Whose Law Governs in a Borderless World?
Law Enforcement Access to Data Across Borders

by Jennifer Daskal

UK law enforcement agents are summoned to the scene of what appears to be the murder of a well-loved schoolteacher from the outskirts of London. It is not thought to be terrorism-related or high profile in any significant way. But it matters enormously to the community, her family, and the many current and former students who adored her. The victim's ex-husband, John, is the prime suspect. Law enforcement authorities act quickly and get a warrant for John's stored emails. They serve the warrant on Google, the provider of his Gmail account, but are told: "Sorry, we are prohibited by U.S. law from turning over the content of communications to foreign governments. You need to make your request directly to the U.S. government." They do, employing what is known as the Mutual Legal Assistance (MLA) process. It takes an average of ten months to get a response. Were John using Virgin Media, or any other U.K.-based email service provider, the authorities would be able to access the data within days, if not sooner.

Around the same time, U.S. law enforcement officials receive a credible tip that an American and two French men living in Brooklyn, New York, are plotting an attack on the Empire State Building. The two French men have Microsoft Outlook accounts. The FBI obtains a warrant to access those accounts, but soon learns that the emails are stored in a datacenter in Ireland. As a result, the U.S. warrant has no force, and the FBI must make a diplomatic request for the data to the Irish government—also waiting months, if not longer, for a response.

In both of these situations, law enforcement's ability to access digitalized evidence turns on where the data is held, or presumed to be held. Many other potentially relevant facts—including the location of the target of the investigation, the location of the victim, or the location of the crime—are deemed irrelevant.

It is an approach that reflects a straightforward, and misguided, application of the rules that apply to data's tangible counterparts.[1] If the investigation of a transnational drug crime generates U.S. law enforcement interest in an alleged drug lord across the Mexican border, U.S. agents cannot unilaterally go and search the drug lord's Oaxaca home—even if they were to somehow convince a U.S. court to issue a warrant to do so. Rather, they must either enter into a joint investigation with Mexican agents or ask Mexican law enforcement to do it for them. This

[1] By use of this terminology, I do not mean to suggest that data lacks a physical presence or weigh into the debates about whether data is "tangible" or "physical" property covered by insurance contracts. *Compare* America Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 96 (4th Cir. 2003) (concluding that data is intangible property and thus not covered by insurance contract) *with* Landmark Amer. Ins. Co. v. Gulf Coast Analytical Labs., 2012 WL 1094761, at *4 (M.D. La. Mar. 30, 2012) (concluding that, although electronic data is intangible, it "has physical existence, takes up space on the tape, disc, or hard drive, makes physical things happen, and can be perceived by the senses" and is therefore "physical" for purposes of insurance coverage). Rather, I merely use the word to distinguish data—which, apart from the devices or data centers that hold it, is not something that can be touched or physically manipulated—from other kinds of property.

makes intuitive sense. Consider a world in which foreign law enforcement officials were given free rein to unilaterally enter into the country and rifle through our homes. Most of us would deem that creepy—and a violation of both U.S. sovereignty and our individual privacy.

But there are several reasons why the simple translation of the traditional rules governing searches and seizures to the world of digital evidence does not make good sense. There are, after all, key—and highly relevant—distinctions between digitalized evidence and its more tangible counterparts. Our failure to adequately account for these differences is having increasingly negative consequences for our security, our privacy, and our economy.

The following highlights the unique features of data, explains why they matter, and suggests a new approach to law enforcement jurisdiction that turns on factors other than the location of the sought. It reflects the understanding that the location of data often is totally unrelated to the key sovereign interests at stake—interests such as regulating access to their own citizens' and residents' data, accessing data critical to the investigation of serious crime, and regulating the corporations that do business in their territory. And it suggests a jurisdictional rule that more closely hews to the relevant interest at stake.

The good news is that a growing number of governments, including the U.S., U.K., European Union, and E.U. Parliament, are already recognizing the negative—and ultimately privacy- and security-reducing—effects of the status quo. These governments are seeking new, and cooperative, ways to access data across borders. This should be encouraged.

