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 AMICUS CURIAE OF U.N. SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY JOSEPH CANNATACI IN SUPPORT OF NEITHER PARTY

VIVEK KRISHNAMURTHY*
MASON KORTZ
CYBERLAW CLINIC, HARVARD LAW SCHOOL
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-384-9125
vkrishnamurthy@law.harvard.edu
**Counsel of Record for Amicus* (*Admission Pending*)

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

TABLE OF AUTHORITIES – Continued

IDENTITY AND INTEREST OF AMICUS CURIAE

Professor Joseph A. Cannataci is the United Nations Special Rapporteur on the Right to Privacy ("Special Rapporteur").[1] Professor Cannataci's three-year Mandate from the United Nations Human Rights Council[2] is to gather information on international and national developments in relation to the right to privacy, to make recommendations to ensure the promotion and protection of this important right, and to report on alleged violations of the right to privacy – including in connection with challenges arising from new technologies. *Id.*

The Special Rapporteur's interest in this case stems from its potential to impact the privacy interests of billions of people around the world who use cloud computing services every day to store their most sensitive data. This brief sets out the views of the Special Rapporteur on the importance of paying due regard to the international conception of the right to privacy and to the differing domestic instantiations of this right in

---

[1] This amicus curiae brief is respectfully submitted pursuant to Supreme Court Rule 37 in support of neither party. Pursuant to Rule 37.6, counsel for the amicus states that no counsel for a party authored this brief in whole or in part, and that no person or entity other than the amicus or his counsel made a monetary contribution to the preparation or submission of this brief. Petitioner and Respondent have filed letters of consent with the Clerk of the Court.

[2] Professor Cannataci's mandate is established by and detailed in Human Rights Council Res. 28/16, U.N. Doc. A/HRC/RES/28/16, at 3-4 (Apr. 1, 2015).

deciding the difficult jurisdictional issues confronting the Court in this case. The Special Rapporteur takes no side in the present litigation, and therefore submits this as a Brief Supporting Neither Party.

SUMMARY OF ARGUMENT

The question before the Court in this case is whether, in view of the other facts of this case, a search warrant issued pursuant to the Stored Communications Act, 18 U.S.C. § 2703, can compel the respondent to produce to the U.S. government the contents of an email account that all parties agree is stored on the respondent's servers in Ireland. This is a question of domestic law on which the Special Rapporteur expresses no view.

This Court's answer to this question, however, will undoubtedly bear on the privacy interests of users around the world who entrust their sensitive data to the respondent's and other similar cloud computing services. This is because this Court cannot decide this case without implicitly endorsing (or rejecting) a theory of what jurisdictional contacts are adequate (or not) for one sovereign to seize certain data unilaterally, when there are other sovereigns with very significant jurisdictional interests in this data. This may pose a danger to the protection of the right to privacy in cyberspace, especially if non-rights-respecting states should adopt for their own ends any jurisdictional theory that this Court espouses. The decision will also

directly impact the universality of the fundamental human right to privacy in a context where new technologies have radically changed the way that this right is experienced worldwide, and at a time when sovereign states are still coming to grips with this new reality.

The Special Rapporteur is an active participant in efforts to resolve the complex jurisdictional questions that confront this Court through international diplomatic processes. He therefore respectfully urges this Court to exercise judicial restraint by deciding the questions presented in this case in the narrowest possible manner. Doing so will incentivize the political branches of the U.S. government to continue their engagement in these international efforts. This is in the interest of all those who care about privacy in the United States and around the world, for only diplomatic processes of negotiation can accommodate and balance all of the very significant interests that are in tension in this case.

ARGUMENT

I. Recent technological developments have reshaped our social and legal understandings of privacy.

The legal dimensions of this case cannot be adequately understood without first identifying how technological change has impacted our conceptualization of what privacy is and why it matters. In *Riley v.*

California, 134 S. Ct. 2473, 2488-91 (2014), this Court recognized how technologies such as the cell phone have fundamentally changed our lives in the two centuries since the framing of the Bill of Rights. As Chief Justice Roberts rightly recognized:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.

Id. at 2495-96. In deciding that the warrant exception for searches incident to arrest did not apply to cell phones, the Court took into account both the technological features of these devices and the social reality of their use. This Court recognized that the term "'cell phone' is itself a misleading shorthand," *id*. at 2489, in view of their myriad functions and their capacity to "stor[e] and access[ ]a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form," *id.* at 2496 (Alito, J., concurring). The Court further recognized that "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at 2484. All of these factors led this Court to the conclusion that a "mechanical application" of the search incident to arrest exception would not respect the realities of that day. *Id.* at 2484.

The instant case calls on the Court to consider particularly challenging legal questions regarding a problem it recognized in *Riley*: searches of those great stores of personal data "in the cloud." *Id.* at 2491. As this Court previously noted, the privacy interests implicated by cloud storage "dwarf" those at issue in many physical searches. *Id.* This case brings those interests even more sharply into view – here, the government's access to remote data is not just a possibility, but the heart of the issue.

In our brave new era of cloud computing, even the savviest of users may not know whether their information is stored on their device or in the cloud. Modern cloud storage services such as Apple's iCloud, Google's Drive, Microsoft's OneDrive, or Dropbox and Box's eponymous services seamlessly and invisibly move a user's files to remote servers and back again, without any direction from the user. These servers physically exist in vast data centers that are intentionally distributed far and wide – including across international borders – to guard against catastrophic data loss. Therefore, what the individual user of a cloud service experiences as their account – a single, unified, and private place in cyberspace – does not relate back to any single location in physical space, since the contents of every single cloud account exist in two or more places at once. Nonetheless, the billions of people around the world who store their most sensitive information in these virtual places expect them to be safe against governmental intrusion except with due process of law.

