AMERICAN CONSTITUTION SOCIETY FOR LAW AND POLICY

Issue Brief October 2017

Access to Data Across Borders: The Critical Role for Congress to Play Now

Jennifer Daskal

In December 2013, the government served a warrant on Microsoft, demanding emails associated with a particular email account. Microsoft refused to comply. The data was stored on a server in Dublin, Ireland, and according to Microsoft, the demand was an impermissible exercise of the government's warrant authority. The government fought back, arguing that Microsoft, as a Washington-based company, could access the data from within the United States, and that this was therefore a territorial – and perfectly permissible – exercise of its authority.

At the heart of the dispute is the Stored Communications Act (SCA), a more than 20-year old statute that both protects the privacy of and regulates the disclosure of stored communications content.[1] The statute, written before there was any such thing as the global Internet, is silent as to its territorial reach. Under longstanding Supreme Court precedent, this means that it is to be interpreted as if it only applies within the territory of the United States.[2] But that leaves open the key question presented by what is now known as the "Microsoft-Ireland case": Does the location of the data or the location of the provider that discloses the data control? Microsoft contends it is the former, while the government asserts the latter. The case is now pending before the Supreme Court.[3]

Federal magistrate and district court judges in the Southern District of New York sided with the government, but the Second Circuit reversed.[4] The result, at least for the Second Circuit: U.S. warrant authority only extends to data stored within the United States, even if the crime is local, the target of the investigation is local, and the *only* foreign government nexus to the data is that the data happens to be stored in that foreign government's jurisdiction. If there isn't a workable framework

[1] 18 U.S.C. §§ 2701-2712 (2012).
[2] *See, e.g.,* Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247, 255 (2010) (emphasizing the "longstanding principle of American law that 'legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'") (citations omitted).
[3] *See* United States v. Microsoft, 2017 WL 2869958 (Mem) (Sup. Ct. Oct. 16, 2017) (granting cert).
[4] *See In re* Warrant to Search A Certain E-Mail Account Controlled and Maintained by Microsoft, 829 F.3d 197, 201-02 (2d Cir. 2016); *In re* Warrant to Search A Certain E-Mail Account Controlled and Maintained by Microsoft, 855 F.3d 53, 54 (2d Cir. 2017) (denying rehearing en banc).

for cooperation with the relevant foreign government or if law enforcement can't actually identify the relevant data location, the government is simply out of luck; there may be no way for law enforcement to lawfully compel production of the data, no matter how serious the crime. Even the judge who authored the Second Circuit's opinion recognized that this was not a satisfactory result and urged Congress to step in and update the statute.[5]

Meanwhile, a handful of magistrates and district court judges have come out the other way in analogous disputes involving Google and Yahoo!, ordering the tech companies to disclose customer data stored overseas.[6] But this result creates problems as well: It essentially says that the U.S. can compel the production of any and all data under the control of a U.S.-based provider, without regard to the potentially legitimate countervailing interests of foreign governments. This sets a concerning precedent that, if adopted widely, would make it harder for the United States to safeguard the data of its own citizens and residents and likely undercut privacy on a global scale. Such rulings also undercut U.S. business interests, which will find it harder to compete globally if and when they are perceived (rightly or wrongly) as a gateway for U.S. surveillance.

With the Supreme Court poised to hear the case, the need for congressional action is greater than ever. The Court is presented with the same stark choice that has faced the lower courts: Either Microsoft wins, and U.S. law enforcement access to data turns on the happenstance of where it is held. Or the government wins, and it can compel the production of data anywhere, without any statutory obligation to take into account countervailing considerations, including the potential legitimate interest of foreign governments in safeguarding the data of their citizens and residents. Neither is a satisfactory result.

Meanwhile, other provisions of the SCA are causing significant problems for foreign law enforcement when investigating criminal activity involving data that happens to be U.S.-held. This is due to provisions that preclude U.S.-based companies from disclosing stored communications content, such as emails, to foreign law enforcement, regardless of the equities in a particular case.[7]

---

[5] *In re* Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft, 855 F. 3d at 55 (Carney, J., concurring) ("It is overdue for a congressional revision [to the SCA] that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose.)

[6] *See In re* Search Warrant to Google, Inc., No. 17-mj-532 (N.D. Ala. Sept. 1, 2017), slip op. 23; *In re* Search Warrant No. 16-960-M-1 to Google, No. 16-960, 2017 WL 3535037, at *11 (E.D. Pa. Aug. 17, 2017), *aff'g* 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017); *In re* Search of Content Stored at Premises Controlled by Google Inc., No. 16-mc-80263, 2017 WL 3478809, at *5 (N.D. Cal. Aug. 14, 2017), *aff'g* 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *In re* Search of Information Associated with [redacted]@gmail.com That is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 3445634, at *27 (D.D.C. July 31, 2017), *aff'g* 2017 WL 2480752(D.D.C. June 2, 2017); *In re* Search of Information Associated with
Accounts Identified as [redacted]@gmail.com, No. 16-mj-2197, 2017 WL 3263351, at *9 (C.D. Cal. July 13, 2017); *In re* Search Warrant to Google, Inc., No. 16-4116, 2017 WL 2985391, at *12 (D.N.J. July 10, 2017); *In re* Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); *In re* Search of Premises Located at [Redacted]@yahoo.com, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017), slip op. 3.