How Data is Different

Data can cross international borders almost instantaneously. It can be copied and held in multiple jurisdictions simultaneously. It can be divided or partitioned. Even a single email is broken up into distinct packets as it transits from one place to a next; the various packets might not all travel the same route; the email itself is only deliverable and decipherable when all of the packets reunite and are reassembled. Larger databases may be partitioned into several parts, each part stored in a different location, with the relevant information only available when reassembled and combined by a user accessing the various parts. Moreover, the growth of the cloud means one can access data remotely; data users often are located in geographically distinct places from the data that they are accessing.

Data thus differs from its more tangible counterparts in at least three salient ways: its rapid mobility; its divisibility; and its location independence from the person using or manipulating it. These features matter to how data is searched and seized and to the practical and normative salience of data location to the rules governing law enforcement jurisdiction.

1. The Search or Seizure

The unique properties of data mean that law enforcement agents—or their proxies—do not need to step foot on another country's soil in order to access sought-after digitalized evidence

that is located across an international border. Rather, they do so remotely.[2] As a result, the only thing that is crossing international lines is a bunch of ones and zeros (through binary code), not any actual law enforcement agent or private sector employee acting at their behest. This eliminates, or at least alters, the very visible sovereignty violation that occurs if, say, Russian law enforcement officials were to knock down a Chicago resident's door.

Moreover, whereas the searching and seizing of more tangible evidence generally deprives the property owner of at least temporary use of his or her property, the search and seizure of digital communications generally leaves the data owner's ability to access and use his or her data intact. It leaves the host country's ability to also access it unaffected as well. This has led some to question whether the copying of data is even a seizure.[3] At the very least it diminishes the *nature* of the intrusion from the perspective of both the user and the state where the data is located. There is, of course, still a privacy intrusion. But it is a *different* kind of intrusion than would result if foreign law enforcement unilaterally carted away physical evidence across the border, thus depriving the owner of its use, or the state the ability to access it.[4]

2. Ease of Evasion

In contrast to tangible property, electronic data can transit such borders almost instantaneously. Moreover, these movements can be remotely dictated and controlled. This creates the possibility that savvy individuals in one jurisdiction could restrict or evade law enforcement simply by moving their data to another jurisdiction. This is both a virtue and a vice. The ability to evade detection can be critical to protecting human rights activists or dissidents. But it also can create a safe haven for criminal activity—permitting bad actors to move their data out of the relevant law enforcement agents' reach, even if they themselves fall within the law enforcement's jurisdiction.

3. Localization Mandates

---

[2] This assumes that law enforcement is only seeking the data and not the device (e.g., a computer or smart phone) that the target uses to send or receive messages. Efforts to access the device itself would trigger the same considerations and rules that apply to other tangible property.

[3] *See, e.g.*, United States v. Gorshkov, 2001 WL 1024026, at *3 (W.D. Wa. May 23, 2001) (concluding that remote copying of data was not a seizure because it did not interfere with anyone's possessory interest in the data).

[4] Arguably, the invisibility of the intrusion makes it more troubling. Whereas one is on notice if law enforcement agents break down his door and cart away his property, there is something deeply unsettling about the idea that law enforcement agents and companies that manage our data can snoop on us without any of us knowing. And in fact there is a large literature about the chilling effects and negative consequences of such a surveillance society. *See, e.g.*, DANIEL SOLOVE, UNDERSTANDING PRIVACY (2008); Danielle Citron & David Gray, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Neil Richards, *The Dangers of Surveillance,* 126 HARV. L. REV. 1394 (2013); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000). But the point here isn't to catalog or rank the harms; rather, I merely seek to highlight the ways in which digitalized evidence is different.

