How Law Enforcement Should Access Data Across Borders

BY ALAN MCQUINN AND DANIEL CASTRO | JULY 2017

The methods that law enforcement use to access data outside their jurisdiction are outdated, and if left unaddressed, risk damaging international comity, U.S. competitiveness, and the global Internet economy.

In late 2013, U.S. federal law enforcement officials obtained a warrant as part of an anti-narcotics investigation to seize the contents of an email account belonging to a Microsoft customer whose data the company stored in Dublin, Ireland.[1] Microsoft refused to comply with the order, arguing that the U.S. government cannot force a private party to do what U.S. law enforcement has no authority to do itself: use a warrant to conduct a search and seizure operation on foreign soil.[2] This case exposed the cracks in the foundation of the current framework used by law enforcement agencies to access digital information and determine jurisdiction on the Internet. Moreover, attempts to resolve this dispute risk either hamstringing law enforcement efforts or distorting the global marketplace for digital services. This report explains the problems with the status quo, describes the limitations of existing proposals, and offers an alternative framework to resolve these issues along with a set of recommendations to operationalize this framework not just within the United States, but globally.

No matter how the courts ultimately decide the Microsoft case or related ones, there are potentially negative implications for U.S. technology competitiveness and the U.S. economy overall. If the court rules for the government and declares that U.S. companies must provide access to data stored abroad, it will create two problems. First, it could hurt the competitiveness of U.S. providers selling services abroad, given the perceived risk of U.S. government access. Data stored abroad by U.S. companies would be treated differently than data stored abroad by foreign providers since foreign providers with no U.S. presence would not be subject to U.S. warrants. As a result, some foreign customers might decide to switch to foreign providers not in the United States, or even be encouraged or required to do so by their government. Second, it would set a concerning precedent, and

other governments might similarly require companies operating in their borders, or subsidiaries of these companies, to produce data stored outside of their borders, including that of U.S. citizens and residents stored in the United States. This situation could be at odds with U.S. protections against unreasonable search and seizure—setting up international conflicts over sovereignty.[3]

Conversely, if U.S. courts rule that search warrants cannot be used to obtain data stored overseas from U.S. providers, foreign governments may try to force U.S. companies to store data within their country's borders to make it impossible for U.S. law enforcement to execute a lawful search and seizure. Such data localization policies would raise costs for businesses and consumers, especially those adopting cloud-based technologies and services.[4] In addition, data localization policies would make it more difficult for U.S. companies to compete abroad as they would have to build more data centers in every market they want to enter. This outcome could also violate the Budapest Convention on Cybercrime, an international treaty signed by the United States and 51 other parties, which requires signatories to maintain compulsory access to all data stored by domestic companies.[5]

Either alternative would make it more difficult for U.S. law enforcement agencies to get access to data in the long run, as it would create incentives for data service providers to keep or move data outside of the United States.

U.S. policymakers should ensure law enforcement agencies can gain lawful access to information to protect their citizens and uphold U.S. laws, but without disadvantaging U.S. companies and workers facing global competition. Achieving this will require modernizing the process by which governments around the world obtain data stored outside their borders. Existing legal processes and treaties are woefully out of date and needlessly complex. Countries have mismatched legal assistance treaties, conflicting laws, and differing norms. Indeed, there is currently no comprehensive framework for how to successfully navigate cross-border jurisdictional disputes, especially those involving the digital economy. Such a patchwork of laws and rules may have been somewhat acceptable before the advent of the digitally-integrated global economy. Now they are not.

No one nation can solve this problem alone. Settling questions of jurisdiction over data will require global reforms. However, the United States can and should lead the way on these reforms, and this report offers a path forward.

This report builds from a previous ITIF report offering a framework on how nations should engage in Internet policymaking given the global nature of the Internet.[6] It makes specific recommendations for how governments can use this framework to establish policies for law enforcement to access data. This report also assesses theoretical approaches to establish jurisdiction over that data, focusing on cross-border law enforcement requests, and not clandestine intelligence gathering for national security purposes. The framework herein is not intended for law enforcement requests for metadata (data that describes information about a communication).

To operationalize the proposed framework, policymakers should pursue the following actions:

- Modernize the internal processes for responding to foreign requests for legal assistance;
- Work with other governments to draft and adopt model MLAT 2.0 language;
- Push back against foreign data-localization requirements;
- Update the Electronic Communications Privacy Act (ECPA) to protect domestic digital communications;
- Restrict companies from storing data in countries with conflicting laws that limit law enforcement;
- Engage with other nations to develop a "Geneva Convention on the Status of Data."

LEGAL PROCESSES U.S. LAW ENFORCEMENT CAN USE TO GAIN ACCESS TO DATA

Law enforcement officials investigating crimes often want to gain access to an individual's data, such as emails or files. But determining where data is stored can be complicated because it can be stored in a variety of different ways and locations. Sometimes companies store customer data in data centers that are located exclusively in a single country. Other times they store data on servers located in a foreign nation. Similarly, companies store customer data in data centers located in multiple countries, splitting data across multiple data centers to provide faster access to data, ensure data is always accessible, and prevent data loss.[7] In this latter case, law enforcement officials will have more difficulty gaining access to personal communications data because it is stored in multiple jurisdictions. And, to make matters more complicated, in addition to the location of data, the location of the company storing that data and the nationality and/or residency of the person or persons to whom the data belongs all can vary.

And yet, law enforcement must untangle this complicated web for every case in which it wants to seek lawful access to data. Law enforcement officials have two paths that they can use to compel access to data during criminal investigations. First, law enforcement officials can use domestic legal authorities to access data, such as search warrants and subpoenas. While U.S. law generally allows U.S. law enforcement to compel companies to turn over their own business records stored overseas, it is still an open question as to whether U.S. law enforcement can compel companies to provide their customers' data through these processes.[8] Second, in some cases where the evidence is not located within their jurisdiction, law enforcement officials may work through international processes, such as treaties for mutual legal assistance or police-to-police cooperation agreements, to access that data.

U.S. Domestic Legal Authorizations for Law Enforcement

The primary U.S. laws that govern how law enforcement can compel an individual or business to disclose private electronic communications data is the Electronic Communications Privacy Act (ECPA) of 1986 and the Stored Communications Act (SCA) of 1986, which amended ECPA.[9] ECPA gives law enforcement agencies a variety of legal tools to seek the contents of stored communications, including subpoenas, court orders, or warrants.[10] Law enforcement can also use traditional search warrants to acquire physical devices that hold data, such as a hard drive or computer, but the information may be encrypted. Notably, U.S. law treats access to digital information differently than physical information based on how old it is, where it is stored, what technology is used to store it, and several other factors. These distinctions are often illogical. For example, as originally specified in ECPA, U.S. law enforcement could use a subpoena, which can be issued without a judge or magistrate's review, to compel production of user content, like the text of emails, stored online after 180 days. Under this law, emails older than six months are treated differently than new emails. Fortunately, judicial opinions and commitments by the Department of Justice have effectively superseded this in practice (although this language remains in the statute).[11] However, this appellate ruling only applies to a portion of the country and a future DOJ could reverse its opinion on the matter.

There are three main methods U.S. law enforcement uses to gain access to data domestically. First, U.S. law enforcement can use a SCA subpoena to require persons or businesses located within the jurisdiction of the court to collect evidence (whether physical or digital) in their direct possession or control, regardless of the items' location, and bring them to court. Recipients can appeal a subpoena in court before it goes into effect. There is no requirement for a judge or magistrate to review a subpoena before law enforcement officials issue it. Indeed, of these legal tools, subpoenas have the lowest threshold for a law enforcement agency to obtain information. However, subpoenas can only compel a company to disclose specific types of information, such as account names, IP addresses (the unique string of numbers separated by periods that a computer uses to identify itself while browsing the Internet) used to create an account, and other basic metadata (i.e. data that describe information about a communication, such as specific times when a user signs in to an account).[12] Subpoenas extend extraterritorially because a court case decided subpoenas can be used by law enforcement to compel an entity to produce documents for law enforcement, even if they are located abroad and doing so would violate foreign laws.[13] The U.S. government does attempt to avoid serving subpoenas if doing so would violate conflicting foreign laws.[14]

Second, law enforcement can seek a court order under SCA, which, like a subpoena, compels access to the same metadata from a person or company but can also compel access to more detailed information about the use of an account.[15] For example, SCA court orders allow law enforcement to compel access to IP addresses associated with a particular email sent from that account and "to" and "from" fields in an email.[16] To obtain an SCA court

order, law enforcement officials must prove to a judge or magistrate that the requested information is relevant and material to an ongoing criminal investigation.

Third, law enforcement can seek a SCA warrant from a court, which gives law enforcement the power to compel the production of stored digital communications. Law enforcement can serve a warrant directly to a user or can serve a warrant on a business for customer communications data. Law enforcement can use a search warrant to obtain the same information as both a subpoena or court order would, as well as the content of private messages. However, warrants require judicial review and the specific description of the data being sought as well as the specific location where the search will take place. While courts have disputed the issue, the Second Circuit Court found in the Microsoft Ireland case that warrants only apply only to information located in the United States.[17] Furthermore, warrants require law enforcement officials to prove probable cause that a crime has been committed and that the search will result in the evidence of that crime, a stricter standard than most other countries set.[18] For example, French law is less strict for access, giving investigating magistrates much broader authority to order a search of any place where data can be discovered without showing probable cause.[19] Therefore, search warrants have the highest threshold for a U.S. government agency to obtain information.

In December 2016, U.S. federal judiciary's Advisory Committee on the Federal Rules of Criminal Procedure passed and the Supreme Court approved a change for Rule 41 of the Federal Rules of Criminal Procedure, which governs how federal criminal prosecutions are handled in the United States, allowing magistrate judges to grant federal agents a single search warrant for multiple computers in different locations, including computers outside their jurisdiction.[20] This change allows law enforcement to get a warrant to compel access to data that is located in a place outside the jurisdiction of the magistrate in the area where the crime occurred, such as in a different state. With these warrants, law enforcement agencies have the authority to use surveillance tools to access data. This rule change helps law enforcement in two primary ways.[21] First, if suspects in an online crime obscure their location, federal agents can now obtain a search warrant letting them attempt to remotely install malware on suspects' computers regardless of where the suspects are located. Second, if a crime involves criminals hacking computers in five or more districts, the changes allow judges to issue a single warrant for all affected computers, regardless of where the computers are located.

In addition to ECPA, national security laws allow law enforcement to compel companies to release information under limited circumstances. For example, the Foreign Intelligence Surveillance Act (FISA) can be used by law enforcement for investigations on U.S. soil.[22] FISA allows law enforcement to compel a company to turn over physical and electronic evidence or conduct surveillance if law enforcement can show probable cause that the target is a foreign power or agent of a foreign power. While these investigations may focus on espionage or terrorism, there is no requirement to show probable cause of these crimes to compel access to this data. Similarly, several federal statues allow the Federal Bureau of Investigations (FBI) to issue administrative subpoenas, commonly called national security

letters, to compel access to metadata stored in the United States by U.S. providers for investigations of international terrorism or clandestine intelligence activities.[23] National security letters allow the FBI to obtain personal metadata records from Internet Service Providers, records from financial institutions, and consumer information from consumer reporting agencies.[24] National security letters often include a gag provision that restricts the company receiving the order from disclosing it until the FBI makes the determination that it can be disclosed (the FBI reviews whether to disclose a letter at the close of each investigation or three years or more after it issues the letter).[25] Although court decisions and the USA FREEDOM Act have since limited these gag provisions, such as by requiring prompt judicial review and a "reciprocal notice" requirement, whereby the government must justify gag orders if the recipient of the letter requests juridical review, it is still an open question whether national-security-letter gag clauses are constitutional.[26]

Cross-border Law Enforcement Assistance Mechanisms

When data is not stored within a country's borders, law enforcement may pursue other legal mechanisms to compel access. U.S. law enforcement has relied on three types of processes to access data stored in other countries: treaties and agreements, letters rogatory (see below), and police-to-police cooperation.

