunek, *Skype loses Belgian court appeal after fails to comply with call data order*, Reuters (Nov. 15, 2017), *available at* https://reut.rs/2AMjvUg.

data was ultimately controlled by a German trustee outside United States jurisdiction.[36]

These episodes illustrate the potential pitfalls of the Justice Department's quest for unfettered access to data with any American nexus. The immediate result may be access to data for a single investigation. The ultimate outcome, however, will be data localization and fragmentation of the technology industry—and corresponding difficulties in future investigations.

Users, unsettled by the flux in regulatory regimes, will veer away from American providers. Technological and business processes will be designed to bypass Justice Department jurisdiction and adhere to European privacy norms and regulations. Further demands will spur additional measures that promote no technological or business objective; rather, their sole purpose will be to avoid legal jeopardy.[37] The Justice Department's position, were it to prevail, would incentivize localization, fragmentation, and technological stagnation. It is a textbook example of

---

[36] *See* Orin Kerr, *Microsoft to offer cloud services from servers in Germany hosted by German company*, Volokh Conspiracy (Nov. 12, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/12/microsoft-to-offer-cloud-services-from-servers-in-germany-hosted-by-german-company/?utm_term=.adf480e0194a.

[37] This perpetual flux would directly contradict the GDPR directive that "[l]egal and practical certainty for natural persons, economic operators and public authorities should be enhanced." GDPR, pmbl. 7, 2016 O.J. (L 119) 1.

overvaluing perceived short-term gains while discounting long-term losses.

III. Endorsing Unilateral Access to Extraterritorial Data Will Result in a Hobbesian Framework of All Against All.

A. Principles of Comity and the Presumption Against Extra-territoriality Weigh Against the Justice Department.

Conflicts of law are not new. To minimize inevitable friction, both United States law and customary international law carefully delineate what is permissible in the context of cross-border investigations.

It is axiomatic that a nation's sovereignty over its own territory necessarily limits other nations' actions on that same territory. *See, e.g.*, *The Schooner Exch. v. McFaddon*, 11 U.S. (7 Cranch) 116 (1812); *see also* Restatement (Third) of Foreign Relations Law of the United States § 432(2) (Am. Law Inst. 1987). Customary international law likewise bars nations from conducting investigations on foreign soil without the host's consent.[38] This Court has long held that it will not construe a statute to violate the law of nations if an alternative construction is available. *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64 (1804).

These principles have given rise to the presumption against extraterritorial application: If a

---

[38] *See* Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. Chi. Legal F. 35, 44 (2001).

statute gives no clear indication of an extraterritorial application, it has none. *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010). This canon acknowledges "that United States law governs domestically but does not rule the world . . . ." *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 454 (2007). Without doubt, this presumption averts "unintended clashes between our laws and those of other nations which could result in international discord." *Kiobel v. Royal Dutch Petro. Co.*, 133 S. Ct. 1659, 1664 (2013) (quoting *E.E.O.C. v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991)).

Yet, the Justice Department argues that the presumption against extraterritorial application is inapplicable here because of Microsoft Ireland's connection to the United States. But any competent law enforcement agency would be able to identify an analogous connection in virtually any conceivable scenario.

Consider the case of a German tourist staying at a Paris Marriott. Could the Justice Department obtain a warrant to search a suitcase in the tourist's Paris hotel room merely by arguing that the hotel is "controlled" from its corporate headquarters in Bethesda, Maryland? Would the German tourist anticipate placing her belongings under American jurisdiction simply by choosing to stay in an American-owned hotel in France? Under settled U.S. and international law, the answer to both questions must be "no."

This scenario highlights the fundamental flaw in the Justice Department's logic: there is no limiting principle to distinguish an American company's

possession or control over overseas *data* from such possession or control over more traditional, *tangible* forms of property.[39]

As this Court has recognized, "the presumption against extraterritorial application would be a craven watchdog indeed if it retreated to its kennel whenever some domestic activity is involved in the case." *Morrison*, 561 U.S. at 266. In a world where data and intangible assets are only increasing in importance, there is simply no reason to undermine this presumption for the convenience of the Justice Department in a single case. To the contrary, the growing importance of data weighs in favor of adhering to well-settled legal principles.