Because data can be copied and duplicated with incredible speed and relative ease, data localization requirements, pursuant to which a copy of certain categories of data must be held locally, become both a possible and appealing way of responding to concerns about evasion and guaranteeing local law enforcement access. Such requirements are proliferating. Russia recently passed a high-profile data localization law.[5] Data localization mandates have or have been actively pursued in multiple other locations as well, including Indonesia,[6] Vietnam,[7] and numerous other locations.[8] A jurisdictional rule that turns exclusively on data localization helps fuel such localization efforts.[9]

Such data localization requirements are costly to the economy, to the growth of the Internet, and ultimately to privacy. Among the many concerns, localization requirements can price smaller businesses and start-ups out of the international market. It costs millions of dollars annually to rent space in a data center and billions to build one; this is not something that small companies can afford. Such requirements also undercut the ability of data to flow in the most efficient manner, Moreover, by enabling local law enforcement to access the data pursuant to their own local standards, they threaten privacy protections that might otherwise apply. From the U.S. perspective, data localization means the loss of any say over the substantive and procedural standards that apply to the foreign government's ability to access data that was formally subject to U.S. control. In most situations, foreign government rules governing law enforcement access to data will be less privacy protective than the U.S. standard of a warrant based on probable case, reviewed by an independent judge.

---

[5] *See, e.g.*, Sergei Blagov, *Russia's 2016 Data Localization Audit Plan Released*, BLOOMBERG LAW (Jan. 13, 2016), http://www.bna.com/russias-2016-data-n57982066291/.

[6] *See* Regulation of the Government of the Republic of Indonesia, Number 82 of 201, Art. 17(2) (specifying that a range of providers operating in Indonesia are "obligated to put the data center and disaster recovery center in Indonesian territory *for the purpose of law enforcement, protection, and enforcement of national sovereignty to the data of its citizens*") (emphasis added), http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html.

[7] Decree on Management, Provision and Use of Internet Services and Online Information arts. 24(2), 25(8), 28(2) (No. 72/2013) (Viet.) (requiring organizations establishing general websites, information service providers, and those establishing "social networks" to have "at least 01 server system in Vietnam *serving the inspection, storage, and provision of information at the request of competent authorities")* (emphasis added), http://www.moit.gov.vn/Images/FileVanBan/_ND72-2013-CPEng.pdf.

[8] *See* Anupam Chander & Uyên P. Lê, Data Nationalism, 64 EMORY L.J. 677, 694-708 (2015) (documenting data localization trends); Albright Stonebridge Group, Data Localization: A Challenge to Global Commerce and the Free Flow of Information (Sept. 2015).

[9] This, however, isn't the sole source of the localization push. The E.U.'s newly enacted General Data Protection Regulation, for example, which is set to go into effect in May 2018, limits the transfer of personal data, absent a determination of adequate personal data protection. *See* Regulation (E.U.) 2016/679. While the provision operates as a de facto data localization measure, it appears to be motivated by a desire to protect E.U. citizens' data, rather than an effort to ensure law enforcement access. A separate directive similarly sets conditions on when data can be transferred out of the E.U. for law enforcement purposes. *See* Directive (E.U.) 2016/680.

3. Location Independence

When the average user accesses a Google Doc, a web-based email account, or other data stored in the cloud, the user generally has no idea where his or her data is being stored.[10] Rather, these are decisions that are generally delegated to the company or app providing the relevant service to the user. The user may not have any connection to the jurisdiction where his or her data is being held, other than the fact that her data happens—due to the choice of a third-party provider—be held there. This is a very different situation than applies when one purchases a home or selects a particular safety deposit box to store one's belongings. In such a situation, one generally makes an active, conscious choice about location. At a minimum, one generally knows where one's property is located, and thus is on notice of the rules that govern law enforcement access.[11]

This lack of notice—or any control as to the rules that apply—raises normative concerns that should be taken into account. Why should the data of a U.S. citizen, who works and lives in the United States, be subject to Irish law enforcement rules simply because her email service provider moved her data there? In most cases, the user will not even know, let alone have any say, as to what jurisdictional rules govern. The user will thus have no ability to contest the applicable rules. Conversely, why should a government lose jurisdiction over data simply because it is being moved across borders for temporary processing reasons? In many cases, the location of data may be totally disconnected from any of the relevant equities at stake.

The Stickiness of Data Location as a Jurisdictional Hook

Despite data location being a particularly poor basis for defining and delimiting law enforcement jurisdiction, it is an approach with bite. The Second Circuit, in what is known as the *Microsoft Ireland* case, entrenched the importance of data location when determining the reach of U.S. warrant authority.[12] And blocking provisions in the Stored Communications Act prohibit foreign law enforcement from directly compelling the content of communications that are U.S.-held. Both raise concerns.