[7] The SCA prohibits providers from turning over the content of communications, except in a limited number of

Consider, for example, U.K. law enforcement seeking emails of an alleged U.K.-based perpetrator in a London murder involving a U.K.-based victim. If the alleged perpetrator used a U.K.-based email service provider, the U.K. officials would likely be able to access that data within weeks, if not days or hours. If, however, he were using Gmail or another U.S.-based provider, the U.K. officials would need to make a diplomatic request for the data – what is known as a "mutual legal assistance request" – and then wait for the United States to respond. This is a lengthy process, requiring multiple Department of Justice reviews and a U.S. attorney to ultimately obtain a U.S. warrant for the data based on the U.S. standard of "probable cause" before transmitting the data to the U.K., a process that has been estimated to take an average of ten months and in many cases much longer.[8] This is so even if the *only* U.S. nexus to the crime is that the data happens to be U.S.-held.

Foreign law enforcement organizations chafe at the notion that they have to employ U.S. process to access data sought in the investigation of local crime involving non-U.S. citizens that are located outside the United States. And their investigations are stymied as a result. They are thus incentivized to pursue a range of concerning responses, including the following: the unilateral extraterritorial assertion of their own compulsory disclosure obligations, thereby putting companies in the middle of a potential conflict of laws, having to decide which law to comply with and which to violate; mandatory—and costly—data localization measures, policies that require data to be maintained locally as a way of ensuring access to it; and pursuit of alternative, and often surreptitious, means of accessing the data, including expanded lawful hacking authority and pursuit of broad decryption mandates.[9]

In fact, finding a solution to this problem is described by U.K. diplomats as one of the top diplomatic priorities of the United Kingdom vis-à-vis the United States. The U.K.'s Deputy National Security Advisor, Paddy McGuinness, has now testified in both the House and the Senate on the issue, highlighting its importance to the U.K. government.[10] And while the United States and United Kingdom have drafted an agreement that would facilitate U.K. access to data of non-U.S. citizens

---

situations. *See* 18 U.S.C. §§ 2702, 2703(a) (2016). While a "governmental entity" may compel such production, pursuant to a lawfully issued warrant, governmental entity is defined as "a department or agency of the United States or any State or political subdivision thereof." 18 U.S.C. § 2711(4) (2012). Thus, foreign governments do not qualify.

[8] The President's Review Group on Intelligence and Communication Technologies, *Liberty and Security in a Changing World* 226-229 (Dec. 12, 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. *See also* Vivek Krishnamurthy, "Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters," *Berkman Klein Center Research Publication No. 2016-3* (Feb. 18, 2016), https://ssrn.com/abstract=2733350 (highlighting problems with the mutual legal assistance system).

[9] For a more in-depth analysis of this issue, *see* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues,* 8 J. NAT'L SECURITY L. & POL'Y 473 (2016).

[10] *See Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights Hearing Before the S. Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 115th Cong. (2017) (statement of Paddy McGuinness https://www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights; *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (2017) (statement of Paddy McGuinness), https://judiciary.house.gov/wp-content/uploads/2017/06/McGuinness-Testimony.pdf.

and residents in the investigation of serious crime, subject to baseline substantive and procedural requirements, the agreement cannot be implemented without legislation amending the SCA.

The good news is that these issues have now been the subject of hearings and legislative efforts in the House and Senate. Of note, Senators Orrin Hatch (R-UT) and Christopher Coons (D-DE) and Representatives Tom Marino (R-PA) and Suzan DelBene (D-WA) have introduced legislation in their respective chambers—the International Communications Privacy Act (ICPA)[11]—which is designed to address the problem identified in the Microsoft Ireland litigation. While there is room for improvement (as discussed in more detail below), the legislation is an important starting point that shifts the focus away from the location of data to the location and identity of the target as a key factor in determining jurisdiction. Importantly, it mandates that the U.S. government obtain a warrant before accessing communications content. This is something already being done as a matter of practice and is required as a matter of law in the Sixth Circuit; codifying this rule would ensure its continued application.[12]

Draft legislation designed to allow the U.S.-U.K. agreement to be implemented and to allow for analogous agreements with other rights-respecting nations has been sent from both the Trump and Obama administrations to Capitol Hill.[13] Specifically, the draft legislation would authorize the executive branch to enter into executive agreements with foreign governments that would permit, on a reciprocal basis, direct access to the communications content of foreigners located outside the United States, so long as a long list of substantive and procedural safeguards are met. Here, too, there is room for improvement, as also discussed below. But as a whole, it is an approach that Congress should endorse—and adopt.