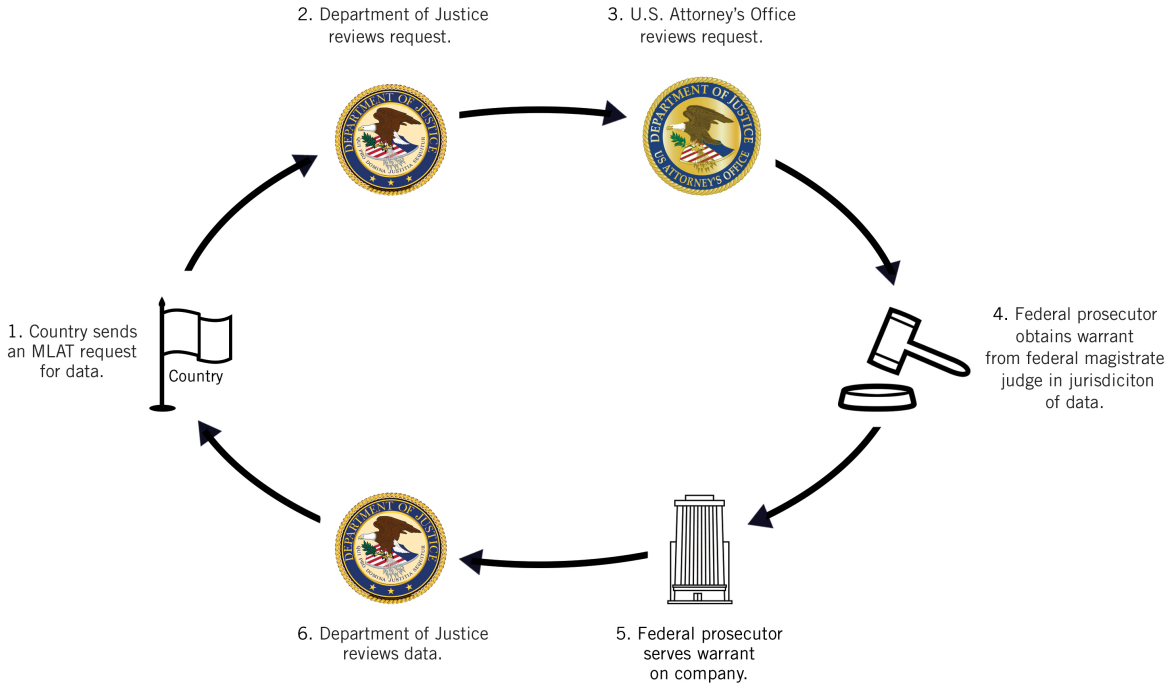
First, two or more countries may enter a treaty or agreement for legal assistance, which can take several forms. The first are mutual legal assistance treaties (MLATs), which encourage law enforcement agencies to provide assistance to their counterparts in other countries.[27] MLATs can be bilateral, multilateral, or regional. The scope of these agreements can also vary to exclude certain crimes. The United States has MLATs with 63 nations.[28] The U.S. government also has mutual legal assistance agreements (MLAAs)—another program for transnational legal assistance—with countries such as China.[29] MLAAs are different from MLATs because they do not require the advice and consent of two-thirds of the U.S. Senate, so long as the agreement is not inconsistent with legislation enacted by the Congress.[30] There are also multilateral treaties with provisions for mutual legal assistance, such as the U.N. Convention on Transnational Organized Crime.[31] In addition, the United States has ratified an agreement, known as the Umbrella Agreement, which added new MLATs or supplemented existing MLATs for each country in the European Union.[32] MLATs, MLAAs, and other agreements reduce the barriers that law enforcement would otherwise encounter when conducting investigations across borders.

The U.S. government created most MLATs and MLAAs during the 20th century, and the system is now out of date and does not meet the demands of the digital age. Prior to 1977, the U.S. government only shared information with other governments through principles of comity and letters rogatory (discussed below).[33] Law enforcement could directly send physical evidence across borders to fulfill these requests. In 1977, the need for more coordination to combat international crimes led the U.S. government to create its first MLAT with Switzerland to investigate money laundering and tax evasion taking place due to Swiss banking secrecy laws.[34] Since then, the U.S. government has entered into multiple differing treaties and agreements that allow for documents to be exchanged between

borders. But this system was put in place before data moved freely across borders over the Internet, and has created issues for law enforcement trying to use an antiquated system to collect digital information.

Because these treaties and agreements are not universal, gaps in the process can leave countries unable to manage law enforcement requests for data where there is no agreement. MLAT and MLAA requests must travel through multiple levels of diplomatic and legal bureaucracy, and are answered at the discretion of the country which receives the request. In the United States, the U.S. Department of Justice's (DOJ) Office of International Affairs serves as the central authority for processing and responding to international requests for data from foreign countries.[35] Because treaties, such as MLATs, come with procedural hurdles, law enforcement agencies—especially within the United States—have complained that these treaties involve a "slow and cumbersome" process that is not especially well-suited for a fast-paced digital environment.[36] When a foreign government submits an MLAT request for personal communications data stored with a domestic company (the process changes for other types of digital content, such as for bank records), the DOJ first reviews the request, then assigns it to a federal prosecutor—often in a U.S. Attorney's Office—to obtain a warrant to compel the company to produce the requested data.[37] The warrant is then served on the company, which provides the data to the DOJ for final review before it is sent to the foreign government (figure 1). The DOJ does not have the resources to adequately handle these requests in an efficient manner.[38] As a result, the U.S. government takes an average of 10 months to complete MLAT requests.[39] This situation has led to a backlog of MLAT-related foreign requests that DOJ projects could grow to as large as 16,000 by 2020.[40]

Figure 1: How the U.S. Government Responds to Foreign MLAT Requests for Personal Communications Data Stored with a Company



Similar lengthy delays are common when U.S. law enforcement initiates an MLAT request with another country. These delays result from several reasons, such as a lack of resources to respond to MLAT requests or limited experience with the evidence-gathering process.[41] For example, the MLAT process between the U.S. and Mexican governments delayed a civil asset forfeiture case over three years because the U.S. government encountered "significant challenges" obtaining formal discovery from Mexico, despite appealing to the Mexican government multiple times.[42] Similarly, the average response time from Ireland to a U.S. MLAT request for digital evidence is approximately 15 to 18 months.[43] U.S. MLAT requests may also be stymied by foreign law enforcement's lack of technical forensic expertise to access data when complying with MLAT requests. For example, in some cases it may be easier for U.S. authorities to request foreign law enforcement to ship seized hard drives to the United States for U.S. law enforcement to directly access data rather than ask a foreign government to conduct its own digital search.[44] Furthermore, U.S. law enforcement often finds a lack of willingness from some of its MLAT partners, especially authoritarian countries, to cooperate with U.S. requests in a timely manner. For example, despite an MLAT existing between Russia and the United States, it is rare that the Russian government assists U.S. law enforcement investigations involving Russian cybercriminals.[45] As a result, U.S. law enforcement must target Russian cybercriminals when they travel outside of Russian borders.[46]

Countries that do not have a formal treaty can still provide each other with legal assistance. If countries do not have an MLAT, treaty, or other agreement, then assistance is usually made based on reciprocity. These agreements also depend on each country's domestic laws. For example, Argentina will provide legal assistance without a formal treaty per its law on international cooperation in criminal matters and upon condition of reciprocity.[47]

Second, in the absence of a treaty or other agreement, a U.S. court can use letters rogatory to obtain judicial assistance from overseas.[48] Letters rogatory are formal requests for assistance from a court in one country to its counterpart in another. This differs from assistance under an MLAT because it is made straight to a court rather than through the government's designated central authority. Letters rogatory are available to both government officials and to individual defendants, but typically are not issued during the investigative stage of a criminal proceeding. It is usually a year or more before the order is executed because these letters are customarily transmitted through diplomatic channels; they can be more unpredictable than MLATs because they are based on relationships or comity between courts rather than formal agreements.[49]

Third, informal international police-to-police cooperation has come to prominence over the last few decades due to the rise of international crimes, such as financial fraud, hacking, or child pornography.[50] This form of international cooperation is not usually governed by a treaty or a statute. For example, Interpol—the world's largest international police organization—was not established by an international treaty.[51] Instead, informal agreements and memoranda of understanding usually govern this form of cooperation.[52]

To participate in police-to-police cooperation, U.S. law enforcement can directly contact its counterparts in another country to seek information. However, informal police-to-police cooperation is often not available for the content of electronic communications held by a third-party provider because host countries typically require a judicial process to compel production of personal communications data.

In addition, domestic laws can affect how foreign law enforcement agencies seek assistance from the United States. For example, ECPA includes provisions that prevent foreign governments from seeking the content of U.S.-held communications directly from U.S. providers without official MLAT requests to the DOJ. (ECPA, by contrast, allows foreign governments to directly request metadata from U.S.-based providers).[53] In effect, this means foreign law enforcement has easy access to digital evidence in its own country, but not digital evidence stored with a U.S. provider. To get access to U.S.-held digital evidence from U.S. providers to further their domestic investigations, foreign law enforcement agencies are forced to file MLAT-based requests (if such an agreement exists) to gain access to the data. Because many multinational communication service providers are U.S.-based, this situation has hampered many foreign investigations and increased the burden of MLATs on the DOJ. For example, Brazil's government arrested a Microsoft employee in 2015 for failing to give local law enforcement Skype data on a Brazilian customer that ECPA prohibits Microsoft from disclosing.[54] In this case, the Brazilian government did not go through the MLAT process with the U.S. government, despite an existing agreement, likely because of the difficulties of using MLAT processes.[55] U.S. law enforcement can help foreign law enforcement side-step ECPA's requirement for companies if it engages in a joint investigation with foreign law enforcement and then shares that information through police-to-police cooperation.[56] But even in those cases, U.S. law enforcement must obtain a warrant based on probable cause in order to compel access to the data.

In recent years, several members of Congress have proposed legislation to update ECPA, modernize the MLAT system, and improve cross-border law enforcement mechanisms. For example, the Law Enforcement Access to Data Stored Abroad (LEADS) Act, introduced in the 114th Congress would have required law enforcement to use MLATs to compel the disclosure of customer content stored outside the United States unless the account holder is a U.S. person.[57] The LEADS Act also would have strengthened how the DOJ processed MLATs. Finally, in the 114th Congress, Sens. Orin Hatch (R-UT), Chris Coons (D-DE), and Dean Heller (R-NV) introduced the International Communications Privacy Act (ICPA), which would allow law enforcement to use a warrant to compel production of data stored abroad if that data belonged to a U.S. citizen, a person physically located within the United States, or if it belonged to a citizen or resident of a country with which the United States does not have a MLAT.[58] However, for non-U.S. individuals from countries where the U.S. government has established an MLAT, ICPA would give those governments veto power over the request. An updated version of ICPA will likely be re-introduced in the current 115th Congress.[59]

THREE THEORETICAL APPROACHES TO CROSS-BORDER ACCESS FOR LAW ENFORCEMENT

To assess the value of any proposal for cross-border access for law enforcement, it is useful to take a step back and analyze the different approaches that countries could use to establish jurisdiction over data.

Whether law enforcement can use domestic legal authorizations or international agreements to obtain information should depend on which country or countries have jurisdiction over the data. There are three main theoretical approaches to resolving this question of jurisdiction: focusing on either the location of the company storing the data, the location of the data, or the citizenship or residency of the data subject. Each approach comes with tradeoffs (table 1). Each of these theoretical approaches assumes countries must defer to treaties when data is stored outside of the jurisdiction of law enforcement to remove unilateral claims of extraterritorial jurisdiction. As previously discussed, actual treaties are laborious and often not used by law enforcement to access data stored abroad. However, these theoretical approaches assess treaties as if in a perfect, or at least much improved, world, where response times are short and access to data across borders respected the jurisdictions of all countries with interest in the data. Further, these approaches are framed with U.S. laws and proposals as examples, but each approach can apply to any country. While no real-world proposal fits perfectly into any one of these approaches, they can help inform the benefits and drawbacks to settling questions of jurisdiction.

Table 1: Pros and Cons of Different Approaches to Cross-border Access for Law Enforcement

Approach	Pros	Cons
Make jurisdiction contingent on the physical location of data.	Respects national sovereignty. Reduces international conflicts for multinational companies.	Limits law enforcement's access to data stored abroad in countries without an MLAT. Complicates access when data is distributed across multiple jurisdictions. Creates incentives for countries to require data localization. Allows for countries to create legal refuges for criminal activity.
Make jurisdiction contingent on the company's location of incorporation.	Allows for direct authority over domestic companies to ensure compliance. *FROM U.S. PERSPECTIVE:* Gives U.S. law enforcement most immediate access to data since most major Internet companies are based in United States.	Limits law enforcement's access to data stored by foreign companies with no domestic presence or MLAT. Allows for conflicting laws from multiple countries for multinational companies. *FROM U.S. PERSPECTIVE:* Hurts U.S. competitiveness because non-U.S.-based companies would have advantage in the marketplace by not being subject to U.S. law enforcement. Could encourage U.S. companies to reincorporate in a foreign nation.
Make jurisdiction contingent on the citizenship or residency of the data subject.	Does not create incentives for data localization or give competitiveness advantage to any country.	Forces companies to comply with laws of every country where they have customers. Limits law enforcement's access to data due to inability to accurately discern the location or citizenship of the data subject. Limits law enforcement's access to data from foreign data subjects. Conflicts may apply when data subject has multiple citizenships. Enables authoritarian governments access to the data of dissidents abroad.