1. The *Microsoft Ireland* Case

The dispute dates back to December 2013, when Microsoft refused to comply with a warrant issued pursuant to the Stored Communications Act (SCA) ordering the production of

[10] This could theoretically change. Companies could be required, either as a matter of law or as a result of consumer demand, to provide notice and opt-out provisions regarding data location. But for most companies this would be both a costly and highly inefficient way of managing data. And most users would not likely have the bandwidth or interest in effectively monitoring the location of their data.

[11] Of course, in many situations such rules are opaque and/or unknown by the user. But at least one is on *notice* as to which nation has law enforcement jurisdiction over one's property and thus which nation's rules apply.

[12] *See In re* Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft, 829 F. 3d. 197 (2d Cir. 2016), *rehearing en banc denied, In re* Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft, 2017 WL 262765 (Jan. 24, 2017).

certain emails. The emails were held in a data center in Dublin, Ireland. Microsoft claimed that SCA warrants only have territorial effect, that the data was located extraterritorially, and that therefore the warrant was invalid. The government fought back. The government emphasized that that the data was under the control of Microsoft, a U.S.-based company; that the data could be accessed by Microsoft employees located in the United States; and that therefore it was a territorial, not extraterritorial assertion of governmental authority.

Although the magistrate and district court judges sided with the government, the Second Circuit reversed.[13] The court concluded that the location of *data*, rather than the location of the provider accessing the data—or any other factor—determined the reach of the U.S. warrant authority under the SCA. Concurring Judge Gerald E. Lynch wrote separately to emphasize the "need for congressional action to revise a badly outdated statute"—namely the SCA.[14] In January, a divided court declined by a 4-4 vote, to rehear the case en banc. The denial prompted 55 pages of discussion, with each dissenting judge writing separately to explain the flaws in the panel court's decision. Each of these judges also concurred in the need for Congress to step in.[15]

As a result of the ruling, U.S. law enforcement cannot directly compel the production of the content of communications that are stored outside the United States, even if they are investigating a U.S. citizen in connection with a local crime.[16] Rather, U.S. law enforcement must make a diplomatic request for such data, employing the time-consuming and highly inefficient MLA process. It takes many months, if not longer, for most countries to respond. In some cases, there is no functioning MLA system and foreign nations may not respond at all.

2. The Blocking Provisions in the Stored Communications Act

Conversely, U.S. law imposes its own limits on foreign governments seeking to access U.S.-held data. Specifically, the SCA blocks foreign government access to stored communications content that is U.S.-held—even if the only U.S. nexus to the data is that it happens to be located within the United States or held by a U.S. company. [17] While providers can

[13] *Id.*

[14] *Id*. at 222.

[15] , *In re* Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft, 2017 WL 262765 (Jan. 24, 2017). *See also* Jennifer Daskal, *Congress Needs to Fix our Outdated Email Privacy Law*, SLATE (Jan. 26, 2017, 1:17 pm), http://www.slate.com/articles/technology/future_tense/2017/01/the_confusing_court_case_over_microsoft_data_on_servers_in_ireland.html.

[16] Even though the opinion is only binding in the Second Circuit, tech companies indicate that they are treating it as if it had nation-wide application, much as was done in the wake of the decision in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), which requires, as a matter of constitutional law, that the government obtain a warrant based on probable cause to compel the production of stored communications content, despite statutory rules that do not require a warrant in all such situations.

[17] The statute does not specify whether its prohibitions apply to all data that is held in the United States, all data that is held by a U.S.-based company, regardless of the location of the data, or both. Whereas the Second Circuit's decision suggests that it is the former—applying based on where the data is located,

(and in fact must) respond to U.S.-issued warrants, they may not turn over the content of communications to a foreign government official, even pursuant to a lawfully issued foreign production order.[18]

As a result, foreign governments must employ the MLA process and make a diplomatic request for all U.S.-held communications content. The process is laborious and time-consuming. The Department of Justice first reviews the request; if approved, it is sent to a U.S. Attorney's office; the U.S. Attorney's office must get a U.S. judge to sign-off on the warrant; the warrant is then served on the provider; any responsive data is then routed back through the U.S. Attorney's office, to the Department of Justice, and back to the foreign government. It takes an average of ten months to complete, and in many cases much longer.[19]