In this Issue Brief, I examine these issues in more detail—providing additional detail on the problem, the need for congressional involvement, and the ideal legislative path forward.

It should be said at the outset that this Issue Brief addresses only one piece of SCA reform that is needed—namely the problems and challenges associated with access to data across borders. Separate bills are also pending that would, among other things, set procedural and substantive rules governing

[11] S. 1671, 115th Cong. (1st Sess. 2017); H.R. 5323, 114th Cong. (2d Sess. 2016).
[12] *See* U.S. v. Warshak, 631 F. 3d 266, 288 (6th Cir. 2010) (holding that "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause").
[13] *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (2017) (statement of Richard W. Downing, Acting Deputy Assistant Attorney General), https://judiciary.house.gov/wp-content/uploads/2017/06/Downing-Testimony.pdf. Almost identical draft legislation introduced by the Obama Administration is available here: https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p1/. Specifically, the draft legislation requires an Attorney General-issued certification that the "domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement" and lists a number of factors to be considered in making this determination, including whether the foreign government "demonstrates respect for the rule of law and non-discrimination."

the acquisition of geo-location data; set much-needed time limits on the use of so-called "gag orders," which prevent service providers from informing their customers that their data has been accessed by the government; and codify the warrant requirement for communications content (in the event it is not clarified as part of these cross-border reforms).[14] These are all pieces of the SCA that also need updating.

I. The Source of the Problem

Until relatively recently, evidence sought in the investigation of local crime tended to be locally held. Of course, exceptions existed—when, for example, a sophisticated criminal ring spirited stolen goods across borders—but those cross-border moves took a great deal of effort, and for the most part local officials investigating local criminal activity could look locally. They could obtain a warrant for, say, the house or office of a suspect, and, if available, find the sought-after evidence nearby—certainly within the state's territorial jurisdiction. And even if the suspect were making phone calls to conspirators across a territorial border, law enforcement could listen in to those communications as they crossed local telecommunications networks.

But the rise of a globally interconnected communications network, coupled with the growing use of encrypted communications technology, has changed that reality. Increasingly, sought-after data is neither locally held nor locally accessible. Rather, law enforcement increasingly finds itself seeking data stored across borders, even in the investigation of local crime.

Consider, for example, a resident of France who uses Gmail. Her data is not likely to be stored in France. In fact, it is likely moved around with some frequency, very likely across multiple borders. Even if it transits through France, it is likely to be encrypted en route. Moreover, these locational choices are made by a third-party provider—in this case Google—that manages her data and moves it around for reasons of efficiency, tax purposes, and energy costs. There may be absolutely no connection between the French resident and where her data happens to be held other than the fact that a private company decided to put it there. The same is true for U.S. users, as well as most users around the world.

The law has not caught up to the reality. The drafters of the SCA were writing before there was a global Internet. Their silence as to its territorial scope reflected the world as they knew it at that time. They simply couldn't have imagined the kind of globally interconnected Internet that exists today, with data crossing borders across the globe at the speed of light, sometimes stored in multiple places simultaneously, sometimes divided and distributed across multiple jurisdictions, and largely based on the business decisions of third-party providers. The drafters never grappled with the complicated jurisdictional issues that this reality generates.

Given the silence of the statute, the Second Circuit in the Microsoft-Ireland case applied the long-

[14] *See, e.g.,* ECPA Modernization Act of 2017, S. 1657. 115th Cong. (1st Sess. 2017); *see also* H.R. 387, 115th Cong. § 4 (1st Sess. 2017); *see also* Email Privacy Act, S. 1654, 115th Cong. (1st Sess. 2017).

standing assumption that location of property (in this case data) delimits territorial jurisdiction. But such a data location-driven approach to jurisdiction fails to reflect the underlying normative interests that this long-standing rule is meant to protect.

Consider, for example, the long-standing international law rule that prohibits State A from unilaterally accessing property in State B, absent State B's consent. Such a rule makes good sense for tangible, non-divisible property. The prospect of foreign law enforcement officials surreptitiously crossing a border to search one's property—or even worse, seize it and spirit it back across the border—is concerning. Such a system runs counter to principles of democratic accountability, undercuts the rule of law, and almost certainly creates international conflict given the prospect of two different sovereigns claiming interest in the same, non-divisible piece of property.

To avoid these problems, both domestic and international rules require that, as a general matter, U.S. law enforcement employ what is known as "mutual legal assistance process" (MLA) if it seeks property in another country. This process entails U.S. law enforcement making a diplomatic request to the foreign government for the property. The foreign government then assesses the request, and if it deems the request appropriate, accesses the property according to its own rules and procedures. The same goes for foreign law enforcement seeking data in the United States.