Location of Data

One theoretical approach to establishing what country has jurisdiction over data would be to hold that only the country where the data is physically located has jurisdiction. Under this kind of system, the U.S. government could compel the production of data using domestic legal process (e.g., a SCA warrant) if the data were physically stored on servers within the United States. U.S. law enforcement would need to compel production of all data stored on servers abroad through international agreements or treaties (e.g., an MLAT). If there is no agreement or treaty with the country in which the data is stored, then U.S. law enforcement would not be able to compel production of the data. Figure 2 explores how this approach would affect investigations in various situations.

Figure 2: How U.S. Law Enforcement Can Compel Access to Data if a Location-of-data Approach were the Legal Standard

Location of Data: United States

Presence of Company	Location of Data Subject: United States	Location of Data Subject: MLAT Nation	Location of Data Subject: Non-MLAT Nation
United States	Access	Access	Access
MLAT Nation	Access	Access	Access
Non-MLAT Nation	Access	Access	Access

Location of Data: MLAT Nation

Presence of Company	Location of Data Subject: United States	Location of Data Subject: MLAT Nation	Location of Data Subject: Non-MLAT Nation
United States	Access	Access	Access
MLAT Nation	Access	Access	Access
Non-MLAT Nation	Access	Access	Access

Location of Data: Non-MLAT Nation

Presence of Company	Location of Data Subject: United States	Location of Data Subject: MLAT Nation	Location of Data Subject: Non-MLAT Nation
United States	No Access	No Access	No Access
MLAT Nation	No Access	No Access	No Access
Non-MLAT Nation	No Access	No Access	No Access

Green: Access Through Domestic Authorizations | Yellow: Access Through Treaties | Red: No Access

This framework closely follows the Second Circuit's ruling in the Microsoft Ireland case, which found that U.S. law enforcement agencies should rely on territoriality, or the

physical location of the data sought, to determine jurisdiction.[60] This is because, the court says, the Stored Communication Act (SCA) does not allow its warrant procedures to take place abroad, as a court's jurisdiction for warrants only extends to U.S. borders (with some exceptions).[61] However, courts have created conflicting rulings on this matter, and the DOJ is appealing this decision to the Supreme Court.[62]

The benefit of this theoretical approach is that it respects each country's national sovereignty, ensuring that each country can establish its own laws on access to data. Law enforcement agencies can easily access data within their own borders through domestic laws, but need to work through treaties and agreements to access data in other jurisdictions. Moreover, it avoids the problem of competing claims of jurisdiction and thus prevents multinational companies from getting caught in the crosshairs of conflicting laws.

However, this approach was designed for a world in which law enforcement primarily seeks access to physical goods or data stored in a single location. Basing a test for jurisdiction solely on where the data is located is problematic for four reasons. First, this approach limits law enforcement's access to data stored abroad in countries where there are no treaties or agreements. To date, the United States has MLATs with 63 of the 196 nations recognized by the U.S. government.[63] In addition, the U.S. government is negotiating or has entered agreements with several other nations, such as a MLAT with Jordan that has not gone into effect.[64] Where there are gaps, U.S. law enforcement has limited options to compel production of data stored abroad. However, the other options, such as international police-to-police cooperation or letters rogatory, are laborious and function upon condition of reciprocity. Therefore, where a country has no MLAT agreement, there is limited guarantee law enforcement can access data they need to further investigations.

Second, the location of data can be difficult to determine, which can complicate access and impede investigations. With the rise of cloud computing, businesses no longer need maintain their own servers to ensure that their data is private and secure—so they can use computing infrastructure anywhere in the world. Modern techniques for storing data, such as sharding, involve breaking up data and storing it in multiple locations, or constantly moving it between different data centers in different countries. Using the physical location of data to determine who has access can create significant complexity. For example, if a company broke the content of a file across servers in five countries, then law enforcement would have to initiate five separate MLAT requests to view that file. And the company would not need to stop at five—it could split the message into a hundred pieces, creating a labyrinthine environment for law enforcement agencies attempting to legally access the data. As a result, if cross-border law enforcement mechanisms (e.g., MLATs) are not updated to meet these demands, this approach would limit governments in their capacity to compel production of data stored abroad because they would be forced to rely on slow and arduous international treaty processes.

Third, this framework would create an incentive for governments to force businesses to store data within their borders, a non-tariff barrier to trade called data localization, to gain

access to it or keep it out of the hands of other governments. For example, in 2016, Germany enacted a new law forcing companies to store telecommunications metadata in Germany as it does not trust other countries with the data.[65] While such a requirement would not prevent citizens from individually choosing to use providers based abroad to make it more difficult for their government to compel production of their data, it could be an effective way to force all businesses, including those widely used by consumers, to store their data on servers located domestically. Moreover, these policies have second-order effects that represent a barrier to global digital trade because impeding data flows—or making such flows more expensive—puts foreign firms at a disadvantage to their domestic competitors. This is because these policies force foreign competitors to build unnecessary local data centers and incur additional costs that domestic firms escape (because they already use local data centers). Data localization is particularly problematic because if every country followed suit it would undermine the significant benefits of cloud computing. Moreover, data localization by foreign governments would move more data outside the jurisdiction of the U.S. government.

Finally, if U.S. law enforcement cannot access information stored abroad through legitimate and straightforward methods—such as cooperation with a foreign country—then criminals and others may store data abroad with providers in certain countries to keep it out of sight of U.S. law enforcement. This framework would enable "data havens," countries that do not create an agreement for legal assistance with the United States, and therefore become a legal refuge for criminal activity. This type of problem exists for other services. For example, several countries have created financial regimes with low taxes, low interest rates, and little corporate transparency, leading to secretive "tax havens" where criminals can hide their money from domestic tax collectors.[66] Similarly, the U.S. Trade Representative has identified several countries with lax intellectual property laws, or "Internet piracy havens," that allow intellectual property theft to flourish online.[67]

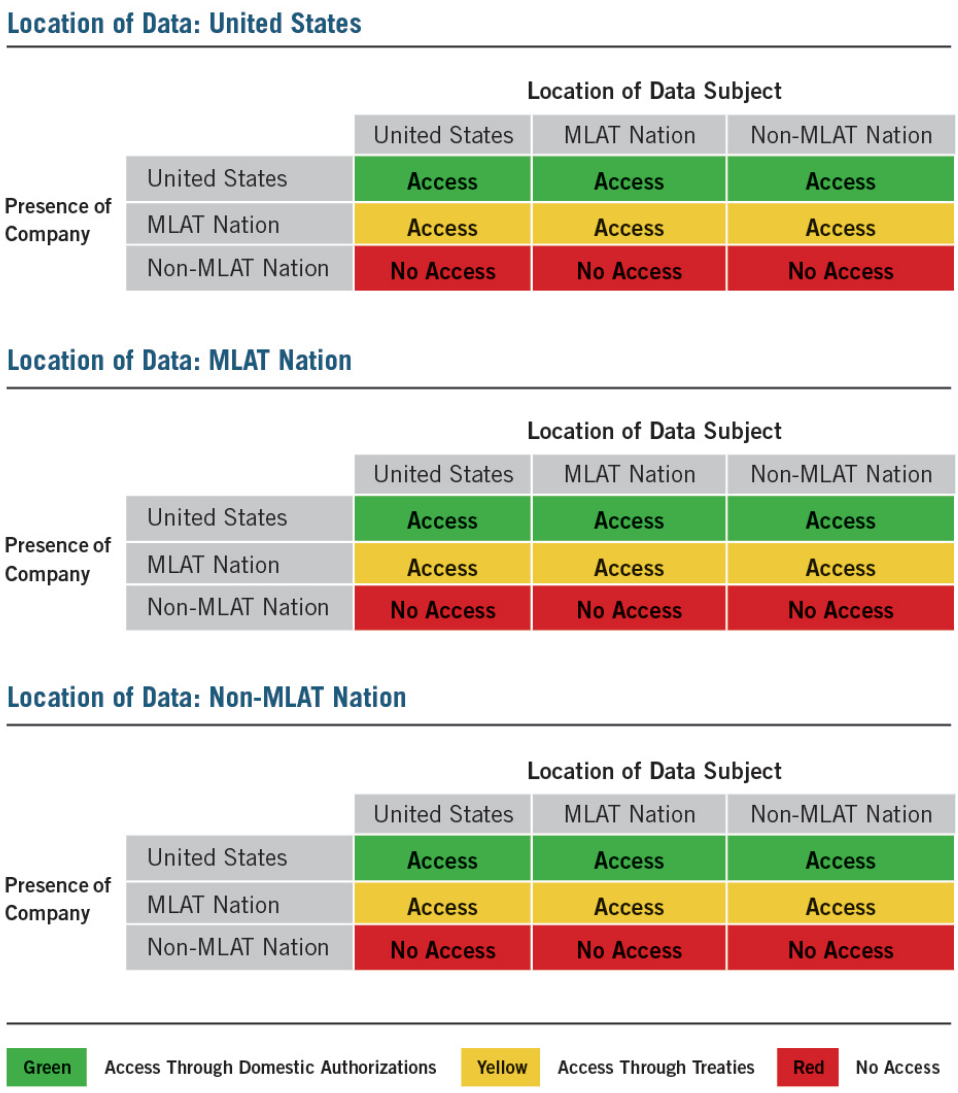
Location of the Company Holding the Data

Another theoretical approach for establishing what country has jurisdiction over data would be to hold that countries have jurisdiction over domestic companies, and can use compulsory processes to access data wherever it is located. This approach could turn on a number of different conditions, such as whether the company is headquartered in a country, whether it purposely targets sales in a country, or whether it has a legal presence in that country. This report will focus on the latter.

Under that approach, the U.S. government would require that any company that has a legal presence within the United States provide law enforcement access to its data using domestic legal authorizations (e.g., a SCA warrant). Law enforcement would be able to compel production of data if the company has an established legal presence in the country, even through a subsidiary. However, for foreign businesses with no legal presence in the United States, U.S. law enforcement would need to go through international agreements or treaties (e.g., an MLAT) to compel production of data stored abroad. If the country has no such agreement or treaty with the United States, then U.S. law enforcement would not be

able compel production of the data. Figure 3 explores how this approach would affect investigations in various situations.

Figure 3: Examples of How U.S. Law Enforcement Can Compel Access to Data Through a Location-of-business Approach



With regard to a company's location, this is currently the basis for how subpoenas or ECPA court orders are executed in the United States. Law enforcement serves a subpoena on a person or business located in the United States, who/which must then produce the sought-after records regardless of where they are stored.[68] The use of unilateral compulsory measures, such as subpoenas, is somewhat in dispute when it creates conflicts with other countries.[69] In the U.S. government's case against Microsoft, the U.S. government argues that it should be able to issue a warrant, which some dispute does not have an extraterritoriality component, on a domestic company to compel production of information regardless of where it is stored or where the data subject is located.[70] These

extraterritorial law enforcement authorities are partially a product of ECPA having been created in the 1980s, long before the Internet and cloud computing made it easy and cost effective for companies to store their data all over the world.

The location-of-data approach is most similar to the status quo, where some domestic authorizations are a compulsory process that U.S. law enforcement can use to compel the production of certain data overseas. This approach allows for a country's direct authority over domestic companies to ensure that they comply with legal authorizations for data, no matter where they store that data or who the data subject is. For example, the French government would be able to compel production of a multinational company's records if a branch of that company is in France, even if that company stores data in another country that has no agreement or treaty with France. This approach would especially benefit law enforcement agencies in developed countries, such as the United States, which have many multinational companies. Given that most major Internet companies with a global presence are located in the United States, U.S. law enforcement would have easier access to the data stored abroad if it did not need to comply with international agreements. However, by relying on the legal presence of companies, this approach would also limit the extraterritorial reach of countries who try to assert jurisdiction over any company that happens to be online. Even though online businesses offer their services globally over the Internet, no organization can realistically comply with the laws of every country, especially those where the company's workers have never even set foot, simply because they are on the Internet and some of their users might be based abroad.