The key question in this case is "whose law?" Since any data stored in the cloud is held in at least two places at once, it will frequently be the case that at least two different sovereigns can lay claim to *in rem* jurisdiction over that data. To further complicate matters, there are *in personam* grounds on which the same or other sovereigns might claim jurisdiction over the same data, such as the countries of residency or nationality of the account holder, or the home country of the cloud storage provider.

The potential for conflicts of law regarding access to data stored in the cloud has long been recognized. Governments have been meeting under the auspices of the United Nations to determine how the law of jurisdiction ought to be applied in cyberspace. Since 2012, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereinafter "GGE") has been tasked by the U.N. Secretary-General with establishing norms of appropriate state behavior in cyberspace. *See* G.A. Res. 66/24, ¶ 4 (Dec. 13, 2011). In 2013, the GGE unanimously recognized that international law applies online as it does offline. Report of the GGE, transmitted by the Secretary-General, ¶¶ 20, 21, U.N. Doc. A/68/98 (June 24, 2013). Since 2014 the U.N. Human Rights Council has repeatedly recognized that fundamental human rights should be enjoyed online as they are offline, though the question of how to operationalize this high-level statement of principle remains open. *See*, *e.g.*, Human Rights Council Res. 68/167, U.N. Doc. A/RES/68/167, at 2 (Jan. 21, 2014) (affirming that the right to privacy applies online);

Human Rights Council Res. 34/L.7/Rev.1, U.N. Doc. A/HRC/34/L.7/Rev.1, at 4-5 (Mar. 22, 2017) (expanding recommendations to member states for protecting online privacy).

It is into these uncharted waters that this Court now sails; an area where the navigational aid that only international law can provide remains to be developed. Were this a dispute about jurisdiction over goods on a ship rather than data on a server, this Court could look to the Law of the Sea for guidance. That this case arises in cyberspace rather than maritime space makes it challenging indeed for this Court to plot a true course as it decides this case.

The Special Rapporteur respectfully submits that it is of the utmost importance for this Court to recognize the universality of the right to privacy, as first recognized in New York on December 10, 1948 when the U.N. General Assembly adopted the Universal Declaration of Human Rights. Privacy is a right to which each of us is entitled by virtue of our humanity. In today's technological world, the privacy of the billions who spend most of their waking hours in cyberspace should not depend on the place where they live, the passport in their pocket, the color of their skin, the gender of their romantic partners, or the accident of where their data happens to be located on a particular day. The fact that a diary is stored as a collection of files in the cloud rather than a sheaf of papers bound into a book should not give governments the right to access the former in ways that are materially different from the latter.

On numerous occasions throughout the term of his mandate, the Special Rapporteur has pointed out how the lacunae in the law of jurisdiction pose problems for the protection of privacy in cyberspace. In his most recent annual report to the U.N. General Assembly, the Special Rapporteur indicated that

> [o]ne of the most meaningful things for the Special Rapporteur's mandate would be to recommend to the Human Rights Council that it supports the discussion and adoption within the United Nations of a legal instrument to achieve two main purposes:
>
> > i. provide the Member States with a set of principles and model provisions that could be integrated into their national legislation embodying and enforcing the highest principles of human rights law and especially privacy when it comes to surveillance; [and]
> >
> > ii. provide Member States with a number of options to be considered to help plug the gaps and fill the vacuum in international law and particularly those relating to privacy and surveillance in cyberspace.

Joseph A. Cannataci, *Report of the Special Rapporteur on the Right to Privacy*, ¶ 5, U.N. Doc. A/72/43103 (Oct. 19, 2017).

As will be explained in more detail below, the Special Rapporteur is leading efforts which have now distilled two years' worth of stakeholder contributions

from around the world into a new draft legal instrument to be presented to the U.N. Human Rights Council for its consideration in March 2018. The level of agreement that currently underpins this draft legal instrument is evidence that a negotiated solution to the jurisdictional problems underlying this case can be reached, though further rounds of intense discussions and negotiations will be needed to achieve that goal.

The technological realities of 2017 require recognition of the necessity of protecting privacy in cyberspace through the development of international law, such as through a multilateral international legal instrument, rather than by unilateral action by any one single nation.

II. Privacy is a universal human right that international law protects to a high minimum standard, with some nations offering even stronger protections under their domestic law.

Privacy is a fundamental human right protected by international and domestic law. International law has expressly recognized and protected the right to privacy since the adoption of the Universal Declaration of Human Rights ("UDHR") in 1948. *See* G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III), art. 12 (Dec. 10, 1948). For its part, the United States should be justifiably proud that its Bill of Rights contains some of the earliest protections of the right to privacy anywhere in the world.

The importance of the right to privacy has steadily increased over time, in view of recent legal, social, and technological developments. The Special Rapporteur has suggested that the right to privacy should be understood as part of a triad: together with freedom of expression and the right to information, it constitutes the basis for the development of personality. Joseph A. Cannataci, *Report of the Special Rapporteur on the Right to Privacy*, ¶ 24, U.N. Doc. A/HRC/31/64 (Nov. 24, 2016). Correspondingly, the right to privacy is at the core of individual freedom and human dignity. Earlier this year, the international community recognized the importance of privacy to the enjoyment of other human rights when the U.N. Human Rights Council adopted a resolution on the Right to Privacy in the Digital Age. U.N. Doc. A/HRC/34/L.7/Rev.1, *supra* p. 5, at 4.

Domestic laws that implicate privacy must comply with standards set by international law. Subject to that limitation, sovereign nations enjoy significant latitude in implementing domestic privacy protections. There are many approaches a sovereign could take to safeguard privacy that meet or exceed the minimum standards established by international law, all of which should be accorded significant respect by other nations.