Foreign governments are understandably frustrated. Why should they have to get a U.S. warrant based on a U.S. standard of probable cause when they are investigating a local crime, local target, and local victim? Of additional concern to many foreign governments, there is *no* mechanism for foreign governments to obtain real-time communications either. The only way to lawfully obtain that data for law enforcement purposes is to open a joint investigation with U.S. law enforcement, but that is obviously not possible with respect to the investigation of local crimes. Thus, if foreign law enforcement is investigating its own locally-based nationals that happen to be using Google's G-chat or another U.S.-controlled messaging service, it has no way to lawfully monitor the chat or obtain in real-time the associated transactional data, such as address and location information.[20]

---

companies like Facebook and Google have long maintained the fiction that all of their data is U.S.-held and thus governed by the statutory requirements, given that it is accessed and controlled from within the United States.

[18] The SCA prohibits providers from turning over the content of communications, except in a limited number of situations. *See* 18 U.S.C. §§ 2702; 2703(a). 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). Thus, foreign governments don't qualify.

[19] *See, e.g.*, The President's Review Grp. on Intelligence and Communication Technologies, *Liberty and Security in a Changing World*, White House 226-229 (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. Moreover, now, as a result of the Microsoft Ireland case, the United States can only be of assistance if the data is, in fact, located within the territory of the United States. In some cases, that means there *no* jurisdiction that has the authority to compel production of access the data.

[20] *See, e.g.*, Council of Europe Cyber Crime Committee (T-CY), *Criminal justice access to evidence in the cloud: Recommendations for consideration by the T-CY*, Final Report of the T-CY Evidence Group (Sept. 16, 2016), at 8 (highlighting the inability of US authorities to obtain content in real-time for foreign authorities), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

Foreign governments are, as a result, increasingly seeking to circumvent this system in a number of concerning ways. As already stated, these include data localization mandates; unilateral assertions of extraterritorial jurisdiction, which create obvious conflict of law problems;[21] and use of other surreptitious means of accessing sought-after data that exploit and potentially introduce vulnerabilities into the system.

* *

Notably, these location-based limits, at least under U.S. law, apply to the content of communications, only. Non-content, including IP address, time and duration of sessions, and even the to/from lines of stored emails, is subject to different rules. Thus, foreign governments can directly demand the production of non-content information directly from U.S.-based providers. And in fact, foreign governments make tens of thousands of requests on U.S.-based providers each year. Similarly, a range of communications information obtainable by subpoena—including IP address, time and duration of sessions, and billing information—is not directly covered by the ruling in the *Microsoft* case. At least one line of cases suggests that this information can be obtained by U.S. law enforcement officials, regardless of where they are stored.[22]

These distinctions stem from the longstanding assumption that governmental access to communications content constitutes a greater invasion of privacy than access to non-content information, or "metadata." There are reasons to question the stark difference in the way content and metadata is treated under the law; after all, so-called metadata can reveal an enormous amount about one's activities and associations. And in fact this has led some to suggest that the rules governing metadata should be made more equivalent to the rules governing content.[23] But while there may be good reason to strengthen protections for metadata, the kind of location-based jurisdictional limits that have been adopted for content are not the way to do so.

A New Approach

A new approach is needed. Jurisdiction over data should turn on a combination of factors, with location and nationality of the *target* replacing the location of *data* as a key factor. This reflects the normative principle that governments should be able to set the privacy protections (and thus rules governing law enforcement access) for their own nationals and persons living within their borders. It also a normative principle—one grounded in principles of both democratic accountability and due process—that individuals should have some notice and at least some choice as to the rules that apply. Whereas individuals are on notice as to laws,

---

[21] In January 2015, for example, a Microsoft executive was arrested and criminally charged for his failure to produce data requested by Brazilian authorities; U.S. law—namely the Stored Communications Act—barred him from doing so. *See* Brad Smith, *In the Cloud We Trust*, MICROSOFT / STORIES, http://news.microsoft.com/stories/inthecloudwetrust/.