However, basing jurisdiction on where a company has a legal presence would have three drawbacks. First, it would limit law enforcement's access to data that is stored by foreign companies that have no domestic presence and are located in countries with no treaty or agreement with the requesting country. For example, if U.S. law enforcement sought records from a Salvadorian company that are stored in Costa Rica, it would not be able to acquire them, because the United States and does not have an agreement with either El Salvador or Costa Rica.

Second, this approach would allow countries to create conflicting laws for multinational companies. In particular, the laws for how a company may respond to law enforcement requests for data may conflict between two or more countries in such a way that it is impossible for a company to follow all of them. Brazil's laws for how the government can access digital records, for example, directly conflict with provisions in ECPA that restrict how foreign law enforcement can access data stored in the United States. This conflict has led to Microsoft being caught in the middle of an international dispute.[71]

Moreover, if democratic countries like the United States ultimately adopt an approach that forces businesses to comply with law enforcement requests on data they store in other countries unilaterally, then authoritarian governments will similarly insist on extraterritorial authority. This form of reciprocity is not promising for the protection of civil liberties. While it is unlikely that U.S. actions one way or the other will be the deciding factor in

what some nations, especially non-democratic ones, do regarding lawful government access to content, this approach will embolden them. For example, in 2016, China promulgated regulations governing the collection and examination of digital evidence for criminal investigations.[72] As part of these rules, when conducting a criminal investigation, Chinese police may extract digital data from servers or hard drives that are located outside of China.[73] Certainty, authoritarian regimes are less likely to use legal processes, such as MLATs, than democratic countries because they have more control over information and lack the constraints of civil liberties.[74]

Finally, this approach would be highly detrimental to U.S. competitiveness. If the U.S. government were to enact this jurisdictional framework, it would feed the perception that the best way to prevent the U.S. government from being able to compel production of data is to store information overseas with a foreign-based provider, which would not be subject to U.S. domestic authorizations. Already, the U.S. government's surveillance programs have created distrust abroad of U.S. tech companies.[75] Several companies have described how this loss of trust has damaged their ability to do business abroad. Verizon, for example, lost a contract with the German government due to concerns over U.S. intelligence activities in 2014.[76] While U.S. market share in Europe has grown despite these concerns, countries have used U.S. surveillance as an excuse to justify protectionist measures; the full cost of this damage of trust is still unknown.[77] It is likely that countries will similarly use law enforcement access as an excuse to limit market access for U.S. companies. Foreign concerns over U.S. surveillance already extend to actions by U.S. law enforcement. For example, in response to the Microsoft case, the former European Union Justice Commissioner warned that if the U.S. government won the case it may violate international law.[78] Indeed, while this approach would be beneficial to law enforcement in the short term, there is no guarantee U.S. law enforcement will keep the same high level of access in the future, as this approach works directly against the market share of the industry they rely on for data. In other words, data would migrate to foreign providers.

Some have proposed a modified version of this approach designed to mitigate against some of these concerns. For example, Professor Jennifer Daskal of American University has proposed a model where U.S. law enforcement can use domestic authorizations from companies with a U.S. legal presence—regardless of where data is stored—if they engage in a comity analysis, which takes into account a foreign country's interest in sought-after data.[79] For example, if U.S. law enforcement seeks data of a non-citizen data subject located outside of the United States, and that domestic authorization (e.g., a SCA warrant) would violate foreign law, then the reviewing court would analyze factors related to the case to decide whether to grant that authorization. These factors could include the location of the data subject, the location of the crime, the possibility of accessing data through other means (e.g., an MLAT), and others.

Location of the Data Subject

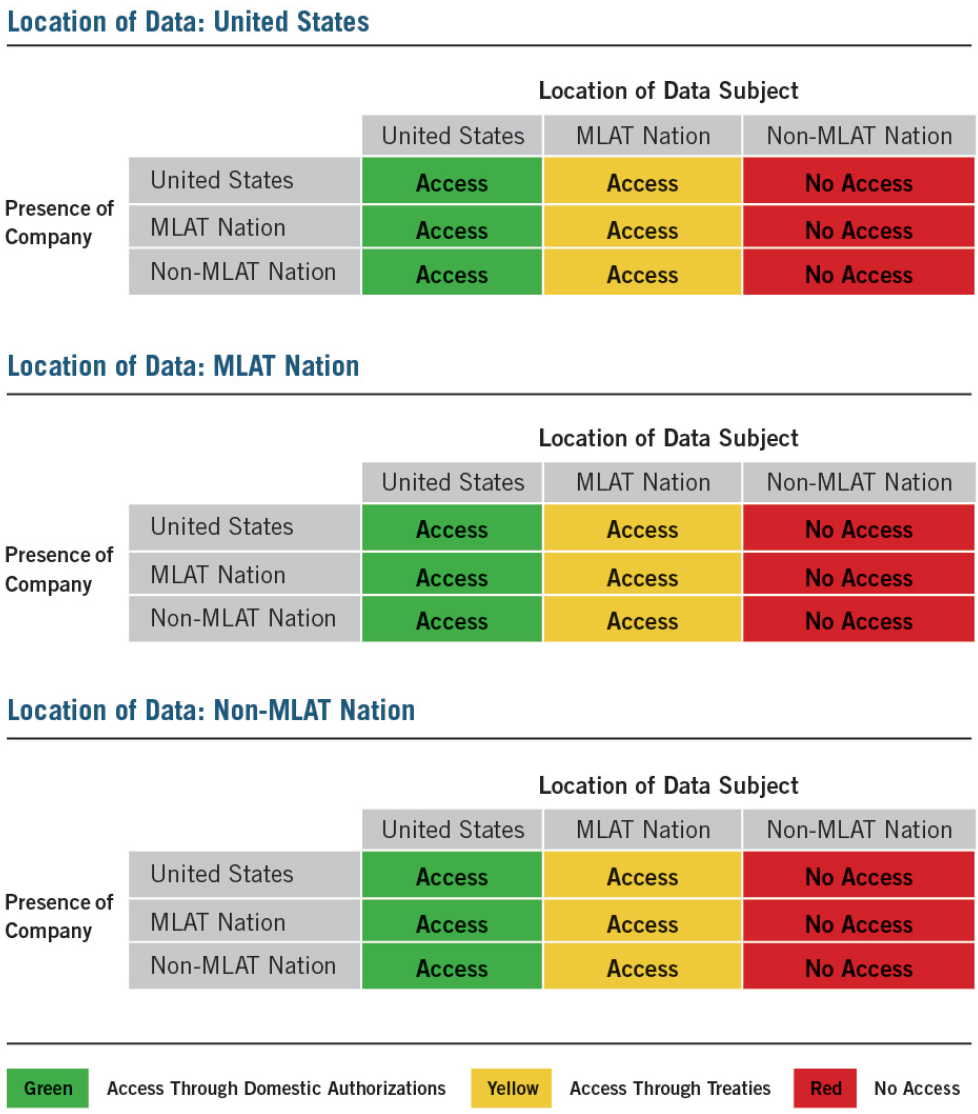
A third approach, that has been discussed as a hypothetical solution but not implemented, would be to settle questions of jurisdiction strictly based on the location or nationality of

the data subject. In this case, the U.S. government would be able to obtain data using domestic legal authorizations (e.g., a SCA warrant) if the data subject is located within the United States or is a citizen of the United States. This process would occur regardless of the location of the data or of the company storing the data. Therefore, U.S. law enforcement would be able to get easier access to offshore data if it regarded a U.S. resident. However, law enforcement would need to go through international agreements or treaties (e.g., an MLAT) to compel production of data that belong to foreign citizens or to people outside U.S. borders, even if it was stored within the United States.

Jurisdiction could be determined based either on the citizenship or the location of the data subject, or a combination of the two. If jurisdiction is based on citizenship, then the rules and laws of the country where the data subject is a citizen would apply no matter where he or she is located. For example, U.S. law enforcement would be able to seek domestic legal authorizations to acquire data for U.S. citizens from companies located within the United States, even if those citizens were located abroad at the time of the request. However, if U.S. law enforcement sought data for foreign citizens—even those located within the United States—they would need to go through international processes. If the country has no such agreement or treaty with the United States, then U.S. law enforcement would not be able to compel production of the foreign citizen's data.

If jurisdiction were based purely on the location of the data subject, then U.S. law enforcement would be able to use domestic authorizations to compel production of data on all data subjects located within the United States (see Figure 4). However, if those data subjects were located outside the United States, even if they were U.S. persons or their data was stored within the United States, U.S. law enforcement would still need to use international agreements or treaties to compel to compel production of that data. If the country has no such agreement or treaty with the United States, then U.S. law enforcement would not be able to compel production of the data.

Figure 4: Examples of How U.S. Law Enforcement Can Compel Access to Data Through a Location of-data Subject Approach



Some proposals work on a combination of these two tests. At least one legislative proposal in the United States has echoed this approach. For example, the International Communications Privacy Act (ICPA) would allow law enforcement to use a SCA warrant to compel production of data stored abroad if it belonged to a U.S. citizen or a person physically located within the United States.[80] However, ICPA would require that law enforcement defer to countries with mutual legal assistance treaties or agreements with the United States for non-U.S. individuals, giving the foreign government 60 days to object to the search and seizure. Similarly, Professor Orin Kerr of George Washington University proposed a variation of this approach, where jurisdiction is based on the perceived location of an individual.[81] Kerr suggests "the default rule might be that a person is presumed to be inside the United States unless there is clear and convincing evidence that the user is

outside the United States" and this standard should incorporate a time element for when law enforcement is reasonably sure the person was on U.S. soil.[82]

An approach based on the location or citizenship of the person would have several advantages. Mostly importantly, under this approach there would be little incentive for governments to mandate data localization requirements for companies for law enforcement purposes regarding wholly domestic cases.[83] If law enforcement was easily able to compel production of data on persons located within their country no matter where it is stored there would be no need to ensure it is stored domestically. Moreover, this approach would ensure a level playing field for all data storage companies because law enforcement would have equal access to all records on domestic cases, regardless of where it is stored. In this approach, cases involving crimes committed by foreign citizens would be subject to treaty processes.

However, basing jurisdiction on user location or citizenship has several drawbacks. First, because this information is frequently not available, this approach would limit law enforcement's access to data. Most online services do not track the nationality of their customers, nor do they have a means by which to verify this information. Neither is location easily verified with the kind of rigor that would be desired when dealing with civil liberties. While Internet service providers usually can tell where their users are located by tracking IP addresses, this information can be easily obscured through technology. For example, virtual private network (VPN) services can obscure the origin of Internet traffic. If law enforcement intercepts this traffic, they would see the IP address of the VPN rather than the original.[84] Similarly, the onion router (Tor) uses a series of computers distributed around the world to hide a user's IP address.[85] Criminals may be motivated to use these services to avoid law enforcement. In effect, this would allow criminals to choose which country's laws they would want to be subject to. In addition, some customers may access services from multiple countries or from businesses that do not have a physical presence in the United States but whose services can be purchased over the Internet (and are thus hard to serve a warrant on). Therefore, if law enforcement is unable to determine the citizenship of a person or their location, then using this jurisdictional framework would limit their capacity to solve crime and stop terrorism.

Second, this approach would limit U.S. law enforcement's access to data from foreign citizens located in the United States or those located in countries with no treaty with the United States. This framework would generate the same problem that a jurisdiction based on location of data would. If there was no agreement or treaty for mutual legal assistance between two countries, law enforcement agencies would rely on slow letters rogatory or police-to-police cooperation. And there is no guarantee law enforcement can access data they need to further investigations of persons located abroad.

Third, this approach would force companies to comply with domestic laws in every country in which they have customers, even if there is no physical office in that country. In the Internet age, the costs of monitoring countless legal requirements and responding to

each law enforcement request for data would be prohibitive for most companies. In addition, countries would subject companies to excessive costs if they had to routinely respond to foreign courts, especially when they have no physical location in that country.

Fourth, jurisdictional conflicts may arise when a data subject has citizenship with multiple countries. Because there is currently no international convention that determines nationality or citizenship, individual governments determine who is a national of their country.[86] As a result, national laws for citizenship often conflict with one another and some people have citizenship in multiple countries. If a data subject is a dual citizen, then there will be a conflict under this approach when law enforcement from one of those countries attempts to compel production of their data. Moreover, some countries—especially authoritarian ones—do not allow citizens to renounce their citizenship. For example, Iran makes renouncing citizenship very difficult and Iranian law does not allow for dual citizenships.[87] Because the Iranian government does not have an MLAT with the U.S. government, whose laws would apply to a former Iranian citizen seeking asylum in the United States who cannot renounce citizenship?