But data is different than other forms of tangible property in three key ways:

- *First*, data can be accessed without any state agent or third party acting on the behest of the state crossing a border. This means there is no physical, tangible entry by foreign law enforcement or any agent of foreign law enforcement in the accessing of data across borders. There may still be an intrusion, but it is not a physical, tangible one.
- *Second,* data can be copied with the original left intact, still available for use by the data subject (the individual with a possessory and privacy interest in the data) and still available to be accessed by the host state. The divisibility of data thus reduces the concern about friction resulting from two sovereigns seeking control over a singular piece of indivisible property.
- *Third*, and critically, the mobility of data coupled with the fact of third-party control means that there may be no connection between the location of the data and the foreign government other than the fact that a third party chose to place it there. As a result, there is no principle of democratic accountability protected by a rule that delimits jurisdiction based on location. There also might not be any link between the location of the data and the key sovereign interests that the jurisdictional rules regarding enforcement are largely meant to protect—namely, the sovereign interest in prosecuting criminal activity with a territorial nexus and the sovereign interest in protecting one's own citizens and residents.

Together, these factors make data location a particularly poor basis for delimiting law enforcement access. Such a rule will inevitably be both over and under-inclusive, granting governments control over data in which they have no legitimate interest and precluding governmental access to data in

which they have legitimate interests simply because of a third-party decision to move it across territorial borders.

What is instead needed is a set of rules that better reflects the key interests at stake: rules that ensure the United States and other countries can regulate access to their own residents' and citizens' data, consistent with principles of democratic accountability and consistent with the sovereign interest in protecting the privacy interests of one's own residents and citizens. Rules also should ensure that such access is conditioned on respect for the rule of law and pursuant to baseline substantive and procedural protections designed to protect privacy and prevent abuse.

In what follows, I suggest ways to amend the SCA in light of this reality, starting first with the question of law enforcement access to extraterritorially-located data, and second, turning to the issue of foreign law enforcement to U.S.-held data.

II. A Microsoft Ireland Solution

The Electronic Communications Privacy Act's (ECPA)[15] silence as to the territorial reach of the government's warrant authority means that the Supreme Court must divine the 1986 Congress's intent. In so doing, it will be presented with one of two stark choices: either the warrant authority reaches all U.S.-controlled data, regardless of location or other potentially relevant considerations; or it reaches only that data that happens to be located within the territorial boundaries of the United States. Neither answer is satisfactory.

Rather than leave the issue to the Court to work out, Congress should now step in and clarify the territorial scope, as numerous judges have urged.[16] In fact, even the companies litigating the cases recognize that this is a matter better left for Congress.[17] A legislative solution should reflect the following three key principles:

First, U.S. law enforcement access to stored communications content should not turn on the happenstance of where it is held. This is a particularly poor basis for delimiting law enforcement jurisdiction. It means that U.S. law enforcement will be unable to access sought-after data in the

---

[15] The SCA was enacted as Title II of ECPA.

[16] *See, e.g., In re* Warrant to Search Certain E-Mail, 829 F.3d. 197, 233 (2d Cir. 2016) (Lynch, J., concurring) ("Although I believe that we have reached the correct result as a matter of interpreting the statute before us, I believe even more strongly that the statute should be revised. . ."); *In re* Warrant to Search Certain E-Mail, 855 F.3d at 55 (Carney, J., concurring) (urging Congress to act); *see also id.* at 62 (Jacobs, J., dissenting) (noting the possibility of congressional action); *id.* at 68 (Cabranes, J., dissenting) (same).

[17] *See, e.g., Facilitating Cooperation and Protecting Rights: Hearing on Law Enforcement Access to Data Stored Across Borders Before the Subcomm. On Crime and Terrorism* of the S. Comm. on the Judiciary, 115th Cong. (2017) (statement of Brad Smith), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Smith%20Testimony.PDF (emphasizing that "litigation is not a substitute for policymaking" and urging Congress to update ECPA); Br. in Opposition, *supra* note 5, at 3 ("Congress alone has the authority and the institutional competence to craft a new legislative scheme for a world not anticipated in 1986."); Kent Walker, *Digital Security and Due Process: A New Legal Framework for the Cloud Era*, The Keyword (June 22, 2017), https://www.blog.google/topics/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/.

investigation of serious crime, even in situations where the target and victim are both U.S. citizens, and even if the place where the data is located has absolutely no connection to the case or individuals being investigated.