A. International human rights law recognizes and protects the right to privacy.

In the seven decades since the adoption of the UDHR, the right to privacy has been enshrined into

many foundational human rights instruments, both international and regional. *See* Elizabeth B. Ludwin King, *A Conflict of Interests: Privacy, Truth, and Compulsory DNA Testing for Argentina's Children of the Disappeared*, 44 Cornell Int'l L. J. 535, 549-50 (2011) (collecting examples). These include, among others, the International Covenant on Civil and Political Rights ("ICCPR"), art. 17, Dec. 16, 1966, 999 U.N.T.S. 171, the Convention on the Rights of the Child, art. 16, Nov. 20, 1989, 1577 U.N.T.S. 3, the American Convention on Human Rights, art. 11, Nov. 22, 1969, 1144 U.N.T.S. 123, the European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 222, and the Cairo Declaration on Human Rights in Islam, Organization of the Islamic Conference, art. 18, OIC Res. No. 49 19-P (Aug. 5, 1990).

The United States demonstrated its dedication to privacy as an international human right in 1992, when the Senate ratified the ICCPR, making the obligations contained therein binding upon the United States government.[3] The rights and guarantees enshrined in the ICCPR comport with "the United States' long tradition of protecting individual human rights." *See* Michael H. Posner & Peter J. Spiro, *Adding Teeth to United States*

[3] At the time of its ratification of the ICCPR, the United States issued a Declaration stating that "the provisions of articles 1 through 2 of the Covenant are not self-executing." 138 Cong. Rec. 8070-71 (1992). However, it also expressed its understanding that the treaty "shall be implemented by the Federal Government to the extent that it exercises legislative and judicial jurisdiction over the matters covered" by the treaty, "and otherwise by the state and local governments." *Id.*

Ratification of the Covenant on Civil and Political Rights: The International Human Rights Conformity Act of 1993, 42 DePaul L. Rev. 1209, 1211 (1993). In fact, the United States was a key player in developing the ICCPR, and consequently the protected rights are "almost entirely consistent with the U.S. Constitution." *Id.*

More recently, the United States has recognized the universality of the right to privacy by enacting special privacy regimes for non-residents. For example, the Judicial Redress Act of 2015 enables some foreign citizens to bring suit against the U.S. government for disclosure of personal information, just as U.S. citizens may under the Privacy Act of 1974. *See* 5 U.S.C. § 552a note (2012). Likewise, Presidential Policy Directive 28 places prudential restraints on the United States' collection of signals intelligence to protect the privacy of all persons, "regardless of their nationality or wherever they might reside, [because] all persons have legitimate privacy interests in the handling of their personal information." Exec. Office of the President, Policy Directive PPD-28, Signals Intelligence Activities (2014). These efforts are all consistent with a strong respect for the universal right to privacy established by international law.

B. Sovereign nations have a duty to implement privacy protections and, in so doing, may afford stronger protections than the floor established by international human rights law.

Sovereignty is the "basic constitutional doctrine of the law of nations." James R. Crawford, *Brownlie's Principles of Public International Law* 447 (8th ed. 2012). The concept "implies a state's lawful control over its territory generally to the exclusion of other states, authority to govern in that territory, and authority to apply law there." Restatement (Third) of Foreign Relations Law § 206 cmt. b (Am. Law Inst. 1987). As a necessary corollary to these powers, "[e]very sovereign state is bound to respect the independence of every other sovereign state." *Underhill v. Hernandez*, 168 U.S. 250, 252 (1897). Sovereign independence is limited, however, by international humanitarian and human rights law. All nations, for example, are bound by *jus cogens* norms "'from which no derogation is permitted.'" *Comm. of U.S. Citizens Living in Nicaragua v. Reagan*, 859 F.2d 929, 940 (D.C. Cir. 1988) (quoting Vienna Convention on the Law of Treaties, May 23, 1969, art. 53, 155 U.N.T.S. 331). Nations may also consent to be bound by additional limitations by entering into treaties with one another. Vienna Convention, art. 2.

International sources of human rights establish a floor beneath which a state may not treat any person by virtue of their humanity. However, it is the domestic implementation of those principles that provide

specific safeguards for individual rights. In view of their sovereignty, states enjoy a margin of appreciation in how they protect human rights within their territorial borders. *See generally* Andreas Fóllesdal, *Subsidiarity and International Human-Rights Courts: Respecting Self-Governance and Protecting Human Rights-or Neither?*, 79 Law & Contemp. Probs. 147, 147-48 (2016). Above the floor set by international law, the sky is the limit as to what protections a sovereign can grant individuals subject to its jurisdiction. This is as true of privacy as it is for any other fundamental right.

The United States, of course, articulated the need for strong constitutional privacy protections before international human rights law had even been theorized. The Fourth Amendment's probable cause standard is widely viewed as among the most privacy-protective standards in the world for authorizing a search. This Court has described "the security of one's privacy against arbitrary intrusion by the police" as being "basic to a free society." *See Wolf v. Colorado*, 338 U.S. 25, 27 (1949), *overruled on other grounds by Mapp v. Ohio*, 367 U.S. 643 (1961). Even outside of government searches, constitutional protections for personal privacy have become a key element of this Court's jurisprudence, dating back to the seminal article by Warren and Brandeis and appearing in landmark opinions ever since. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890); *Roe v. Wade*, 410 U.S. 113, 153 (1973). Numerous other

countries have likewise adopted strong domestic constitutional protections for the right to privacy.[4]

Domestic constitutions and international human rights instruments both tend to articulate the right to privacy at a high level of generalization. It is the role of ordinary domestic law to operationalize those general principles into specific protections. Some such protections are derived from judicial interpretation of overarching principles. *See Riley*, 134 S. Ct. at 2488-91; *Lawrence v. Texas*, 539 U.S. 558, 579 (2003) ("As the Constitution endures, persons in every generation can invoke its principles in their own search for greater freedom."). Others are created via the legislative process. For example, in the United States, the Privacy Act of 1974, 5 U.S.C. § 552a, protects the privacy of personal data collected by the government; the Family Educational Acts and Privacy Act of 1974, 20 U.S.C. § 1232g, protects the privacy of educational records; and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, protects the privacy of medical records.