Finally, as suggested by the previous drawback, this approach could have a potential negative impact on dissidents of authoritarian countries living abroad. With this approach, countries such as China, Russia, Syria, Turkey, or Iran would have the ability to seek information on agitators living in exile. As a result, without protections for human rights, this approach could endanger civil liberties.

A BETTER APPROACH TO CROSS-BORDER ACCESS FOR LAW ENFORCEMENT

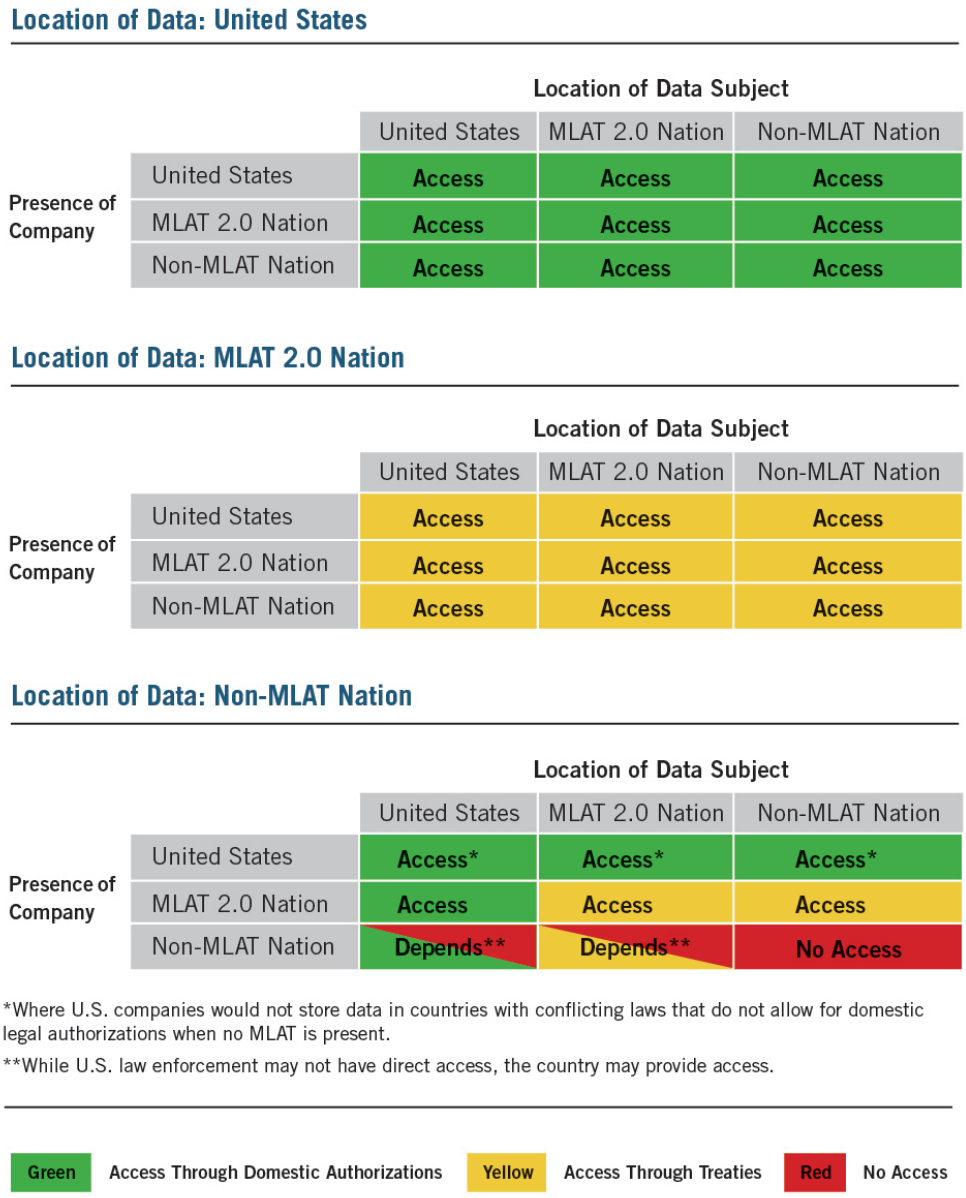
While each of these approaches to cross-border access for law enforcement has advantages and disadvantages, none is without merit. A focus on the location of data protects an individual country's sovereignty. A focus on the location of the company storing the data gives law enforcement agencies additional tools to compel production of data stored outside their borders. And a focus on the data subject would ensure a level playing field for different countries trying to compel production of data stored abroad on their citizens. Combining various aspects of each of these approaches could capture the best of each while sidestepping their pitfalls.

First, any approach should recognize national sovereignty. Different nations have different sets of values, priorities, and legal systems. And because Internet companies offer services over global networks, it is often the case that two or more countries have interests in the same data. The model approach should not force a particular nation's policies on the rest of the world, such as promoting the strict standard of probable cause to gather evidence (as in the case of the United States) or allowing government access to evidence at the detriment of personal freedoms (as in the case of nations like China and Russia). Therefore, each business should be subject to the law of each country in which they have a legal presence. This principle would ensure that no company can escape complying with a nation's laws by simply transferring data overseas.

Governments should also respect international agreements. Therefore, if the data that U.S. law enforcement is seeking is not stored in the United States, the U.S. government should use international agreements (see the discussion of MLAT 2.0 below) to compel production of the data. If the country does not have a treaty with the United States, then the U.S. government should seek to establish a treaty but should not interfere with that country's sovereignty, especially if it would affect users outside of U.S. borders.[88] This step would partially restrict the access of U.S. law enforcement agencies to data stored abroad under some circumstances by forcing them to use established international agreements to compel production of data. MLATs today do not obligate countries to follow them, and because of their ineffectiveness, many countries seek unilateral extraterritorial access. For this step and the previous one to work, countries must fundamentally change their treaties and agreements, which will not be an easy task, but is a necessary one.

Finally, any approach should recognize the needs of law enforcement to access digital information stored abroad when no MLAT agreement exists. When U.S. law enforcement encounters problems seeking data in countries that have no agreement or treaty with the United States, the U.S. government should use an approach that focuses on the location of the data subject and location of the company storing the data by going through domestic legal authorizations (e.g., a SCA warrant) to compel production of the data. For example, if a U.S.-based person is storing data in a non-MLAT country using a U.S.-based company, then U.S. domestic authorizations should apply to accessing that data. In other words, U.S. authorities should be able to compel the company to turn over the data to U.S. law enforcement providing they go through the proper legal steps. This step will mitigate the repercussions of a jurisdictional test that focuses on the location of the data by allowing U.S. law enforcement to further domestic investigations when the territory jurisdictional test fails. This step should be conducted in good faith in tandem with attempts by the U.S. government to establish an MLAT treaty with the other country's government.

Figure 5: Examples of How U.S. Law Enforcement Can Compel Access to Data Through the Proposed Balanced Approach



Ultimately, issues concerning cross-border access to data for law enforcement are not a problem that the United States or any single nation can solve. Questions of jurisdiction and access to data will require international cooperation. For this proposed approach to work, the United States and like-minded countries will need to enact some significant rule changes.

First, MLAT processes will need significant improvements to bring them in line with the demands of modern investigators. Because the framework is primarily based on the location of the data, this approach relies on the effectiveness, efficiency, and reach of MLATs and

other international agreements. However, existing MLATs have significant technological and procedural issues. Countries should work together to develop "MLAT 2.0" agreements, increasing the effectiveness and modernizing the processes by which countries coordinate with one another. This process will involve ensuring countries can easily access data located across one another's borders through agreed upon methods, as well as modernizing how law enforcement agencies can submit and track MLAT 2.0 requests electronically and reduce response times. Recommendations for these concepts will be explored in further detail below.

Second, companies with a domestic presence should not store data in countries with conflicting laws that do not allow them to comply with legal processes to aid in domestic law enforcement investigations (or foreign ones), whether that is through a treaty (e.g., MLAT 2.0) or domestic legal authorization (e.g., a SCA warrant) when no treaty exists. Importantly, companies could still operate in non-MLAT countries and can choose to store data in all countries where there are no conflicting laws. This component of the proposal should be used to incentivize more participation in MLAT 2.0 agreements between countries and prevent the establishment of data havens that are beyond the rule of law. But this requirement is not an attempt at data localization, a policy that restricts companies from transferring data outside of a country's borders, because companies would be under no obligation to store data domestically. Countries participating in MLAT 2.0 treaties should also push back against data localization policies as these would be unnecessary for law enforcement access, especially for those countries that adopt this framework.

This approach avoids the drawbacks of approaches based solely on location of data, location of business, or location of person. By first deferring to international agreements and working in good faith to establish them where none exist, the U.S. government can push back against other countries' attempts to compel extraterritorial access to data stored in the United States. In addition, this approach will ensure that the U.S. government's actions do not conflict with its international agreements. All countries should be held to their commitments, and should not enact policies that conflict with formal international agreements. Furthermore, this approach gives law enforcement additional power to investigate crimes and prevent terrorism across borders where there are no formal international agreements. This approach will help modernize authorizations to better deal with cross-border crimes.

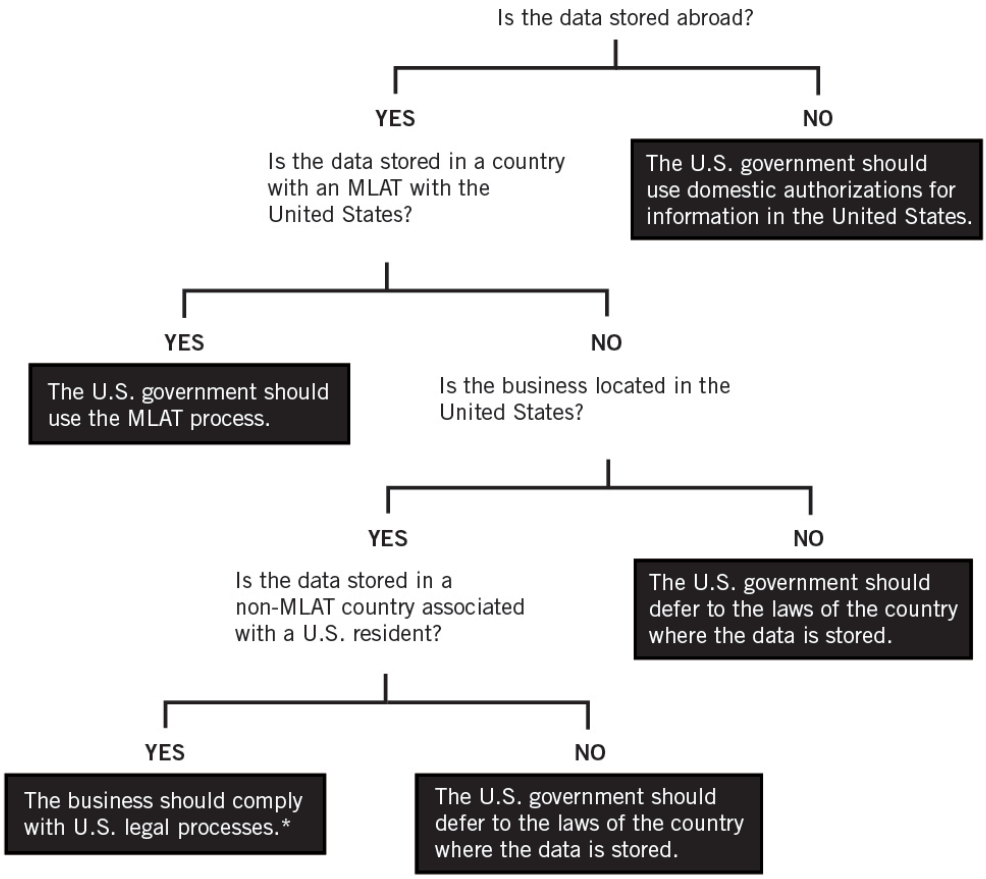
How This Framework Would Work in Practice

Nations around the world should use this framework to decide what processes to use to compel access to data stored abroad. As figure 6 illustrates, law enforcement officials should consider the location of the data, company, and data subject in their decisionmaking when pursuing criminal investigations.

The first question is where the data sought by law enforcement officials is stored. If the data is stored in the country, then law enforcement officials should be able to use domestic legal authorizations to compel production of the data. For example, if the data is stored in

the United States, U.S. law enforcement should be able to use a subpoena, court order, or warrant to compel production of that data, whether the company is foreign or domestic. This step does not assume the citizenship or location of the data subject.

Figure 6: How the U.S. Government Should Evaluate What Jurisdictional Test to Follow



* U.S. businesses should not store data in any country that does not allow them to comply with established legal processes whether U.S. legal processes or MLAT processes.