B. The Justice Department's Position Undercuts Investigatory Norms.

By disregarding fundamental principles of international cooperation, the Justice Department's position undermines both E.U. privacy laws and U.S. comity principles.[40] It also discourages international

---

[39] To further illustrate the point, federal courts handling international discovery currently balance various factors, including comity with foreign nations, MLATs, and the Hague Convention in determining whether to order discovery from abroad. If the Justice Department's position is accepted, then the existing process would no longer matter. The physical location of the data in a different country would be irrelevant. The only question will be: Can the data can be accessed from the United States? If so, nothing else matters.

[40] *See, e.g.*, *Volkswagen, A.G. v. Valdez*, 909 S.W.2d 900, 901–03 (Tex. 1995) (granting Volkswagen's writ of mandamus because the trial court did not consider the competing interests

cooperation and invites foreign regulatory countermeasures.

The Justice Department itself has previously warned, "[C]onsider how we would react to a foreign country's 'search' of our defense-related computer systems based upon a warrant from that country's courts."[41] Yet, that is precisely the kind of conduct advocated by the Justice Department in this case. After all, if the United States elects to forego carefully negotiated treaty frameworks for the convenience of direct and unilateral access to data, then it is ill-positioned to protest when foreign nations use the same tactics to obtain the data of American businesses or citizens.

These scenarios are not hypothetical. Mere days before the Second Circuit arguments in this case, Chinese authorities seized Microsoft servers in China and demanded passwords that would enable them to seek information stored in the United States.[42]

---

of Germany's Federal Data Protection Act when it compelled discovery of foreign information in accordance with Texas law).

[41] U.S. Dep't of Justice, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet 21–22 (2000), *available at* https://www.hsdl.org/?view&did=3029.

[42] *See* Neil Gough, et al., *China's Energetic Enforcement of Antitrust Rules Alarms Foreign Firms*, N.Y. Times (Aug. 10, 2014), https://www.nytimes.com/2014/08/11/business/international/china8217s-energetic-enforcement-of-antitrust-rules-alarms-foreign-firms.html; *see also* Paul Mozur & Nick Wingfield, *Microsoft Faces New Scrutiny in China*, N.Y. Times (Jan. 5, 2016), https://www.nytimes.com/2016/01/06/business/international/microsoft-china-antitrust-inquiry.html.

The concerns are compounded by the prospect of foreign demands for questionable purposes, which would create enormous vulnerabilities for international trade. What happens if the Chinese government seeks to compel Microsoft to turn over data belonging to the Polish competitor of one of China's state-owned companies? What happens if the Russian government demands the data of a French company negotiating a large corporate transaction with a Russian enterprise with close ties to the Kremlin?

In sum, a Justice Department victory will erode data protection norms and weaken the ability of American companies to resist similar demands levied by foreign powers.

IV. Ultimately, the Justice Department's Position Would Adversely Affect All Interests.

A. The Justice Department's Position Would Harm the American Technology Industry and the European Companies that Rely Upon It.

The United States remains the dominant global leader in computing.[43] However, permitting the Justice Department's unrestrained data collection would have severe repercussions on the United States

---

[43] *See* The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 100 (Feb. 23, 2012), *available at* http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=jpc.

technology industry. This is because users, resistant to being caught between competing regimes or losing control of their data, will veer away from American vendors.[44] Instead, they will turn inward and rely on "localized" networks immune from these conflicting obligations.[45] This digital protectionism would prove costly to providers and users alike.

To be sure, government policies on data transfers have significant economic impacts on the private sector. In the wake of Edward Snowden's revelations regarding National Security Agency surveillance, for example, American technology companies found themselves under an unprecedented cloud of

---

[44] Many European companies already approach cloud computing with caution. For example, less than 10% of Polish businesses purchased cloud services in 2016. *See* Central Statistical Office of Poland, Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2012-2016 [Information Society in Poland: Results of statistical surveys in the years 2012–2016] 70 (Dec. 2016), *available at* http://stat.gov.pl/download/gfx/portalinformacyjny/en/defaultaktualnosci/3417/1/3/1/information_society_in_poland_2012-2016.pdf. For those businesses that chose not to purchase cloud services, more than 70% reported doing so based upon concerns over the location and security of their data. *See id.* at 71. Endorsing the Justice Department's views would only amplify those concerns.