The incorporation of general principles of privacy into specific legislation and case law in the United States illustrates well the right of a sovereign to

---

[4] *See*, *e.g.*, Grundgesetz arts. 10 & 13, *official translation at* https://www.btg-bestellservice.de/pdf/80201000.pdf (Ger.); Basic Law: Human Dignity and Liberty, 5752-1992, S.H. No. 1391, *official translation at* http://www.mfa.gov.il/MFA/MFA-Archive/1992/Pages/Basic%20Law-%20Human%20Dignity%20and%20Liberty-.aspx (Isr.); R. v. O'Connor, [1995] 4 S.C.R. 411 at paras. 17, 18 (Can.).

implement – and expand upon – the universal right to privacy in the manner it deems best. The United States is distinctive in that it has developed numerous sector-specific statutes and doctrines; most other nations have opted for "omnibus" privacy legislation that applies across the public and private sectors. For example, the German Data Protection Law establishes general privacy principles that apply to data processing activities of federal, state, and private entities. Bundesdatenschutszgesetz [Federal Data Protection Law], § 1(2) (Ger.), *official translation at* https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html. There are over 100 countries with privacy laws broadly reflecting these principles, including the members of the data protection treaty commonly referred to as Convention 108. *See* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108. This includes a number of non-European states such as Uruguay and Tunisia. *See id.*

These examples provide a flavor of how the interaction of international law and domestic sovereignty leads to a variety of privacy protections. One nation may see the right to privacy as requiring strict limitations on governmental access to personal information. *See Riley*, 134 S. Ct. at 2490-91. Others might regulate private actors that traffic in personal data. *See* Council Regulation 2016/679, General Data Protection Regulation, art. 5, 2016 O.J. (L 199) 1 (EC). Still others might articulate privacy as a right to personal control over information about oneself. *See* Art. 43, Constitución

Nacional (Arg.). This last is a right that has manifested in different nations as the right to informational self-determination, BVerfG [Federal Constitutional Court], Dec. 15, 1983, 1 BVR 209/83 (Dec. 15, 1983) (Ger.), the right to access and correct information about oneself, Protection of Personal Information Act 4 of 2013 § 5 (S. Afr.), or the "right to be forgotten." Sri Vasunathan v. Registrar General, WP 62038/2016 (Kar. Jan. 23, 2017) (India); Press Release, Korean Communications Commission, KCC Takes Measures to Guarantee "Right To Be Forgotten" (Apr. 29, 2016) (S. Kor.). All of these formulations of the right to privacy are equally valid expressions of the same underlying universal right, and basic principles of international law counsel that they be given due respect.

III. "Jurisdiction in cyberspace is hard, but we're working on it."

This case raises hard questions about whose privacy laws should govern a law enforcement agency's access to private data stored "in the cloud" with a third-party provider. The source of the difficulty lies in the technology underlying cloud storage. Unlike tangible items of evidence – be they daggers or diaries – that can only be in the territory of one sovereign at a time, the contents of a cloud storage account are distributed between multiple physical storage devices. *See How Cloud Object Storage Works*, IBM, https://www.ibm.com/cloud-computing/products/storage/object-storage/how-it-works/ (last visited Dec. 9, 2017). These devices are intentionally dispersed, often across national

borders, to protect against unforeseen outages. *See*, *e.g.*, *AWS Global Infrastructure*, Amazon Web Services, https://aws.amazon.com/about-aws/global-infrastructure/ (last visited Dec. 9, 2017) (describing automatic failover between international "Availability Zones"). When an account is accessed, the cloud storage provider retrieves the "slices" of data that have been stored on different devices and reassembles them. *Id.* Further complicating matters, data dispersal algorithms may automatically move data between locations based on users' locations, available bandwidth, or even legal constraints. *See* Sharad Agarwal et al., *Volley: Automated Data Placement for Geo-Distributed Cloud Services*, 10 NSDI 28 (2010).

None of this complexity is apparent to the end user, though. From the user's point of view, there is a single account, and it exists in a single place: cyberspace. To the extent that lay people think of these matters at all, they likely believe that their privacy rights in cyberspace are the same as in whatever physical place they reside. At the very least, most users would find it surprising, and perhaps unfair, to learn that the right to privacy in the non-territorial world of cyberspace is based on distinctly territorial notions.

All of this makes it very hard for any court to determine whether one country's domestic legal process is sufficient to obtain data subject to competing jurisdictional claims, or whether some form of transnational legal process is required in view of the interests of other sovereigns. While territoriality is the starting place for such a determination, this hoary doctrine is

often incapable of answering the tough jurisdictional questions that arise in the unique realm of cyberspace. Consequently, policymakers around the world are looking beyond territoriality to create specific rules that operationalize the universal right to privacy in a space that transcends national borders.

A. Territoriality is the starting point for jurisdiction, online and offline.

Under both international and U.S. law, a sovereign possesses jurisdiction over all persons and things located within its territory. One corollary of this doctrine is that "[jurisdiction] cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention." S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, ¶ 45. Extraterritoriality is therefore the exception, rather than the rule, in matters of jurisdiction. This Court has recognized as much in the presumption that U.S. laws apply only within U.S. territory, absent a clear legislative indication to the contrary. *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255-56 (2010); *E.E.O.C. v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991).