If the data is stored abroad, then the second consideration is whether the law enforcement conducting the investigation has a modern agreement for legal assistance (MLAT 2.0) with the country where the data reside. If there is a treaty or agreement, then the country's law enforcement should respect that agreement, regardless of the locations of the data subject or the company that stores the data. For example, if the U.S. government discovers that data it needs for a criminal investigation is located abroad in a country it has an MLAT 2.0 with, then U.S. law enforcement agencies should work with their foreign counterpart to compel production of the information. The MLAT 2.0 should obligate countries to provide timely legal assistance to all lawful cases except under narrow circumstances (e.g., an investigation would interfere with national security). This step assumes the company has a legal presence in both countries, but does not assume the citizenship or location of the data subject.[89]

Third, if the government does not have an updated treaty or agreement with a country and there is no easy other method of international cooperation to acquire the data, then that country's law enforcement officials should consider the legal presence of the business storing the data. If the business is only located abroad, then the U.S. government should defer to the laws of the country hosting the data. However, if there are no conflicting laws and the U.S. government has jurisdiction over the company holding the data, then U.S. law enforcement may use domestic authorizations to compel access to that data (see next step).

Finally, if the business has a legal presence within the United States, the U.S. government should consider the individual or individuals that are the target of the investigation. If the data subject is located within the country where the investigation is taking place, then that country's government should be able to use domestic legal processes to acquire the data from the company. For example, if the data subject is in the United States, then the U.S. government should issue a warrant to acquire the data from the company storing the person's data. If the data subject is located abroad, the U.S. government should defer to the laws of the country hosting the data. If the government cannot determine where the data is located or the location of the data subject, then if law enforcement has jurisdiction over the company holding the data, it should use domestic legal authorizations to compel access. To ensure law enforcement agencies can effectively prosecute crimes and prevent terrorism, businesses based in MLAT 2.0 countries should not store data in any country that does not allow them to comply with legal processes in other countries where they do business.

This framework comes with a few caveats and drawbacks. For example, U.S. law enforcement would find it difficult to acquire evidence from a business with no legal presence in the United States or data stored in a country that has no treaty or agreement with the U.S. government. However, we estimate the likelihood of such a fringe case impeding a domestic criminal investigation to be small. Similarly, as with each of these jurisdictional tests, this hybrid framework assumes law enforcement can establish the location of the data, business, and data subject. As we previously explained, current technology can make identifying these relevant details difficult to accomplish. But as noted above, there is no perfect solution that optimizes all parameters; only solutions that are better than others.

How U.S. Policymakers Should Update Processes to Optimize this Approach

To optimize this hybrid approach, the U.S. government will need to update its laws and processes to better keep up with the demands of law enforcement in the digital age. This will require updates to ECPA and domestic MLAT processes. These changes should be in tandem with good-faith efforts to establish model MLAT agreements with all countries around the world and, more generally, international legal standards for government access to data. Furthermore, like-minded nations should use this opportunity to push back against ill-advised data localization policies.

The U.S. Congress Should Fund, Modernize, and Strengthen the MLAT process

The U.S. government should take the lead in creating a timely and efficient international framework for allowing foreign governments to request access to data stored within the United States, pressing other countries to follow suit. Streamlining the response time for the DOJ to its foreign counterparts will alleviate many of the concerns brought on by the hybrid approach, including weakening the incentives for data localization.

Since 2000, the number of requests from foreign authorities handled by the DOJ has increased nearly 85 percent.[90] A 2013 report interviewed several U.S. officials, concluding that electronic evidence transfers are the most resource-intensive demands on the DOJ's Office of International Affairs.[91] In 2015, the DOJ requested an additional $24 million in its budget to hire additional personnel to handle MLAT requests and train foreign law enforcement officials about how to meet U.S. evidentiary standards for MLAT requests.[92] The request also sought to expand MLAT responsibilities to the Federal Bureau of Investigation by creating a dedicated unit managing intake and tracking of MLAT requests.[93] In 2015, Congress partially funded this request ($20 million). The request increased to $32 million and 141 positions related to MLAT reform in 2016.[94] But this request was denied. In 2017, the DOJ requested $10 million for the same purposes, including the hiring of 97 positions related to MLAT reform.[95] The U.S. Congress should give DOJ the funding it needs to modernize how it can respond to foreign MLAT requests.

In addition to funding, Congress should direct the DOJ to review and streamline the process it uses to fulfill foreign MLAT requests. The 114th Congress considered several pieces of legislation that would improve the effectiveness and efficiency of this process, including provisions in ICPA.[96] The 115th Congress should pass similar legislation to improve the MLAT process. For example, Congress should direct DOJ to create an online submission process for MLAT requests on the DOJ's website, improving how these requests are submitted and tracked. Similarly, Congress should direct DOJ to create an online docketing system for all MLAT requests to allow foreign governments to track the status of their requests, improving the overall transparency of the system. In addition, Congress should direct DOJ to consolidate the Office of International Affairs' and the U.S. Attorney's Office's MLAT review functions for digital communications requests into a single office.[97] This docketing system should be capable of reporting performance metrics such as the number of MLAT requests received, the response time for requests, and the status of pending requests. Finally, Congress should direct DOJ to allow record holders (e.g., U.S.-based service providers) to provide information directly to the requesting law enforcement agency through the docketing system, thereby reducing overall response time.[98] Currently, DOJ reviews all data it receives from companies pursuant to an MLAT request before forwarding that data to the requesting government (figure 1). However, because both DOJ and the U.S. Attorney's office have already cleared this request before serving it on the company, this step is unnecessary.

By funding the DOJ's ability to streamline and modernize MLAT processing as well as hire additional staff, Congress can improve MLAT response time. Cutting this response time

from 10 months to a matter of weeks would help reduce tensions with other countries that have MLATS with the United States, making distinctions inconsequential for legitimate law enforcement requests.

The U.S. Government Should Work with its Foreign Partners and International Economic Forums to Draft and Adopt Model MLAT 2.0 Agreements

Since 1977, the U.S. government has negotiated 65 MLAT treaties with foreign governments, including the Umbrella agreement with each member state of the European Union and the Inter American Convention on Mutual Legal Assistance with members of the Organization of American States.[99] In addition, the U.S. government has established bilateral executive agreements on forfeiture cooperation with 20 countries.[100] However, the various components and standards of the MLAT agreements vary. Furthermore, while the United States has established the most MLAT agreements, there are still many countries on every continent with which the U.S. government does not have a treaty. And many other nations around the world also do not have comprehensive MLAT agreements. For example, the French government only has these agreements with five other countries, Australia, Canada, Hong Kong, India, and the United States.[101]

To encourage more countries to adopt MLATs with each other, governments must first standardize and strengthen these agreements. The U.S. government should work with major economic organizations and forums, such as the European Union, the Organization of American States, and Asia Pacific Economic Cooperation (APEC) to establish and adopt model MLAT language, or "MLAT 2.0." This treaty should create a common process so that governments no longer need to individually negotiate agreements with one another, but can sign onto a standard agreement across many nations. The goals of MLAT 2.0 will be four-fold. First, MLAT 2.0 should create a common framework for when and how countries can use domestic authorizations to access data outside their borders. This may include arrangements such as reciprocal recognition of domestic search warrants when countries meet certain legal standards, to expedite the process. Similarly, the agreement may include comity analyses or notice requirements as a condition of this reciprocal recognition. Second, MLAT 2.0 should commit countries to modernizing their methods for responding to foreign data requests, such as through the processes outlined in the previous recommendation. Third, countries should commit to complying with their counterpart's lawful requests for data in a timely fashion, unless those requests would violate mutually-agreed upon provisions, such as for national security reasons. Fourth, countries should report the number of requests they receive, the number of requests they fulfill, response times, and progress in their modernization efforts. The goal of reporting is to hold participating nations publicly accountable for their timeliness in adopting and modernizing MLAT processes, as well as to identify inefficiencies in the process.

Once adopted, each country should push their trading partners to use this MLAT 2.0, encouraging more countries to adopt improved MLATs with one another. The U.S. government should then work in good faith to update its MLATs to fit this model and establish new MLATs with countries where no treaty currently exists. Working in tandem

with the approach to cross-border law enforcement requests, the U.S. government and these economic forums can streamline and expand the number of countries with MLATs. By establishing these model agreements, the U.S. government can build an alliance against bad actor countries (i.e. data havens), which would reduce the likelihood of U.S. law enforcement encountering a situation where they cannot compel access to data.

In addition, the U.S. DOJ and U.S. Department of State should host an annual global workshop on international mutual legal assistance. The workshop should focus on how to modernize MLAT agreements to update and improve the handling of requests for evidence by both the U.S. government and its foreign partners. In addition, the workshop can support training efforts for foreign law enforcement to ensure they can meet U.S. evidentiary standards, which will improve how the DOJ can respond to MLAT requests.

The U.S. Government Should Work with its Allies to Push Back Against Foreign Data Localization Requirements and Data Havens

Countries that adopt MLAT 2.0 should also pledge not to impose data localization restrictions on companies for law enforcement purposes. Indeed, as the Information Technology and Innovation Foundation has shown in previous reports, there is no benefit to privacy or cybersecurity based on geographical location.[102] With this approach and an efficient MLAT process, the same would be true for law enforcement access to data. In fact, if other countries adopt data localization policies, countries would not be able to fully reap the benefits of the approach advocated in this report because the more siloed the system gets the more countries may try to stop their counterparts from accessing data stored within their borders. Indeed, many governments already see limiting foreign investigations as a justification for enacting data localization policies.[103] Therefore, all countries using this framework should actively push back against data localization efforts by other countries through trade agreements or by establish MLAT 2.0 for their own country.

As part of these efforts, Congress should work with DOJ and the U.S. Trade Representative to label countries that attempt to circumvent international processes for providing law enforcement agencies lawful access to data as "data havens." These countries would not be those that merely fail to create MLATs with other countries, but rather those who actively attempt to circumvent lawful investigations, thus creating a refuge for companies that allow criminal activity. For extreme cases and as a last resort when MLAT negotiations fail, Congress should consider blocking access to services from countries labeled as unlawful data havens in the United States.[104]

Congress Should Pass Legislation to Update ECPA to Protect Domestic Digital Communications

The U.S. Congress should pass the Email Privacy Act, introduced by Representatives Kevin Yoder (R-KS) and Jared Polis (D-CO), which would impose a uniform warrant requirement for law enforcement to compel access to users' content, such as emails.[105] This law would remove unnecessary legal loopholes that treat digital content differently than physical content. For example, one loophole allows law enforcement to gain access to email content stored with a cloud provider using a less-rigorous subpoena after just 180 days. If

the email is under 180 days old, law enforcement must seek a warrant to access it, which requires a stricter evidentiary standard than subpoenas. While the current DOJ does not actively enforce this loophole, it could choose to do so in the future. The Email Privacy Act would close this loophole once and for all. This legislation would ensure ECPA does not treat data differently based on where and how it is stored, and would safeguard the privacy of U.S. persons without compromising law enforcement's ability to prosecute and solve crimes.

Congress Should Restrict Companies from Storing Data in Non-MLAT Countries That Prohibit Companies from Complying with U.S. Law Enforcement Domestic Authorizations

In order for the approach proposed in the report to be effective, companies cannot be allowed to store data outside of the reach of domestic law enforcement. This step requires that the U.S. Congress prohibit companies from storing data on U.S. persons in countries that do not have an MLAT with the U.S. government and that have domestic laws preventing U.S. companies from complying with U.S. requests for data on U.S. persons. This rule would only prohibit companies from storing data in another country if it passes conflicting laws that would restrict it from sharing data with U.S. law enforcement when served with domestic legal authorizations (in lieu of an MLAT). To accomplish this, Congress should set a deadline of five years for countries to eliminate conflicting laws or establish an MLAT with the United States, after which this rule would take effect. After the deadline, U.S. companies would not be able to store data in that country unless given a waiver by U.S. DOJ if that country is currently in the process of negotiating an MLAT agreement with the United States or is removing its conflicting laws. Moreover, U.S. trade negotiators should insist that other nations not use this provision to limit data flows to the United States if the U.S. government is willing to negotiate an MLAT with the foreign government.

The U.S. Government Should Work with its Allies to Establish International Legal Standards for Government Access to Data

The global nature of the Internet makes access to information by law enforcement difficult to enforce and legal jurisdictions hard to define. As the threat of cybercrime rises and the importance of trade in digital goods and services in our global economy continues to grow, there is an increasing need for clarity on these questions, particularly regarding government access to data outside of its borders.