[45] *See* International Trade Administration, A Market Assessment Tool for U.S. Exporters 9 (Apr. 2016), http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf ("Following some surveillance disclosures in recent years, trust-related issues have increasingly caused hesitations amongst those considering purchasing of cloud services from U.S. vendors, especially those vendors who do not store data locally. Thus, some U.S. companies operating in foreign markets are storing data in-country due to strict data policies.").

suspicion.[46] While the precise magnitude of the ensuing business losses is disputed, there is no doubt that a key American industry suffered a significant blow.[47]

The repercussions were not limited to decreased revenue for stigmatized companies. Public pressure abroad forced governments to respond, prompting blocking measures, complicating trade negotiations, imperiling the Safe Harbor data transfer regime, and driving efforts in the European Parliament to kill the proposed E.U. data protection regulation.[48]

The issues at stake in this case are neither technical nor narrow, because the Justice Department offers no limiting principles. Instead, the Justice Department's position seeks unrestricted access to internal data transfers of foreign companies. For example, could the Justice Department seize

---

[46] *See* Joris van Hoboken & Ira S. Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 Me. L. Rev. 487, 494 (2014) ("The revelations have also dealt a significant blow to the reputation of major Internet industry players, which have seen their brands implicated in the reporting about NSA spying programs.").

[47] For example, the German government responded by cancelling a major contract with Verizon. *See id.* at 495; *see also* Anton Troianovski & Danny Yadron, *German Government Ends Verizon Contract*, Wall St. J. (June 26, 2014), https://www.wsj.com/articles/german-government-ends-verizon-contract-1403802226 (describing German government's cancellation of contract with Verizon following revelations about U.S. surveillance programs).

[48] *See* Hoboken & Rubinstein, *supra* n. 46, at 493–94.

sensitive human-resources data stored in BMW's Munich headquarters, simply because that data might be accessible by a human-resources executive at a BMW plant in Spartanburg, South Carolina? Nothing about the Justice Department's position suggests that this would be out of bounds.

If that position is accepted, Europeans would view it as an egregious violation of their values and sovereignty. Amici members would have to factor in additional risks in dealing with their American counterparts. Businesses operating in the United States would find themselves at a competitive disadvantage globally. At a time when state governments actively court foreign investments such as BMW plants in South Carolina, Volvo facilities in North Carolina, and Mercedes manufacturing in Alabama, this needless antagonism seems inexplicable at best, and counterproductive at worst.

B. Allowing the Warrant Would Undermine Legitimate Law Enforcement Needs.

By encouraging digital protectionism and legal uncertainty, the Department of Justice is undercutting its own objectives in three ways.

First, the Justice Department's insistence on unilateral unfettered data access erodes existing mechanisms such as MLATs. This overreaching would diminish cooperation among law enforcement

agencies, as other nations will be compelled to stonewall overly aggressive data collection tactics.[49]

Second, the Justice Department's position would increase uncertainty for law enforcement investigations. Procedures and training depend on an understanding of how companies will respond to requests for legal assistance. If the current MLAT framework is ignored in favor of a patchwork of conflicting legal requirements, responses will be similarly inconsistent.

Lastly, wary users will be more likely to steer data to uncooperative nations. This means the United States would find less, not more, data available in future investigations. In essence, the Justice Department would punish America's friends and reward recalcitrant nations. Again, actors respond to incentives, and the Justice Department's position creates all the wrong ones.

---

[49] Law enforcement cooperation between closely allied neighbors also suffers in the presence of extra-territorial action. For example, even the United States and Canada have communicated their distaste for the other's unilateral action on their territory. *See, e.g.*, *United States v. Licht*, 2002 BCSC 1151 (Can.); *United States v. Orphanou* (2004), 19 C.R. 6th 291 (Can. Ont. Sup. Ct. J.); John Nicol & Dave Seglins, *L.A. cocaine bust threatens Canada-U.S. police relations*, CBC News Canada (Feb. 12, 2013), http://www.cbc.ca/news/canada/l-a-cocaine-bust-threatens-canada-u-s-police-relations-1.1374897.