[22] *See, e.g.*, United States v. Bank of Nova Scotia, 740 F.2d 817 (11th Cir. 1984); Marc Rich v. United States, 702 F.3d 663 (2d Cir. 1983).

[23] *See, e.g.*, Greg Nojeim, *MLAT Reform Proposal: Protecting Metadata*, LAWFARE (Dec. 10, 2015, 2:43 pm), https://www.lawfareblog.com/mlat-reform-proposal-protecting-metadata.

including those governing law enforcement access of the place where they are located, they often have no say over and no ability to effectively monitor where their third party provider holds their data at any given moment.

Additional factors should also matter, including the location of the provider, the nature of the crime, and the strength of the government's interests in the data. But the evaluation of these factors should take into account the countervailing interests of foreign states in regulating access to their own residents' and nationals' data. Those interests should generally be respected, so long as the foreign government adheres to baseline substantive and procedural protections in the ways in which they access that data.

Of course, it will not always be possible to determine target location. And it will be even harder to determine target nationality in many cases. A set of presumptions will be needed to operationalize this kind of rule. But it seems that a jurisdictional rule that takes into account target location and nationality makes much more practical and normative sense than one which turns exclusively on data location.

The following focuses on how this approach would play out with respect to the two areas discussed above—the reach of U.S. warrant authority, and the ability of foreign governments to access U.S.-held communications content. Importantly, any shifts in the law and policy should be made with care, so as to ensure the kind of leveling up, rather than leveling down, of the privacy protections that might otherwise result.

U.S. Access to Extraterritorially Located Data

Congress should, as multiple Second Circuit judges have now urged, amend the SCA to clarify the reach of the United States' warrant authority for data that is located extraterritorially. In doing so, it should pursue rules that mirror those that it expects others to employ with respect to data that is U.S.-held.

The legislation should effectively reverse the Second Circuit ruling by specifying that U.S. law enforcement is, as a general matter, able to compel, via a warrant based on probable cause, U.S.-based providers to disclose communications content within their custody or control, regardless of where the data is located. But Congress also should ensure that the countervailing interests of sovereign states in regulating access to the data of their own citizens and residents are taken into account. Specifically, it should specify that if the warrant targets a non-U.S. person (meaning not a citizen or legal permanent resident) located outside the United States, the reviewing court *must* take into account potential foreign governments' interests—effectively requiring as a matter of statute what is now done by courts as a matter of discretion. In cases of conflict, the U.S. government should be required to make a mutual legal assistance request for the data, absent a finding of an urgent need for the data and the absence of a workable alternative for accessing the data in a timely matter.

Such an approach reflects the notion that the United States should be permitted to access, pursuant to valid warrants, the stored communications of its citizens and residents in the investigation of criminal activity, regardless of where the data is located. This offers both a shield and a sword—ensuring that the relatively robust warrant requirement applies when the law

enforcement seeks the data of U.S. citizens and residents and guaranteeing that the government can access that data when the warrant standard is met. Such an approach also reflects the view that governments have a sovereign interest in controlling access to data of their citizens and residents—and that these interests need to be taken into account. Conversely, they do not have a strong sovereign interest in controlling access to data that just happens to be held in their jurisdiction, absent some other territorial nexus between the data and the host state.

Blocking Provisions in the SCA

The United States also should amend the SCA to permit foreign governments—in specified circumstances—to directly access the content of communications from U.S.-based providers. Notably, the Department of Justice has already proposed legislation to that effect.[24] It would amend ECPA to permit the executive branch to enter into agreements with partner governments; the agreements 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 as to 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. Similarly, it could not use this system to indirectly target U.S. persons, either on its own or at the behest of U.S. government officials. Again, this reflects the principle that U.S. law 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.

[24] The draft legislation is available here: https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p1; *see also* Jennifer Daskal & Andrew Woods, *Congress Should Embrace the DOJ's Cross-Border Fix,* JUST SECURITY (Aug. 1, 2016), https://www.justsecurity.org/32213/congress-embrace-dojs-cross-border-data-fix/; David Kris, *U.S. Government Presents Draft Legislation for Cross-Border Data Requests,* LAWFARE (July 16, 2016), https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests; Jennifer Daskal, Statement before the Judiciary Committee, U.S. House of Representatives, *Hearing on International Conflicts of Law Concerning Cross-Border Data Flow and Law Enforcement Requests* (Feb. 25, 2016), https://www.justsecurity.org/wp-content/uploads/2016/02/WrittenStatement-Daskal-HouseJudiciary-022516.pdf.