Therefore, the United States should engage with its trade partners to develop a "Geneva Convention on the Status of Data."[106] This would create a multi-lateral agreement that would establish international rules for transparency, settle questions of jurisdiction, engender cooperation for better coordination of international law enforcement requests, and limit unnecessary access by governments to citizens of other countries. This would also help countries to follow similar rules and procedures for cross-border law enforcement requests and actions. The agreement would also address the issues of localization and barriers to data flows. In addition, a multilateral agreement could clarify which country's laws take precedence when companies encounter conflicting rules.

Conclusion

The framework discussed in this report is conceptually simple; it is necessary to ensure law enforcement has access to the data it needs to further criminal investigations while respecting the national sovereignty of other countries. The U.S. government should lead by example by creating a timely and efficient international framework for allowing governments to request access to data stored within its borders and abroad. This framework would help meet the needs of law enforcement agencies operating in a digital world and keep the U.S. tech sector competitive globally by making border distinctions inconsequential for legitimate law enforcement requests.

Just as aeronautical law evolved to support the expansion of global civil aviation, international maritime law advanced to support the development of a global shipping industry, and international space law governs the exploration and use of outer space, so too should international stakeholders construct a framework to govern how law enforcement agencies can work together to solve crimes in the global data economy.

ENDNOTES

1. The user in the case enters in a "country code" at registration, which Microsoft uses to migrate that user's data to the closest data center, which is in Dublin, Ireland. At the time that the warrant was issued, the U.S. government did not know where the data were stored. Microsoft Corporation v. United States, 15 F. Supp. 3d 466 (S.D.N.Y. 2014), *Document Cloud*, 3, http://www.documentcloud.org/documents/1149373-in-re-matter-of-warrant.html.
2. Ibid.
3. Such as protections outlined in Electronic Communications Privacy Act of 1986, 18 U.S.C. §121 (1986).
4. Nigel Cory, "Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
5. "Convention on Cybercrime, European Treaty Series – No 185" (Council of Europe, November 23, 2001), accessed July 12, 2017, https://rm.coe.int/1680081561.
6. Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy" (Information Technology and Innovation Foundation, September 2014), http://www2.itif.org/2014-crossborder-internet-policy.pdf.
7. Jeeyoung Kim, "How Sharding Works," *Medium*, December 5, 2014, https://medium.com/@jeeyoungk/how-sharding-works-b4dec46b3f6.
8. There is divided precedent, with several magistrate courts affirming such authority and one appellate court rejecting it. For examples, see: In re. two email accounts stored at Google, Inc., Case No. 17-M-1234, Case No. 17-M-1235, 2017 WL 706307 (E.D.Wis. 2017), *Just Security,* https://www.justsecurity.org/wp-content/uploads/2017/04/Google.Yahoo_.pdf; In re. Search of Yahoo, Inc., No. 6:17-mj-1238 (M.D. Fla. 2017), *Just Security*, https://www.justsecurity.org/wp-content/uploads/2017/04/Florida-case.pdf; In re Search Warrant No. 16-960-M-01 to Google, Inc, Misc. No. 16-960-M-01, 2017 WL 471564 (E.D.Pa. 2017), *Washington Post*, https://www.washingtonpost.com/news/volokh-conspiracy/wp-content/uploads/sites/14/2017/02/Opinion.pdf?tid=a_inl; with a differing opinion in Microsoft Corporation v. United States, No. 14-2985 (2d Cir. 2017).
9. Electronic Communications Privacy Act of 1986, 18 U.S.C. §121 (1986).
10. The Government has also argued that a subpoena can compel disclosure of opened email regardless of age. See: "Microsoft Ireland Case: Backgrounder," (Center for Democracy and Technology, July 17, 2014), https://cdt.org/files/2014/07/Microsoft-Ireland-Memo-formatted.pdf.
11. Reforming the Electronic Communications Privacy Act, 113th Cong. (March 19, 2013) (testimony of Elana Tyrangiel, acting assistant attorney general of the U.S. Justice Department), *U.S. Department of Justice*, accessed July 14, 2017, https://www.justice.gov/opa/speech/acting-assistant-attorney-general-elana-tyrangiel-testifies-us-house-judiciary; Warshak v. United States, 631 F.3d 266; 2010 WL 5071766 (6d Cir. 2010), http://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf.
12. "Google Transparency Report" (Google, 2017), accessed June 28. 2017, https://www.google.com/transparencyreport/userdatarequests/legalprocess/.
13. Bank of Nova Scotia v. United States of America, 740 F.2d 817, (11th Cir. 1984), *Justia*, http://law.justia.com/cases/federal/appellate-courts/F2/740/817/233788/.
14. "279 Subpoenas," *Offices of the U.S. Attorneys,* accessed June 29, 2017, https://www.justice.gov/usam/criminal-resource-manual-279-subpoenas.
15. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2703(d) (1986).
16. "Google Transparency Report," Google.
17. Microsoft Corporation v. United States, No. 14-2985 (2d Cir. 2017).
18. Winston Maxwell and Christopher Wolf, "A Global Reality: Governmental Access to Data in the Cloud," (Hogan Lovells, July 18, 2012), accessed June 28, 2017.

http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf.

19. Peter Swire and Debrae Kennedy-Mayo, "How Both the EU and the U.S. are 'Stricter' than Each Other for the Privacy of Government Requests for Information," *Emory Law Journal*, Vol. 66:617, 2017, 644, http://law.emory.edu/elj/_documents/volumes/66/3/swire-kennedy-mayo.pdf.
20. Alan McQuinn and Daniel Castro, "Congress Needs to Check Government Hacking Powers," *Christian Science Monitor*, December 14, 2016, accessed July 17. 2017, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/1214/Opinion-Congress-needs-to-check-government-hacking-powers.
21. Leslie Caldwell, "Rule 41 Changes a Judge May Consider Warrants For Certain Remote Searches," *U.S. Department of Justice*, June 20, 2016, accessed July 17, 2017, https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.
22. Foreign Intelligence Surveillance Act (1978), 50 18 U.S.C. Ch. 36 (2015), Cornell University, https://www.law.cornell.edu/uscode/text/50/chapter-36.
23. If the metadata of a target citizen is deemed "relevant" to an investigation into terrorism or clandestine activities, the FBI can send a national security letter to a provider to access non-content, and the provider is prohibited from revealing receipt of the letter for 180 days. These letters are authorized by several federal statutes, including the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2709 (1986); the National Security Act of 1947, 50 U.S.C. § 3162 (1947); the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3414 (1978); the Fair Credit Reporting Act of 1970, 15 U.S.C. §1681u, v.); and the USA PATRIOT Act of 2001, Section 505, P.L. 107-56, 115 Stat. 365-66 (2001).
24. "Termination Procedures for National Security Letter Nondisclosure Requirement," *Federal Bureau of Investigation*, November 24, 2015, accessed June 30, 2017, https://www.fbi.gov/file-repository/nsl-ndp-procedures.pdf/view.
25. Ibid.
26. In re National Security Letter, No. C 11-02173 SI (N.D. Cal. 2013), *Electronic Frontier Foundation*, https://www.eff.org/document/nsl-ruling-march-14-2013; Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, 18 U.S. Code § 2709 (2015). Several companies and activist groups are currently challenging national security letters and other gag orders under 18 U.S. Code § 2709. See, Andrew Crocker, "Adobe puts an End to Indefinite Gag Orders," *Electronic Frontier Foundation*, April 24, 2017, accessed July 14, 2017, https://www.eff.org/deeplinks/2017/04/adobe-puts-end-indefinite-gag-order.
27. Winston Maxwell and Christopher Wolf, "A Global Reality: Governmental Access to Data in the Cloud."
28. "2016 International Narcotics Control Strategy Report" (Bureau of International Narcotics Control, U.S. Department of State, 2016), accessed March 28, 2017, https://www.state.gov/j/inl/rls/nrcrpt/2016/vol2/253357.htm.
29. "2014 International Narcotics Control Strategy Report," *Bureau of International Narcotics Control,* U.S. Department of State, 2014, accessed March 28, 2017, https://www.state.gov/j/inl/rls/nrcrpt/2014/vol2/222469.htm.
30. Ibid.
31. The United Nations Convention against Transnational Organized Crime, United Nations, 2000, accessed July 13, 2017, https://www.unodc.org/unodc/en/treaties/CTOC/.
32. Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses, U.S.-E.U., 2016, accessed June 20, 2017, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.
33. Peter Swire and Justin Hemmings, "Re-Engineering the Mutual Legal Assistance Treaty Process," *Draft for NYU Law and PLSC Conferences,* May 14, 2015, accessed June 29, 2017, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahU

KEwjTusWFmePUAhWCOT4KHbnzCPoQFggkMAA&url=http%3A%2F%2Fwww.heinz.cmu.edu%2F~acquisti%2FSHB2015%2FSwire.docx&usg=AFQjCNEAFPmCRy3DHAk0XI9VrMDMCLqt1w.

34. "Mutual Legal Assistance Treaty with Switzerland 94-2" (Swedish Federal Department of Justice and Police, January 25, 1973), accessed June 30, 2017, https://www.rhf.admin.ch/dam/data/rhf/strafrecht/rechtsgrundlagen/sr-0-351-933-6-e.pdf.
35. "Performance Budget, FY 2017 President's Budget," (Criminal Division, U.S. Department of Justice, 2017), accessed June 28, 2017, https://www.justice.gov/jmd/file/820926/download.
36. Microsoft Corporation v. United States, No. 14-2985 (2d Cir. 2017), "Government's Memorandum of Law in Opposition to Microsoft's Motion," (Preet Bharara, Attorney for the United States, April 20, 2014), *Just Security*, accessed June 29, 2017, https://www.justsecurity.org/wp-content/uploads/2014/05/Governments-Memorandum-of-Law-in-Opposition-to-Motion-to-Vacate-doc-97....pdf.
37. Different types of digital content follow different MLAT procedures. Hearing on International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests, 114th Cong. (February 25, 2016) (testimony of Jennifer Daskal, assistant professor at American University Washington College of Law), *Just Security*, accessed June 29, 2017, https://www.justsecurity.org/wp-content/uploads/2016/02/WrittenStatement-Daskal-HouseJudiciary-022516.pdf; Corey Smith, "Obtaining Foreign Evidence Outside of the Mutual Legal Assistance Treaty Process," *U.S. Attorney's Bulletin*, March 2017, accessed July 12, 2017, http://www.assetsearchblog.com/wp-content/uploads/sites/197/migrated/USABulletin07.pdf.
38. "FY 2017 Budget Request – National Security" (U.S. Department of Justice, 2016), accessed June 29, 2017, https://www.justice.gov/jmd/file/822376/download.
39. Richard Clarke et al., "Liberty and Security in a Changing World" (White House, December 18, 2013), accessed June 29, 2017, 227, https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world.
40. See Projected OIA Backlog Increases FY 2015-2020, "FY 2016 President's Budget" (Criminal Division, Department of Justice, 2016), accessed June 29, 2017, 25, https://www.justice.gov/sites/default/files/jmd/pages/attachments/2015/02/02/10._criminal_division_crm.pdf.
41. "Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges" (Federal Judicial Center International Litigation Guide, 2014), accessed June 28, 2017, 8-10, https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf.
42. United States v. $93,110.00 in U.S. Currency; No. 2:08-cv-01499-MHB (D. Ariz. 2010), *Court Listener*, https://www.courtlistener.com/docket/4132440/united-states-v-9311000-in-us-currency/.
43. *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights*, 115th Cong. (May 24, 2017) (testimony of Brad Wiegmann, Deputy Assistant Attorney General of the U.S. Department of Justice), accessed July 12, 2017, https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf.
44. Virginia Kendall and T. Markus Funk, Child Exploitation and Trafficking: Examining Global Challenges and U.S. Responses, (Maryland: Rowman & Littlefield, 2012), 215.
45. Bradley Barth, "Cybercriminals find many safe havens," *SC Magazine*, November 1, 2016, accessed July 12, 2017, https://www.scmagazine.com/cybercriminals-find-many-safe-havens/article/569177/.
46. Jeff Roberts, "Russian Hackers Are Afraid to Travel After U.S. Arrests Spam King," *Fortune*, April 11, 2017, accessed July 12, 2017, http://fortune.com/2017/04/11/russian-hackers-levashov-arrest/.
47. Stolen Asset Recovery Initiative, "Requesting Mutual Legal Assistance in Criminal Matters from G20 Countries: A Step-by-step Guide" (World Bank and UNODC, 2012), accessed June 29, 2017, https://star.worldbank.org/star/sites/star/files/los_cabos_2012_mla_guide.pdf.
48 "Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges," Federal Judicial Center International Litigation Guide.
49. Ibid; "Preparation of Letters Rogatory" (U.S. Department of State), accessed June 29, 2017, https://travel.state.gov/content/travel/en/legal-considerations/judicial/obtaining-evidence/preparation-letters-rogatory.html.