Second, U.S. law enforcement should be required to obtain a warrant to compel production of communications content, regardless of where it is held, even if it is located overseas.[18] This is something that is required by the Sixth Circuit[19] and is done by the executive branch as a matter of practice, but is not required by statute. The SCA's outmoded distinctions based on type of service provider and length of time of storage—pursuant to which data stored 180 days or less is protected by the warrant requirement, but data stored longer is not—should be eliminated.[20]

Third, U.S. law should respect the legitimate interests of foreign governments in delimiting access to data of their own citizens and residents, much as the United States correctly insists on when foreign governments seek the data of U.S. citizens and residents. This is important as a means of standard setting, something that will ultimately inure to the benefit of U.S. citizens and residents. As the home to some of the world's largest tech companies that control so much of the world's communications content, this may not seem particularly important now. But as foreign-based companies gain a greater share of the market, it will be increasingly important to put in place protections that ensure respect for U.S. rules governing access to U.S. person data. It is also a means of protecting U.S. companies and thus the economy. Rightly or wrongly, much of the rest of the world fears what they see as pervasive U.S. surveillance. A rule that permits U.S. law enforcement to access U.S.-held data anywhere around the world without regard to any countervailing considerations, feeds into these fears and makes it harder for U.S.-based service providers to compete globally. The Microsoft-Ireland case, and the way in which the issue ultimately gets resolved, is being watched not just in the United States, but all around the world precisely for this reason.

The recently introduced International Communications Privacy Act (ICPA) is a good place to start.[21] It requires a warrant for all stored communications content, shifts the focus away from the location of the data to the nationality and location of the target, and seeks to accommodate—on a reciprocal basis—foreign governments' interests in protecting the data of their own citizens and residents. That said, it does so through a complicated and cumbersome scheme that only comes into play if and when a foreign government seeking the data of a U.S. citizen or legal permanent resident self-certifies that it will, among other things, provide reciprocal notice and an opportunity to object, *and*

[18] If, as Microsoft contends, the SCA only regulates domestic stored communications, its protections (including the warrant requirement) would not extend to data that is stored outside the United States. *See In re* Warrant to Search Certain E-Mail, 855 F.3d at 73 (Raggi, J., dissenting) (warning that "the same reasoning that leads the panel to conclude that § 2703(a) warrants cannot reach communications that Microsoft has stored in Ireland might also preclude affording § 2702(a) privacy protections to such materials.")
[19] *Warshak*, 631 F.3d at 288.
[20] See 18 USC §§ 2703(a)-(b) (2012).
[21] S. 1671, 115th Cong. (1st Sess. 2017); H.R. 5323, 114th Cong. (2d Sess. 2017).

the Attorney General and Secretary of State determine that a number of conditions are met.[22] As a practical matter, the list of so-called "qualifying foreign governments" is likely to be null, or at least very small, in the short to medium term. The legislation also somewhat unusually gives qualifying countries an opportunity to come to U.S. court and effectively move to quash the warrant.[23]

Such a scheme should be supplemented—and perhaps replaced—with a requirement that courts do a comity analysis *any time* the U.S. government is knowingly seeking the data of a foreigner located outside the United States and that request creates a conflict of laws. This would codify something that is now done as a matter of discretion, ensuring that such judicial review takes place and codifying the factors the court must consider in issuing the warrant, including the location of the crime, victim, and alleged perpetrator; the seriousness of the crime; the importance of the data to the investigation of the crime; the possibility of accessing the data via other means; U.S. interest in prosecuting the offense; and the relevant foreign governmental interest.

An alternative, broader proposal would require such comity analysis any time the U.S. government is knowingly seeking the data of a foreigner located outside the United States, without regard to the question of whether there is a conflict of laws. In such a situation, the courts would then take into account the existence (or not) of such conflicts. This has the advantage of ensuring that potential foreign government interests are taken into account in *all* situations in which the United States is seeking the data of a foreigner outside the United States. However, it has the arguable disadvantage of putting an additional burden on the requesting law enforcement officials and courts that are then required to do the comity analysis in a broader number of cases.

Importantly, either scheme would require such a comity analysis in *all* situations in which the United States is seeking the data of a non-citizen located outside the United States and the relevant conditions apply, irrespective of any separate executive branch agreement on reciprocal notice and opportunity to object. Such a mechanism would ensure that the interests of foreign governments are considered, thus setting a precedent that the United States would want and expect other countries to engage in if accessing the data of U.S. citizens and residents. It would also address concerns about unbounded U.S. surveillance.

At the same time, it would protect the interests of the United States in getting access to data in serious cases. It would avoid giving foreign governments a right to access U.S. courts or hold up issuance of warrants in legitimate cases, and it would not in any way preclude the United States from negotiating the kind of agreements provided for in ICPA—requiring reciprocal notice and an

[22] S. 1671 § 3, 115th Cong. (1st Sess. 2017). Among other things, the Attorney General, in consultation with the Secretary of State, must determine that the foreign country "affords robust substantive and procedural protections for privacy and civil liberties" and "adheres to applicable international human rights statutes.