- 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 to protect, among other things, against the dissemination of U.S. person information.

- 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-year 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.

The DOJ-proposed legislation is not perfect, and would benefit from some modifications as it goes through the legislative process. Specifically, the legislation should require judicial "authorization" as opposed to "review or oversight." It should require foreign partners to disavow mandatory localization measures. And it should provide for enhanced accountability and transparency mechanisms, by, among other things, giving Congress a greater say in which countries qualify to enter into these kind of agreements and by requiring governments to publish data on the number and type of requests made pursuant to these agreements.

But it is in general an approach to be applauded. 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 communications. Meanwhile, it ensures that U.S. standards continue to apply to the direct collection of U.S. person and U.S. resident targets.

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. At around the same time as these negotiations, the UK government passed new legislation that, for the first time in U.K. history, provides for judicial oversight of warrants for communications content.[25] The U.K. government reportedly endorsed

[25] *See* Investigatory Powers Act 2016 c. 25 (Eng.), § 23, http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf
The legislation has been labeled a "snoopers' charter" and is likely to be subject to ongoing court challenge. But while there are many parts of the legislation that expand and authorize broad-based surveillance, the addition of judicial review procedures is an example of an additional *check* on UK authorities that had not previously been in place.

such judicial review provisions because it, among other reasons, wanted to be able to meet the standards demanded by the United States as a precondition for benefiting from this type of agreement.

In sum, legislation uses the United States' unique position as the home of the world's largest tech companies, and thus a significant share of the world's data, to specify baseline substantive and procedural standards governing the collection of data—ideally helping to elevate the standards that apply. These are critical protections that, among other things, will ultimately inure to the benefits of U.S. citizens and residents that may be subject to foreign government collection of their data. At some point, however, this U.S. leverage will be lost. As foreign-based 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. [26]

Conclusion

Data can move around the world almost instantaneously; can be divided and held in multiple locations at once; and can be remotely accessed hundreds of thousands of miles from where it actually resides. Yet our rules governing law enforcement access to data generally treat the location of data as the key, and sole determinant, of jurisdiction. The Second Circuit recently ruled that the U.S. warrant authority under the SCA does not extend to data located outside the United States. And the same statute prohibits direct foreign law enforcement access to U.S.-held data, even in situations when the *only* U.S. nexus is that the relevant data happens to be held in the United States. This makes little practical or normative sense—and ultimately has negative consequences for our security, privacy, and economy. Among the many concerns, the current state of affairs is incentivizing data localization requirements as a means of ensuring local governmental access to data, as well as the use of other surreptitious means of accessing sought after data.

It is time to shift the focus away from data location, and toward a range of factors that better reflect the sovereign, security and privacy interests at stake. In particular, target location and nationality should replace data location as key bases for determining law enforcement jurisdiction over data. Additional factors such as the location of the provider and strength of the government's interest in the data should also be taken into account. Two key changes to the SCA would begin to make that shift. First, Congress should expand the reach of the U.S.'s warrant authority to cover U.S. persons and residents wherever located and otherwise ensure U.S. law enforcement access—pursuant to a warrant based on probable cause—to sought-after data in a timely manner. Second, Congress should amend the provision of the SCA that categorically bars foreign governments from accessing sought-after communications content from U.S. providers.

---

[26] 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 __ (forthcoming 2016).

It should permit partner governments direct access to data of foreign nationals outside the United States, pursuant to baseline procedural and substantive standards and detailed agreements spelled out by the executive branch. This would help to stave off data localization requirements, conflicting assertions of jurisdiction, and other surreptitious means of accessing data—and raise the applicable standards in the process. As home to such a significant quantity of the world's data, the U.S. is in a unique position to set the applicable standards and rules. But U.S. leverage in this space will not last forever. The time to act is now.