The international community – including the United States – has recognized that territoriality is the starting point for establishing the jurisdiction in cyberspace as well. In 2013, for example, the GGE issued the following consensus statement regarding sovereignty and jurisdiction in cyberspace:

> State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of [Information and Communication Technology]-related activities, and to their jurisdiction over ICT infrastructure within their territory.

U.N. Doc. A/68/98, *supra* p. 4, ¶¶ 20, 21. Since a U.S.-appointed expert from the State Department participated in the drafting of the consensus statement, *id.* at p. 13, it is fair to say that this statement represents the view of at least the U.S. Executive Branch on this matter. It is likewise fair to say that the fragile initial international agreement regarding jurisdiction over ICT infrastructure does not sufficiently distinguish such infrastructure from the international cyberspace that it supports, but does not on its own create. Accordingly, state activity in cyberspace that crosses traditional borders remains the subject of much debate.

B. Territoriality is hard to operationalize in cyberspace.

The central problem in this case is that no one agrees on how to apply principles of territoriality to determine which sovereigns' laws may appropriately authorize the disclosure of private data held "in the cloud." The problem arises from four aspects of cloud data storage that render inchoate the traditional doctrines of territoriality.

First, whereas physical evidence generally exists in one place at one time, data can be stored in multiple

places at once. *See generally* Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 365-75 (2015). Consequently, accessing the contents of a single, apparently unitary account may require retrieval of data stored on the territory of multiple sovereigns.

Second, there is no necessary correspondence between the physical storage location of an account's contents and the account holder's current location. J.A. at 133. All things being equal, cloud service providers prefer to store a user's data close to the user's primary location, *see id.* at 31, but oftentimes there will be an international or sub-national border between a user and their data, *see* Daskal, *supra*, at 365-69.

Third, because cloud data is partitioned, stored, and moved automatically by algorithms, no one – not the account holder, the cloud service provider, or the government agency requesting the data – can be sure where it is physically stored at any given time, unless and until they attempt to retrieve it. John Cauthen, *Executing Search Warrants in the Cloud*, FBI L. Enforcement Bull. (Oct. 7, 2014), https://leb.fbi.gov/articles/featured-articles/executing-search-warrants-in-the-cloud. In this case, the location of the data was not evident until a Microsoft employee looked up the account indicated on the warrant. J.A. at 35.

Fourth, the identity, nationality, and residency of the account holder – or even whether they are a natural or a legal person – is often unknown to both the cloud storage provider and the requesting agency. This is true in the case at bar, where the record is silent as

to the identity, residency, and citizenship of the individual whose emails the United States is seeking from Microsoft. J.A. at 141.

These and other factors make it very difficult to operationalize the principle of territoriality in cyberspace. Indeed, there are at least four different grounds on which a state could assert a jurisdictional claim to data in cyberspace based on a territorial connection:

First, a state may claim jurisdiction over data that is physically stored on an electronic medium located within its territory (jurisdiction *in rem* over the data).

Second, a state may claim jurisdiction over data that belongs to an account holder presently located on its territory (jurisdiction *in personam* over the data owner).

Third, a state may claim jurisdiction over data that is held by a service provider located on its territory (jurisdiction *in personam* over the service provider).

Fourth, a state may claim jurisdiction over any data that may be controlled by a service provider from within its territory (a fact-specific variation of jurisdiction *in personam* over the service provider).

Jurisdiction over data stored "in the cloud" may also be asserted on grounds other than territoriality, such as the nationality of the account holder or of the cloud storage provider. In the proceedings below, however, both Microsoft and the United States argued that territorial jurisdiction decisively answers the question

now before the Court. Microsoft argued that the location of the data in Ireland (the first of the four aforementioned jurisdictional grounds) bars the United States from relying on its legal process to compel Microsoft, a company based in the United States, to produce the emails for criminal investigative purposes. The United States, meanwhile, argues that Microsoft's substantial connections to the United States and its capability to retrieve the emails from a facility in California (the third and fourth of the aforementioned jurisdictional grounds) are adequate to compel the company to produce the emails, regardless of where they are stored.

The Special Rapporteur has no view on whose interpretation of the Stored Communications Act is correct as a matter of U.S. domestic law. In deciding this question, however, the Special Rapporteur would encourage the Court to be mindful of three considerations.

The first consideration is factual. This Court should bear in mind that Ireland can make the same assertions of territorial jurisdictional over Microsoft as the United States can. Under the third of the four jurisdictional theories described above, the emails at the heart of this case are stored on servers controlled by Microsoft Ireland Operations Limited, an Irish corporation. J.A. at 30. Similarly, under the fourth theory, Microsoft possesses the means to retrieve the emails from Ireland as well as the United States. *Id.* at 31-32. Thus, it can be said that the territorial claims of the

United States and Ireland regarding the emails are in equipoise.

The second consideration is prudential. In answering the question presented in this case, the Court will be deciding, at least implicitly, whether the jurisdictional connections between the United States and the emails are sufficiently strong that it is appropriate to rely on U.S. rather than international legal process to obtain the data, in light of Ireland's equivalent jurisdiction connections to the emails.

The third consideration is practical. The Special Rapporteur notes that U.S. courts have found it difficult to allocate jurisdiction between the several States when it comes to online conduct. *See*, *e.g.*, *Zippo Mfg. Co. v. Zippo Dot Com*, 952 F. Supp. 1119, 1123 (W.D. Pa. 1997); Alan M. Trammell & Derek E. Bambauer, *Personal Jurisdiction and the "Interwebs,"* 100 Cornell L. Rev. 1129, 1157-61 (2015) (evaluating traditional personal jurisdictional principles as applied to cyberspace). This Court has grappled with the same difficulties; as Justice Breyer queried in a recent concurrence, "[W]hat do those [jurisdictional] standards mean when a company targets the world by selling products from its Web site?" *J. McIntyre Mach., Ltd. v. Nicastro*, 564 U.S. 873, 890 (2011) (Breyer, J., concurring).