50. Michael Walton, "Informal Transnational Police-to-Police Information Sharing: It's Structure and Reform," *Osgoode Hall Law School of York University*, 2016, accessed June 29, 2017, http://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1001&context=llm.
51. "An Organization Under International Law," *INTERPOL*, accessed June 29. 2017, https://www.interpol.int/About-INTERPOL/Legal-materials/An-organization-under-international-law.
52. "Informal Transnational Police-to-Police Information Sharing: It's Structure and Reform."
53. Kate Westmoreland, "ECPA Reform is Not Just a U.S. Issue" (Center for Internet and Society, April 10, 2014), accessed June 29, 2017, http://cyberlaw.stanford.edu/blog/2014/04/ecpa-reform-not-just-us-issue.
54. Brad Smith, "In the Cloud We Trust," *Microsoft*, January 21, 2015, accessed June 29, 2017, https://news.microsoft.com/stories/inthecloudwetrust/.
55. See the Brazilian Prosecutor Federico Meinberg Ceroy's remarks. Martin Kaste, "For U.S. Tech Firms Abroad and Data in the Cloud, Whose laws Apply?" *NPR*, March 3, 2016, accessed June 29, 2017, http://www.npr.org/sections/alltechconsidered/2016/03/03/469066176/for-u-s-tech-firms-abroad-and-data-in-the-cloud-whose-laws-apply.
56. "Frequently Asked Question," *MLAT.Info*, accessed June 29, 2017, https://mlat.info/faq.
57. Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015).
58. International Communications Privacy Act, S. 2986, 114th Cong. (2016).
59. Senator Orrin Hatch, "Hatch's International Communication Privacy Act (ICPA) Praised in Hearing," press release, May 24, 2017, accessed June 29, 2017, https://www.hatch.senate.gov/public/index.cfm/2017/5/hatch-s-international-communication-privacy-act-icpa-praised-in-hearing.
60. Microsoft Corporation v. United States, No. 14-2985 (2d Cir. 2017).
61. Ibid.
62. Joe Uchill, "DOJ Applied to take Microsoft Data Warrant Case to Supreme Court," *The Hill*, June 23, 2017, accessed July 12, 2017, http://thehill.com/policy/cybersecurity/339281-doj-applies-to-take-microsoft-data-warrant-case-to-supreme-court.
63. "2016 International Narcotics Control Strategy Report," *Bureau of International Narcotics Control,*
64. Bureau of International Narcotics and Law Enforcement Affairs, "Treaties, Agreements, and Asset Sharing," *U.S. State Department*, 2014, accessed June 29, 2017, https://www.state.gov/j/inl/rls/nrcrpt/2014/vol2/222469.htm.
65. Lothar Determann and Michaela Weigl, "Data Residency Requirements Creeping into German Law," *Bloomberg BNA*, April 11, 2016, http://www.bna.com/data-residency-requirements-n57982069680/.
66. Nicholas Shaxson, "Explainer: What is a Tax Haven?," *Guardian,* January 9, 2011, accessed June 29, 2017, https://www.theguardian.com/business/2011/jan/09/explainer-what-is-tax-haven.
67. "2016 Special 201 Report" (U.S. Trade Representative, April 2016), accessed June 29, 2017, https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf.
68. Bank of Nova Scotia v. United States of America.
69. "279 Subpoenas," *Offices of the U.S. Attorneys,* accessed June 29, 2017, https://www.justice.gov/usam/criminal-resource-manual-279-subpoenas.
70. Microsoft Corporation v. United States, 15 F. Supp. 3d 466 (S.D.N.Y. 2014).
71. Microsoft has since begun to store data in countries that allow it to share information with the Brazilian government as shown in its transparency reporting. "Law Enforcement Requests Report" (Microsoft, 2016), accessed July 12, 2017, https://www.microsoft.com/en-us/about/corporate-responsibility/lerr; Smith, "In the Cloud We Trust."
72. "On the Handling of Criminal Cases to Collect and Review the Provisions of a Number of Issues to Determine the Electronic Data," *Supreme People's Procuratorate*, September 20, 2016, accessed June 29, 2017, http://www.spp.gov.cn/xwfbh/wsfbt/201609/t20160920_167380_1.shtml.
73. Susan Hennessey and Chris Mirasola, "Did China Quietly Authorize Law Enforcement to Access Data Anywhere in the World?" *Lawfare*, March 27, 2017, accessed June 29, 2017,https://lawfareblog.com/did-china-quietly-authorize-law-enforcement-access-data-anywhere-world.

74. Jaclyn Kerr, "The Digital Dictator's Dilemma: Internet Regulation and Political Control in Non-Democratic States," (Stanford University, October 16, 2014) accessed July 19, 2017, http://cisac.fsi.stanford.edu/sites/default/files/kerr_-_cisac_seminar_-_oct_2014_-_digital_dictators_dilemma.pdf.

75. Daniel Castro and Alan McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness" (Information Technology and Innovation Foundation, June 9, 2015), accessed June 29, 2017, https://itif.org/publications/2015/06/09/beyond-usa-freedom-act-how-us-surveillance-still-subverts-uscompetitiveness.

76. Anton Troianovski and Danny Yadron, "German Government Ends Verizon Contract," *Wall Street Journal*, June 26, 2014, accessed May 29, 2017, https://www.wsj.com/articles/german-government-ends-verizon-contract-1403802226.

77. Castro and McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness"; Angus Loten, "U.S. Cloud Firms 'Out Innovated' Competitors in Wake of NSA Leak," *Wall Street Journal*, August 4, 2016, accessed July 18, 2017, https://blogs.wsj.com/cio/2016/08/04/u-s-cloud-firms-out-innovated-competitors-in-wake-of-nsa-leak/?shareToken=st71be6ffadf574052ae75ea7a58717d86&reflink=article_email_share.

78. Letter from Viviane Reding to Sophie in't Veld, *European Parliament*, June 24, 2014, accessed June 30, 2017, http://www.nu.nl/files/nutech/Scan-Ares-MEP-in%27t-Veld-.pdf.

79. Jennifer Daskal, "A Microsoft Ireland Fix: Time to Act is Now!" *Just Security*, April 14, 2017, accessed July 11, 2017,https://www.justsecurity.org/39959/microsoft-ireland-fix-time-act-now/.

80. International Communications Privacy Act, S. 2986, 114th Cong. (2016).

81. Orin Kerr, "The Next Generation Communications Privacy Act," *University of Pennsylvania law Review,* Vol. 162: 373, 2014, 216, https://www.pennlawreview.com/print/162-U-Pa-L-Rev-373.pdf.

82. Ibid, 217.

83. There are still other purposes that countries claim when they enact localization policies, such as privacy or cybersecurity concerns. Cory, "Cross-Border Data Flows: Where are the Barriers, and What Do They Cost*?"* Information Technology and Innovation Foundation.

84. Andrew Tarantola, "VPNs: What They Do, How They Work, and Why You're Dumb for Not Using One," *Gizmodo*, March 26, 2013, accessed June 29, 2017, http://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one.

85. "Tor: overview," *Tor*, accessed June 29, 2017, https://www.torproject.org/about/overview.html.en.

86. "7 FAM 080 - Dual Nationality," *U.S. Department of State*, December 10, 2012, accessed June 29, 2017, https://fam.state.gov/fam/07fam/07fam0080.html.

87. "Renouncing your Iranian Nationality," *Islamic Republic of Iran*, accessed June 29, 2017, http://www.mfa.gov.ir/index.aspx?siteid=3&pageid=24718; Zahra Alipour, "How dual nationality became a key controversy in Iran," *AL-Monitor*, October 25, 2016, accessed June 29, 2017, http://www.al-monitor.com/pulse/originals/2016/10/iran-dual-nationals-citizenship-key-controversy.html#ixzz4lQ2pgzbF.

88. Daniel Castro and Rob Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy" (Information Technology and Innovation Foundation, September 2014), http://www2.itif.org/2014-crossborder-internet-policy.pdf.

89. If the company does not have legal presence in the country where law enforcement officials are conducting the investigation, then those officials should still follow MLAT processes.

90. "Performance Budget, FY 2017 President's Budget" (Criminal Division, U.S. Department of Justice, 2017), accessed June 28, 2017, https://www.justice.gov/jmd/file/820926/download.

91. Ibid.

92. Department of Justice, "Attorney General Holder Announces President Obama's Budget Proposes $173 Million for Criminal Justice Reform," press release, March 4, 2015, accessed June 29, 2017, https://www.justice.gov/opa/pr/attorney-general-holder-announces-president-obama-s-budget-proposes-173-million-criminal.

93. FY 2014 had no current FBI services for MLAT reform initiatives. The FY 2015 request had $3.2 million and 14 positions, including 7 agents, for these FBI efforts. "FY 2015 Budget Request - Mutual Legal Assistance Treaty Process Reform" (U.S. Department of Justice, 2014), accessed June 29, 2017, https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.
94. "FY 2016 Budget Request – National Security" (U.S. Department of Justice, 2015), accessed June 29, 2017, https://www.justice.gov/sites/default/files/jmd/pages/attachments/2015/01/30/1_national_security_fact_sheet.pdf.
95. "FY 2017 Budget Request – National Security" (U.S. Department of Justice, 2016), accessed June 29, 2017, https://www.justice.gov/jmd/file/822376/download.
96. Congressman Tom Marino, "Reps. Marino, DelBene Introduce LEADS Act," press release, February 27, 2015, accessed June 29, 2017, https://marino.house.gov/media-center/press-releases/reps-marino-delbene-introduce-leads-act; Senator Orrin Hatch, "Hatch, Coons, and Heller Introduce Bipartisan LEADS Act to Protect Data Stored Abroad," press release, February 12, 2015, accessed June 29, 2017, https://www.hatch.senate.gov/public/index.cfm/2015/2/hatch-coons-and-heller-introduce-bipartisan-leads-act-to-protect-data-stored-abroad; Senator Orrin Hatch, "Hatch, Coons, Heller Introduce Bipartisan International Communications Privacy Act," press release, May 25, 2016,, accessed June 29, 2017, https://www.hatch.senate.gov/public/index.cfm/2016/5/hatch-coons-heller-introduce-bipartisan-international-communications-privacy-act.
97. Peter Swire and Justin Hemmings, "Re-Engineering the Mutual Legal Assistance Treaty Process." *Draft for NYU Law and PLSC Conferences.*
98. Ibid.
99. Inter-American Convention on Mutual Assistance in Criminal Matters, US-OAS, April 19, 1996, accessed June 30, 2017, https://www.oas.org/juridico/english/Treaties/a-55.html; Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses, U.S.-E.U., 2016, accessed June 20, 2017, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.
100. Bureau of International Narcotics and Law Enforcement Affairs, "Treaties, Agreements, and Asset Sharing." *U.S. State Department*, 2014.
101. "France," *MLAT.Info*, accessed June 29, 2017, https://mlat.info/country-profile/france.
102. Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), accessed June 29, 2017, http://www2.itif.org/2013-false-promise-data-nationalism.pdf; Cory, "Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?"
103. Castro and McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness."
104. Nigel Cory, "How Website Blocking Is Curbing Digital Piracy Without 'Breaking the Internet'," (Information Technology and Innovation Foundation, August 2016), accessed June 29, 2017, http://www2.itif.org/2016-website-blocking.pdf.
105. Email Privacy Act, H.R. 387, 115th Cong. (2017-2018).
106. Daniel Castro, "The False Promise of Data Nationalism."

ACKNOWLEDGMENTS

The authors wish to thank the following individuals for providing input to this report: Rob Atkinson, Alex Key and Sue Wonder. Any errors or omissions are the authors' alone.

ABOUT THE AUTHORS

Alan McQuinn is a research analyst at ITIF. His research areas include a variety of issues related to emerging technology and Internet policy, such as cybersecurity, privacy, virtual currencies, e-government, and commercial drones. Prior to joining ITIF, McQuinn was a telecommunications fellow for Representative Anna Eshoo (D-CA) and an intern for the Federal Communications Commission in the Office of Legislative Affairs. He got his B.S. in political communications and public relations from the University of Texas at Austin.

Daniel Castro is vice president of ITIF. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office, where he audited IT security and management controls at various government agencies. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as one of the world's leading science and technology think tanks, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.