C. Existing MLATs Provide the Appropriate Mechanism for Balancing Competing Interests.

The MLAT processes represent carefully negotiated arrangements that reconcile the principle concerns of key stakeholders. They have the approval of the political branches, and Amici's members conduct their businesses under the understanding that the applicable MLAT guidelines will be respected. Indeed, MLATs are manifestations of fundamental principles of state sovereignty—that one sovereign nation's officials will not exercise their jurisdiction in a foreign state without consent. *See* Restatement of Foreign Relations § 432(2); *see also supra* n. 28 (discussing MLATs with Germany, Ireland, Poland, and France).[50]

No system will be perfect. But the Justice Department's concerns regarding the efficacy of MLAT procedures overlook noteworthy MLAT successes. For example, in response to the March 2017 terror attacks in London, Microsoft provided law enforcement with requested information less than 30

---

[50] In addition, MLATs can be modified to meet changing needs of the parties. In fact, Congress recently passed laws designed to improve existing MLATs. *See, e.g.*, 155 Cong. Rec. 15598 (2009) ("Setting a high standard of responsiveness will allow the United States to urge that foreign authorities respond to our requests for evidence with comparable speed."); *see also* The Law Enforcement Access to Data Stored Abroad Act, S. 512 114th Cong. (as referred to S. Comm. on the Judiciary, Feb. 12, 2015) (bipartisan bill that would ensure non-U.S. personal data located abroad is accessed only through the MLAT process).

minutes after receiving an order.[51] The FBI also relied on an MLAT in arresting Ross Ulbricht and shutting down the Silk Road network.[52] Similarly, in *United States v. Getto*, 729 F.3d 221 (2d Cir. 2013), evidence from the Israeli national police obtained through the MLAT process helped convict a defendant in a multi-million-dollar wire fraud scheme.

In an increasingly interconnected world, it serves the interest of all parties concerned—the United States, the Justice Department, European businesses, the American technology industry, and consumers—to strengthen and develop, not undermine and undercut, the MLAT process.[53] Its backdoor destruction by yielding to the Justice Department's desire for a quick fix in a single case will prove to be damaging to all interests in the long term.

---

[51] *See* Press Release, Responding to lawful requests, Microsoft News Centre UK (March 27, 2017), *available at* https://news.microsoft.com/en-gb/2017/03/27/responding-lawful-requests/. The E.U.-U.S. MLAT also includes express provisions for expediting requests. *See* E.U.-U.S. MLAT, *supra* n. 28, at 15.

[52] Donna L. Leger, *How FBI brought down cyber-underworld site Silk Road*, USA Today (May 15, 2014), https://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/.

[53] It is telling that Microsoft was supported at the Second Circuit by amici comprising 29 technology and media companies, 23 trade associations and advocacy groups, 35 leading computer scientists, and the government of Ireland. *See* Docket, *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

CONCLUSION

The problem of contradictory legal mandates governing the production of information is an old one. However, technological and political progress and integration has lent it a new urgency.

To this end, various sovereigns have devoted considerable time and resources to create cross-border legal frameworks that reconcile and accommodate divergent local notions of data privacy. The Justice Department seeks to tear apart this carefully constructed and fragile set of international understandings.

In doing so, the Justice Department is undermining the expectation that governmental agencies will abide by agreed-upon methods of obtaining information. The end result could be true Balkanization—a complete absence of bridges between differing privacy regimes.

Ultimately, a Justice Department victory would be disastrous: (1) Amici members would find themselves ensnared between competing laws; (2) users would steer data to non-U.S. providers, actually undermining U.S. law enforcement efforts; and (3) modern commercial ties, which depend on integrated technology and the ability to transfer data across borders, would be undercut. None of these developments are in the interest of the United States, Europe, or their commercial or law enforcement efforts. At best, it would be a short-term "win" for the Justice Department, and a long-term defeat for everyone—including the Justice Department.

For all of these reasons, Amici respectfully request that the Second Circuit's decision be affirmed.

Respectfully submitted,

/s/ Saad Gul
SAAD GUL
Counsel of Record
MICHAEL E. SLIPSKY
JOHN M. DURNOVICH
POYNER SPRUILL LLP
P.O. Box 1801
Raleigh, NC 27602
sgul@poynerspruill.com
(919) 783-1170
Counsel for Amici Curiae Bundesverband der Deutschen Industrie e.V., Deutscher Industrie- und Handelskammertag e.V., Ibec clg, Konfederacja Lewiatan, and Mouvement des Enterprises de France