In view of these considerations – especially the difficulties that courts have encountered in developing the law of jurisdiction within the United States – the Special Rapporteur urges this Court to exercise the

utmost caution in deciding this case. Even though the facts of the case at bar are relatively simple (insofar as only two countries have plausible jurisdictional claims over the data at issue), the questions of law are as difficult as their answers likely to prove politically sensitive.

C. Efforts are underway to solve the problem of jurisdiction in cyberspace.

As global commerce and traffic in data increases, the international legal system is increasingly developing granular and operational privacy protections. Given the complexity of applying the doctrine of territoriality to the jurisdictional questions in this case, the Special Rapporteur respectfully submits that negotiation and legislation are the most appropriate means of developing mechanisms by which a state may efficiently obtain access to cloud data.[5]

Some such processes of negotiation and legislation are already under way, driven by the recognition that the current generation of Mutual Legal Assistance treaties ("MLATs"), which were designed to facilitate the transfer of tangible evidence across borders, are

---

[5] In this regard, the Special Rapporteur finds it noteworthy that, within the United States, questions regarding which federal district court could appropriately issue a warrant "to use remote access to search electronic storage media [and] copy electronically stored information" were ultimately resolved not by litigation, but by the legislative process of enacting a rule permitting a magistrate judge "in any district where activities related to a crime may have occurred" to issue such a warrant. Fed. R. Crim. P. 41(b)(6).

functionally obsolete. These processes seek to create new processes that operationalize the universal right to privacy in the international world of cyberspace, much as domestic law has traditionally operationalized that right in the territorial world of physical spaces.

As indicated previously, the Special Rapporteur is playing an important role in facilitating and fostering these efforts. For example, in conjunction with the MAPPING project,[6] the Special Rapporteur has been developing a Draft Legal Instrument on Government-Led Surveillance ("LI") with the input of experts from governments, international organizations, civil society, corporations, and academia. The current version of the LI suggests the creation of an International Data Access Warrant ("IDAW") that governments can use to obtain private data for investigative purposes in situations such as the one at bar, when multiple sovereigns can make *bona fide* jurisdictional assertions over the same data. The current LI further suggests the creation of an International Data Access Authority composed of retired judges from the contracting states who would evaluate IDAW applications against international human rights norms before authorizing them.

---

[6] MAPPING stands for "Managing Alternatives for Privacy, Property and Internet Governance." The project is administered by the University of Groningen in the Netherlands and its partners include universities and research institutions across Europe as well as INTERPOL. MAPPING receives the majority of its funding from the European Union. For more information, see https://mappingtheinternet.eu.

Other examples of constructive, multilateral efforts in this sphere can be found in the European Union. Since May of this year, a judicial authority in a participating member-state may issue a "European Investigative Order" that is valid, enforceable, and directly executable in 24 of the European Union's 27 member-states. *See* Council Directive 2014/41, art. 1, 2014 O.J. (L 130) 1 (EC). European Investigative Orders may be used by one member-state to obtain evidence within the jurisdiction of a fellow participating member-state, among other purposes. *Id.* Additionally, the Council of Europe's Cybercrime Convention Committee recently approved terms for the preparation of an additional protocol to the Budapest Convention on Cybercrime, aimed at providing effective mutual legal assistance in relation to evidence stored "in the cloud." *See Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime*, Cybercrime Convention Committee, T-CY(2017)3. As a party to the Budapest Convention, the United States will likely play an active role in drafting this protocol.

There are also efforts to address this problem underway in the United States. The Department of Justice has proposed draft legislation that would enable bilateral agreements with approved foreign governments, starting with the United Kingdom, under which the domestic legal processes of one country could be used to request data held by service providers based in the other country. *See* Office of Legislative Affairs, U.S. Dept. of Justice, Letter to the President of the Senate (July 15, 2016), available at

http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf; *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 1 (2017) (statement of Richard W. Downing, Acting Deputy Assistant Att'y Gen. of the United States). The Special Rapporteur views the proposed legislation as a constructive contribution to finding a negotiated solution to the problem of data access across borders, though he has expressed concerns regarding the adequacy of the privacy protections that are incorporated into the current working draft.

Finally, the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks demonstrate the promise of multilateral negotiations to address national and regional differences in the right to privacy at the international level. *See generally* Program Overview, Privacy Shield Framework, https://www.privacyshield.gov/Program-Overview (last visited Dec. 10, 2017). Faced with the need to facilitate transfers of personal data between the two continents, the United States and the EU negotiated a mechanism for enforcing data protection standards that are functionally equivalent to those provided by European law against companies in the United States. Later, the United Stated entered into a substantially similar agreement with Switzerland. Under these agreements, no nation was required to alter its domestic laws. Rather, international cooperation between sovereign governments and inter-governmental organizations led to mutually acceptable privacy

protections. While the Privacy Shield Frameworks do not address the question of whose law may appropriately authorize a law enforcement request for access to data, the success of the Privacy Shield framework illustrates the real potential for diplomatic efforts in this field to bear fruit.

IV. In light of the potential impact of this decision on international law and foreign relations, the Court should rule narrowly.