[23] *Id.* Additionally, the legislation fails to specify who is to be provided notice if the target is a foreign citizen of State A located in State B. Is it State B or State A or both?

opportunity to object—anytime the United States determines it is in its interest to do so.

In sum, Congress can and should step in now to ensure that the relevant interests are taken into account by adopting the kind of nuanced solution that Congress, not courts, is equipped to provide.

III. Foreign Government Access

The problem of foreign government access is the exact converse of the problem presented by the Second Circuit's ruling in the Microsoft Ireland case. It, too, has roots in the SCA, stemming from provisions that prohibit U.S.-based providers from disclosing communications content to foreign law enforcement.[24] This prohibition applies even if law enforcement is seeking the email account of a foreigner located outside the United States in the investigation of a solely foreign crime. Because U.S.-based providers now control so much of the world's data, and because so much information is now digitalized, this has become an increasingly potent problem for foreign law enforcement.

The Obama and Trump administrations have proposed almost identical legislation to begin to address the concerns of foreign governments.[25] The legislation would amend the SCA to permit foreign governments in specified circumstances to directly access the content of communications from U.S.-based providers. Specifically, it would permit the executive branch to enter into agreements with partner governments that would permit those governments to directly request specified communications content from U.S.-based providers, subject to a number of limitations.

The draft legislation includes three key sets of conditions on how these agreements would be operationalized:

First, there are limits on the kinds of countries that could be eligible for these expedited data-sharing agreements. Such agreements only would be permitted with respect to countries that have been certified by the Attorney General, in conjunction with the Secretary of State, as affording "robust substantive and procedural protections for privacy and civil liberties" with respect to data collection and the other activities subject to the agreement. This helps protect against foreign governments gaining access to data in order to harass or otherwise abuse.

Second, there are several procedural and substantive requirements that must be met regarding the substance of each request made pursuant to such a system.

- The partner government could *not* directly access the data of a U.S. citizen or legal permanent resident or any person located in the United States; those requests would still need to be made through the MLA process. This reflects the principle that U.S. law

[24] As with questions of a U.S. warrant's reach, there is an open question as to whether the SCA applies to all data held by U.S.-based companies or only data that happens to be located in the United States. According to the Second Circuit's reasoning, it would be the latter. *In re* Warrant to Search A Certain E-Mail Account Controlled and Maintained by Microsoft, 829 F. 3d. 197, 222 (2d Cir. 2016).
[25] Testimony by Downing, *supra* note 12.

should govern access to the data of U.S. citizens, legal permanent residents, and persons located in the United States. Conversely, U.S. law should not control foreign government collection of information on foreigners outside the United States, so long as the foreign government satisfies minimum procedural and substantive standards in the way it accesses, processes, and uses such data.

- Various measures are in place to further protect data of U.S. persons (defined to include citizens and legal permanent residents) and others in the United States: First, the foreign government could not target a non-U.S. person with the purpose of obtaining data concerning a U.S. person or other person located in the United States. Second, the foreign government would be prohibited from disseminating content of a U.S. person to a U.S. authority unless it relates to significant harm or threat of such harm to the U.S. or U.S. persons. Third, non-relevant data, including data of U.S. persons, must be sealed, segregated, and deleted.
- Requests must be particularized, lawful, and based on articulable and credible facts, and they must be reviewed or overseen by a court or other independent authority.
- Intercept orders must be of a fixed, limited duration, and permitted only when that same information could not be obtained by a less intrusive method.
- Acquired data must also be subject to minimization procedures, including requirements that non-relevant information be sealed, segregated, and deleted.
- Acquired data cannot be used to infringe freedom of speech.

Third, the draft legislation imposes accountability and review mechanisms. Specifically, agreements would be a maximum of five-years in duration, unless renewed. Partner governments must provide for periodic compliance reviews by the United States, and the United States reserves the right to rescind any aspect of the agreement for which compliance is lacking. The draft legislation also specifies that the U.S. must be granted a reciprocal right of access to foreign-held data.

This DOJ-proposed legislation is not perfect and would benefit from some modifications. Specifically, the legislation should explicitly require judicial "authorization" as opposed to "review or oversight" of compulsion orders for content. It should provide for enhanced accountability and transparency mechanisms, by, among other things, requiring governments to publish data on the number and type of requests made pursuant to these agreements. It should require partner countries to explicitly disavow data localization mandates. And it should provide an explicit mechanism that permits third-party providers to submit requests to the U.S. government for additional review if there are questions about whether or not the requirements are met, and protects them from foreign government compliance demands in the interim.