The question presented in this case is whether, under the particular factual circumstances of this case, a warrant obtained by the United States pursuant to the Stored Communications Act, 18 U.S.C. § 2703, compels Microsoft to produce the contents of an email account stored on a server in Ireland. This Court may well find that U.S. domestic law is sufficient to answer this question. The Special Rapporteur nevertheless wishes to highlight the significant international repercussions of its decision, particularly on the right to privacy as it is enshrined and protected by the domestic laws of various states. In this sense, the Special Rapporteur agrees with the observation of the Second Circuit that:

> it [is] difficult to dismiss [foreign data protection] interests out of hand on the theory that the foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to "collect" from servers located overseas and "import" into the United States data, possibly belonging to a foreign citizen, simply because the

> service provider has a base of operations within the United States.

Pet. App. 17a. The decision of this Court will be highly influential beyond the borders of the United States, given the respect this Court enjoys internationally and the key role this country plays in cyberspace. Accordingly, the Special Rapporteur respectfully urges the Court to consider the interests of governments around the world in ensuring that their choice to adopt privacy laws that exceed the minimum required by international human rights law is effectuated in our new digital age. Furthermore, the Special Rapporteur believes it would be appropriate for this Court to consider how its ruling would impact the privacy guarantees enshrined in the U.S. Constitution were the facts of this case reversed. Finally, the Special Rapporteur urges the Court to be cognizant of the ongoing diplomatic and legislative efforts to address the difficult jurisdictional issues regarding law enforcement access to data stored "in the cloud."

The Special Rapporteur believes that a narrow, fact-specific ruling would be most helpful to furthering the interests of the United States and the international community, and urges the Court to consider such an approach to the extent that it is consistent with principles of U.S. law. In advocating for a narrow ruling, the Special Rapporteur is not suggesting that the Court should abdicate its responsibilities. Rather, the Special Rapporteur asks that the Court observe the longstanding judicial practice of exercising restraint in the face of uncharted territory, sweeping assertions,

foreign interests, and politically-tinged issues so that the coordinate branches of government may effectuate their constitutionally appropriate role. *See*, *e.g.*, *Bank Markazi v. Peterson*, 136 S. Ct. 1310, 1317 (2016) (executive or legislative action in realm of foreign policy "warrants respectful review by courts"); *Mathews v. Diaz*, 426 U.S. 67, 82 (1976) (need for flexibility "dictate[s] a narrow standard of review" in areas implicating foreign relations); *Harisiades v. Shaughnessy*, 342 U.S. 580, 589 (1952) ("[P]olicies in regard to the conduct of foreign relations [are] entrusted to the political branches of government [and] largely immune from judicial inquiry. . . .").

A. Ruling narrowly will respect the privacy interests of other nations and foster international cooperation.

As explained in Part II, *supra*, all nations have the duty and the power to protect the right to privacy. Though nations differ in their conceptions of this right, all are deserving of respect. *See Underhill*, 168 U.S. at 252. This is in accord with the principle of comity, "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation. . . ." *Hilton v. Guyot*, 159 U.S. 113, 164 (1895). In the judicial context, comity "refers to the spirit of cooperation in which a domestic tribunal approaches the resolution of cases touching the laws and interests of other sovereign states." *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa*, 482 U.S. 522, 543 n.27 (1987). While not an

"absolute obligation," *id.*, courts are expected to take comity considerations into account whenever the laws of this country impose legal duties or consequences beyond its borders, *see id.* at 545-46 (in adjudicating discovery requests, "courts should . . . take care to demonstrate due respect . . . for any sovereign interest expressed by a foreign state"); *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 128 (2013) (Breyer, J., concurring) (noting importance of comity to limiting reach of Alien Tort Statute); *see also Tiffany (NJ) LLC, Tiffany & Co. v. China Merchants Bank*, 589 F. App'x 550, 553 (2d Cir. 2014), *as amended* (Sept. 23, 2014) (ordering district court to "consider[] principles of international comity" before asserting jurisdiction over foreign banks). This Court has recognized comity as an animating principle behind enforcement of foreign judgments in U.S. courts, *Hilton*, 159 U.S. at 206, foreign sovereigns' access to U.S. courts, *Guar. Tr. Co. of New York v. United States*, 304 U.S. 126, 134-35 (1938), and the act of state doctrine, *Banco Nacional de Cuba v. Sabbatino*, 376 U.S. 398, 416-18 (1964).

Respect for foreign sovereigns is not, however, premised solely on an abstract notion of sovereign independence. Rather, it is a practical element of fostering positive diplomatic and commercial relationships between nations and preventing "international discord." *Arabian Am. Oil*, 499 U.S. at 248. Nor is comity solely the concern of the judiciary. As this Court observed in *F. Hoffmann-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 164-65 (2004), it is assumed "that legislators take account of the legitimate sovereign interests of other nations when they write American

laws[, which] helps the potentially conflicting laws of different nations work together in harmony – a harmony particularly needed in today's highly interdependent commercial world." Executive agencies are similarly expected to consider the interests of foreign sovereigns when enforcing domestic laws. *See*, *e.g.*, Fed. Trade Comm'n, Antitrust Guidelines for International Enforcement and Cooperation 27-29 (2017); Offices of the U.S. Att'ys, U.S. Dept. of Justice, Criminal Resource Manual § 279(B).

Although the outcome of this case may turn entirely on the law of the United States, it will have an international effect. Data which currently resides on a server located in Ireland will either be disclosed to the U.S. government or not, based on this Court's ruling. This decision will no doubt resonate throughout the international community. Foreign courts interpreting their laws governing searches and seizures in cyberspace will surely consider this Court's jurisdictional analysis in deciding cases with similar facts. The European Commission's Article 29 Working Party ("WP29") has already noted the impact this decision may have on the development of EU cross-border electronic search regulations. *See Data Protection and Privacy Aspects of Cross-Border Access to Electronic Evidence*, European Commission Article 29 Working Party (Nov. 29, 2017), http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801.