But it is, in general, an approach to be applauded, as I and numerous others have urged elsewhere.[26]

[26] *See, e.g.,* David Kris, *U.S. Government Presents Draft Legislation for Cross-Border Data Requests,* LAWFARE (July 16, 2016, 8:07 AM), https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests; Testimony,

It reflects the normative position that foreign governments should be able to access their own citizens' and nationals' data, so long as they abide by baseline requirements in how they access and manage data. And it lays out with specificity the procedural and substantive standards that are required, using U.S. leverage as the repository of so much of the world's data as an incentive for partner nations to comply. This is important. These are standards that ultimately protect U.S. persons in addition to their foreign counterparts with whom they are in communication. Meanwhile, it ensures that U.S. standards continue to apply to the direct collection of data from U.S. persons and residents.

The United States and United Kingdom reportedly have drafted an agreement that comports with these requirements, although the agreement cannot be implemented until the U.S. Congress first amends the SCA to permit these types of agreements to go forward. Some have objected to this agreement on the grounds that it would permit foreign governments to bypass the mutual legal assistance process. In particular, some have expressed concern that these agreements permit access upon a showing of a "reasonable justification based on articulable and credible facts," as compared to the "probable cause" standard that is now demanded when a U.S. warrant is obtained.[27] As an initial matter, it is not obvious that the "reasonable justification based on articulable and credible facts" standard is in fact lower than—and certainly not significantly lower than—that of probable cause.[28] But even if the critics are correct, it is not clear why the United States should insist on imposing its particular and idiosyncratic probable cause standard, so long as sufficient substantive and procedural standards are in place. Continued insistence on the probable cause standard—a standard that makes little sense to the rest of the world—is likely to doom such agreements, thus further feeding the incentives for data localization mandates and other surreptitious means of

---

Brad Smith, *supra* note 15; Walker, *supra* note 15; Tiffany Lin & Mailyn Fidler, *Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K Agreement* 8, Berkman Klein Center for Internet & Society (Sep. 7, 2017) (concluding that, despite concerns, "the proposed legislation could be a huge step forward in updating an outdated system that was not designed for the today's technological paradigm and was not built for such a high volume of requests"), http://nrs.harvard.edu/urn-3:HUL.InstRepos:33867385. Jennifer Daskal & Andrew K. Woods, *Congress Should Embrace the DOJ's Cross-Border Fix,* JUST SECURITY (Aug. 1, 2016, 8:03 AM), https://www.justsecurity.org/32213/congress-embrace-dojs-cross-border-data-fix/; *Facilitating Cooperation and Protecting Rights: Hearing on Law Enforcement Access to Data Stored Across Borders Before the Subcomm. On Crime and Terrorism of the S. Comm. on the Judiciary*, 115th Cong. (2017) (statement of Jennifer Daskal), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Daskal%20Testimony.pdf. *See* Peter Swire and Deven Desai, *A 'Qualified SPOC' Approach for India and Mutual Legal Assistance*, LAWFARE (Mar. 2, 2017, 12:14 PM), https://www.lawfareblog.com/qualified-spoc-approach-india-and-mutual-legal-assistance (suggesting a mechanism for expanding agreements to a wider range of countries).

[27] See, e.g., Center for Democracy & Technology, "Cross-Border Law Enforcement Demands: Analysis of the US Department of Justice's Proposed Bill" (Aug. 17, 2016), https://cdt.org/files/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf; ACLU, Amnesty International, and HRW Letter Opposing Department of Justice Proposal on Cross Border Data Sharing (Aug. 9, 2016), https://www.aclu.org/letter/aclu-amnesty-international-usa-and-hrw-letter-opposing-doj-proposal-cross-border-data-sharing.

[28] See, e.g., U.S. v. Ortiz, 669 F.3d 439, 446 (4th Cir. 2012) (probable cause requires nothing more than a "reasonable ground"—which is "less demanding than a standard requiring a preponderance of the evidence for the belief"); Illinois v. Gates, 462 U.S. 213, 231-32 (1983) (defining probable case as a "practical, non-technical standard" that turns on the "assessment of probabilities") (citations omitted).

accessing data. If that happens, the United States will have *no* say in the standards that are applied.

Critics also worry that there are insufficient protections for U.S. person information.[29] But this critique fails to account for the significant protections in place for U.S. person information, including the limits on both direct and indirect targeting of U.S. person information, the restrictions on dissemination of U.S. person information, and the auditing that is required. And it too reflects a misguided assumption that the status quo is permanent. If we instead move to a world in which foreign governments access such data unilaterally (either via data localization mandates, extraterritorial claims that prevail, or surreptitious means) *none* of these protections for U.S. person data will be put in place.

Importantly, the legislation reflects an attempt by the United States to use its current leverage as the home for so much of the world's data to insist on—and ideally raise—baseline substantive and procedural baseline protections. And in fact, the interactions with the U.K. suggest that such benefits are possible. As the negotiations over this draft agreement were ongoing, the U.K. government passed new legislation that, for the first time in U.K. history, provides for judicial oversight of warrants for communications content.[30] The U.K. government reportedly endorsed such judicial review provisions because, among other reasons, it wanted to meet the judicial review standards demanded by the United States.

In sum, the draft legislation is something that should be pursued, albeit with some improvement. It relies on the United States' unique position as the home of the world's largest tech companies to set baseline substantive and procedural standards governing the collection of data, ideally helping to elevate the standards that apply. The generation of such standards will ultimately inure to the benefit of U.S. citizens and residents that may be subject to foreign government collection of their data. But this is a time-limited opportunity. As foreign-based service providers gain increasing shares of the market, and foreign governments successfully impose data localization mandates, foreign governments will be able to access sought-after data locally without ever having to make cross-border requests to the United States. The United States then will have little to nothing to say about the standards that apply, even with respect to the U.S. person data that is stored in foreign jurisdictions and either directly or incidentally collected by foreign governments. This would be an unfortunate result.[31]

Conclusion

Governments increasingly need digital evidence that is located across borders in the investigation of

[29] *See* ACLU, Amnesty International, and HRW, Letter, *supra* note 26.
[30] *See* Investigatory Powers Act 2016 c. 25 (Eng.), § 23, http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf. While the legislation has been defined as a "snoopers charter" that authorizes broad-based surveillance the addition of judicial review procedures is an example of an additional *check* on U.K. authorities that had not previously been in place. *Id.*
[31] For a more in-depth analysis of this issue, *see* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues,* 8 J. NAT'L SECURITY L. & POL'Y 473 (2016).

local crime. The rules have not yet caught up to that reality. Congress has a critically important role to play in revising those rules, and doing so in a way that accommodates the relevant security, privacy, sovereignty, and economic interests at stake. This is not an issue that should be delegated to the Supreme Court, which is not in the position to address the complicated interests at stake with the kind of nuance they deserve. Several judges and other commentators have urged the same.[32] The time to act is now.

About the Author

Jennifer Daskal is an Associate Professor of Law at American University Washington College of Law, where she teaches and writes in the fields of criminal, national security, and constitutional law. From 2009-2011, she was counsel to the Assistant Attorney General for National Security at the Department of Justice. Prior to joining DOJ, Daskal was senior counterterrorism counsel at Human Rights Watch, worked as a staff attorney for the Public Defender Service for the District of Columbia, and clerked for the Honorable Jed S. Rakoff. She also spent two years as a national security law fellow and adjunct professor at Georgetown University Law Center, and was recently the recipient of an Open Society Institute Fellowship to work on issues related to privacy and law enforcement access to data across borders. Daskal has published op-eds in *The New York Times*, *Washington Post*, and *International Herald Tribune*, and has appeared on BBC, C-Span, MSNBC, and NPR, among other media outlets. She is an Executive Editor of and regular contributor to the Just Security blog. Daskal is a graduate of Brown University, Harvard Law School, and Cambridge University, where she was a Marshall Scholar.

About the American Constitution Society

The American Constitution Society (ACS) believes that law should be a force to improve the lives of all people. ACS works for positive change by shaping debate on vitally important legal and constitutional issues through development and promotion of high-impact ideas to opinion leaders and the media; by building networks of lawyers, law students, judges, and policymakers dedicated to those ideas; and by countering the activist conservative legal movement that has sought to erode our enduring constitutional values. By bringing together powerful, relevant ideas and passionate, talented

[32] *In re* Warrant to Search A Certain E-Mail Account Controlled and Maintained by Microsoft, 829 F.3d at 222 (2d Cir. 2016) (Lynch, J., concurring (emphasizing the "the need for congressional action to revise a badly outdated statute"); *In re* Warrant to Search A Certain E-Mail Account Controlled and Maintained by Microsoft, 855 F.3d at 55 (2d Cir. 2017) (Carney, J., concurring in the order denying rehearing en banc) (arguing that the SCA is "overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose"); Brad Smith, *U.S. Supreme Court will hear Petition to Review Microsoft Search Warrant Case While Momentum to Modernize the Law Continues in Congress*, MICROSOFT ON THE ISSUES (Oct. 16, 2017), https://blogs.microsoft.com/on-the-issues/2017/10/16/us-supreme-court-will-hear-petition-to-review-microsoft-search-warrant-case-while-momentum-to-modernize-the-law-continues-in-congress/; Kent Walker, *Digital security and due process: A new legal framework for the cloud era*, GOOGLE BLOG (June 22, 2017), https://www.blog.google/topics/public-policy/digital-security-and-due-process-new-legal-framework-cloud-era/. *See also* Jennifer Daskal, *There's No Good Decision in the Next Big Data Privacy Case*, N.Y. TIMES (Oct. 18, 2017), https://www.nytimes.com/2017/10/18/opinion/data-abroad-privacy-court.html

people, ACS makes a difference in the constitutional, legal, and public policy debates that shape our democracy.

All expressions of opinion are those of the author or authors. The American Constitution Society (ACS) takes no position on specific legal or policy initiatives.