Moreover, the political branches of foreign governments may believe the Court to be endorsing a particular conception of the right to privacy and respond accordingly, whether or not that is in fact the Court's

intent. The WP29 recently observed, in a similar context, that

> the adoption of [a] production order towards organizations which are not established in the EU could also increase the risk of adoption by non-EU countries of similar instruments that would enter in direct conflict with EU data protection law.

Article 29 Working Party, *supra*, at 9. The same is true for this Court's ruling on the appropriateness of the United States asserting jurisdiction over the data at issue in this case. It is appropriate for the Court to consider the impact on the United States if another nation – potentially one less protective of the right to privacy – asserted a similar theory to access data stored within the borders of this country, for "[e]xtraterritorial assertions of jurisdiction are not one-sided." *Societe Nationale*, 482 U.S. at 544 n.29.

The "lesson of comity" here is that the interpretation of the Stored Communications Act vis-a-vis the territoriality of data does not take place "in a world of only one sovereign." *Id.* The Special Rapporteur respectfully asks that the Court rule consider the extensive effects its decision may have on foreign sovereigns, as well as the United States' relationships with those sovereigns, in deciding this case.

B. Ruling narrowly will permit political efforts to address international jurisdiction over data to proceed unhindered.

This Court has long recognized the undesirable consequences of parallel judicial and political action, including the potential to undermine the other branches of government. *Baker v. Carr*, 369 U.S. 186, 226 (1962). These concerns are heightened when, as here, the political action at hand touches on foreign relations. *Banco Nacional*, 376 U.S. at 437. Justice Marshall eloquently described the tension between international political processes and judicial review of foreign policy in his dissent to *Alfred Dunhill of London, Inc. v. Republic of Cuba*:

> [I]t has . . . been suggested that a doctrine of deference based upon the absence of consensus as to controlling principles of international law allocates legal competence among nations in a manner that promotes the growth of international law. Whether considerations of its contribution to the development of international law provide a basis for the act of state doctrine independent of the notion of separation of powers is a question that the Court . . . need not consider. It is worth noting, however, that the *Sabbatino* Court was sensitive to the fact that a court's invalidation of a foreign sovereign's acts on the basis of principles of international law that are not the subject of "unambiguous agreement," is unlikely to be regarded as impartial.

425 U.S. 682, 727 n.12 (1976) (citations omitted). The question now before the Court – whether an appropriate basis exists for the United States to assert its jurisdiction over data held in Ireland – may be justiciable. *See Baker*, 369 U.S. at 211 ("[I]t is error to suppose that every case or controversy which touches foreign relations lies beyond judicial cognizance."). Nevertheless, the concerns identified by Justice Marshall in *Alfred Dunhill* and this Court in *Sabbatino* also lurk in the peripheries of this case. There is an absence of consensus under international law, and the Court's ruling, though impartial, is unlikely to be neutral in its effect on the international political process. A sweeping ruling from the Court may discourage negotiations over access to data, either because there is no need for such negotiations under a broadly permissive conception of territoriality, or because such negotiations appear doomed under an overly narrow conception of territoriality.

Recent developments on the ground give weight to such concerns. After a record of success in previous years, the failure in the June 2017 round of GGE negotiations prompted a public statement from the U.S. representative. In her June 23, 2017 address to the Chair of the GGE, U.S. Deputy Coordinator for Cyber Issues Michele Markoff echoed the Special Rapporteur's long-held view that the GGE has failed to "fulfil the mandate given to [the GGE] by the U.N. General Assembly to study *how* international legal rules and principles [of humanitarian law, self-defense, and state responsibility] apply to the use of ICTs." Michele

Markoff, Office of the Secretary of State, Explanation of Position at the Conclusion of the 2016-2017 U.N. GGE (June 23, 2017), https://usun.state.gov/remarks/7880. Her frustration with governments that "seem to want to walk back progress made in previous GGE reports" and "believe their States are free to act in or through cyber-space to achieve their political ends with no limits or constraints on their actions" highlights the sensitivity of current negotiations in that field.

Deputy Coordinator Markoff's comments are equally applicable to the field of online privacy. No country has the right "to act in or through cyber-space to achieve their political ends" without regard for the universal right to privacy. However, unilateral action taken without due consideration of the different – but equally valid – privacy protections of other nations may be perceived as asserting just such a right. As Deputy Coordinator Markoff saw firsthand, such an assertion could have deleterious, if not fatal, effects on attempts to reach international agreement on the matter. Accordingly, any one court in any one country should not be substituting its judgment for political and diplomatic processes, however wise and distinguished that court may be.

CONCLUSION

Questions regarding the territoriality of data held "in the cloud" are marked by an abundance of plausible

theories and a dearth of international agreement as to which one is correct. This is the result of the unique complexities of applying traditional concepts of territoriality to information that could potentially reside in, and be accessed from, any one of a number of sovereign territories – or even more than one. Any court that engages with such questions should remain cognizant of the ongoing diplomatic and legislative efforts to address these complexities, as outlined in Part III, *supra*.

The Special Rapporteur respectfully submits that if the Court rules on the issue of jurisdiction over the emails in question, the grounds for finding or not finding such jurisdiction should not be rooted in the physical location of the data or the territorial presence of the data provider. Rather, it should be explicitly attributed to the absence of controlling international law on the issue. The Special Rapporteur respectfully asks that the Court issue a narrow ruling that provides ample room for current and future efforts to reach international agreements as to the principles of jurisdiction and privacy in cyberspace to continue.

Respectfully submitted,

VIVEK KRISHNAMURTHY
MASON KORTZ
CYBERLAW CLINIC, HARVARD LAW SCHOOL
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-384-9125
vkrishnamurthy@law.harvard.edu

Dated: December 13, 2017