Toward A Modern Statutory Framework For Law Enforcement Access To Electronic Communications

Viet D. Dinh & Jeffrey M. Harris

Viet D. Dinh is the founding partner of Bancroft PLLC. A leading expert on corporate governance and regulatory compliance, he has counseled corporations and their leaders on a range of transactional and governance issues. Dinh also advises individuals and organizations through high-stakes conflicts, existential risk, and national security issues. He is also Professorial Lecturer in Law and Distinguished Lecturer in Government at Georgetown University, where he specializes in corporations and constitutional law. He served as U.S. Assistant Attorney General for Legal Policy from 2001 to 2003, where he played a key role in developing legal policy initiatives to combat terrorism, including the USA Patriot Act. Dinh clerked for U.S. Supreme Court Justice Sandra Day O'Connor and for D.C. Circuit Judge Laurence H. Silberman. He graduated *magna cum laude* from Harvard College and Harvard Law School, where he was a Class Marshal and an Olin Research Fellow in Law and Economics.

Jeffrey M. Harris is a partner at Bancroft PLLC. His practice focuses on Supreme Court, appellate, and complex litigation, and he has handled cases involving constitutional law, national security, telecommunications, labor and employment, antitrust, criminal law, administrative law, intellectual property, and many other areas. Mr. Harris previously served as a law clerk to Chief Justice John G. Roberts, Jr., in the Supreme Court of the United States, and to Judges David B. Sentelle and Laurence H. Silberman of the U.S. Court of Appeals for the D.C. Circuit. He graduated *magna cum laude* from Harvard Law School in 2006, where he served as a senior editor on the *Harvard Journal of Law and Public Policy* and an officer of the Federalist Society.

Bancroft PLLC serves as counsel to Microsoft but the views expressed in this paper are solely those of the authors.

Executive Summary

Government access to email correspondence is currently governed by a statute—the Electronic Communications Privacy Act ("ECPA")—that is nearly 30 years old and was enacted when the Internet was still in its infancy. The ECPA framework was based on a world in which data storage was costly, the Internet was primarily used within the United States, and consumers had very different expectations of privacy than they do today. For example, ECPA provides different levels of privacy protection depending on whether emails have been stored for more or less than 180 days—a line that no longer makes any sense given that data storage costs have become *de minimis.* And ECPA says nothing whatsoever about how to resolve disputes that cross jurisdictional lines, such as when U.S. law enforcement officials seek email communications stored on a server in a foreign country.

There is broad agreement among consumers, technology companies, law enforcement officials, and other stakeholders that reform is badly needed. But interested parties have diverged about the best way to accomplish this goal. In this paper, we analyze two recent legislative proposals—the Law Enforcement Access to Data Stored Abroad Act ("LEADS Act") and the Email Privacy Act—and discuss the extent to which this legislation would remedy the flaws of the ECPA regime.

Both the LEADS Act and the Email Privacy Act would unquestionably fix several of ECPA's key deficiencies. In particular, both proposed statutes would eliminate the oft-criticized 180-day rule and provide that law enforcement officials must *always* obtain a search warrant to compel the disclosure of customers' private email communications. Both the LEADS Act and the Email Privacy Act would also promote constitutional values by providing that law enforcement must generally notify a customer within 10 days if that person's email communications have been disclosed pursuant to a warrant.

The LEADS Act would also improve upon the ECPA framework by clearly articulating the territorial scope of the warrant power. Under the LEADS Act, law enforcement could obtain a warrant to compel a provider to disclose: (1) emails that are physically stored within the United States; and (2) emails of U.S. nationals that are stored outside the United States. Both of those provisions are well-grounded in U.S. and international law. It is perhaps the most basic principle of national sovereignty that a country may exercise jurisdiction over persons or things that are *physically located* within its own territory. And it is equally well established that a country may exercise jurisdiction over its nationals even when they are not physically present in the country. For example, the United States requires its citizens to make annual disclosures of their foreign holdings, and has required certain multinational banks to disclose accounts held abroad by U.S. citizens. It is thus entirely consistent with existing law for the LEADS Act to allow law enforcement to access the communications of U.S. citizens with a warrant, even if those communications are stored on a server in a foreign country.

Moreover, the LEADS Act contains several other provisions that are designed to prevent inter-jurisdictional conflicts while promoting international cooperation in law enforcement investigations. For example, the LEADS Act provides that a warrant may be vacated or modified if the disclosure would violate the laws of a foreign country where the data is stored. This

provision helps minimize conflicts with foreign countries, and ensures that providers are not placed in the fraught position of having to choose between complying with U.S. law and complying with foreign law.

The LEADS Act also recognizes that inter-jurisdictional requests for information should primarily be handled through the well-established Mutual Legal Assistance Treaty ("MLAT") process. When one country seeks information about another country's nationals—such as when U.S. law enforcement officials seek information about foreign citizens that is stored on a server in a foreign country—this should be addressed on a government-to-government basis through an MLAT request. It is wholly inappropriate to insert an email provider into what is fundamentally a dispute between two sovereign nations. The LEADS Act recognizes the primacy of the MLAT process and makes several common-sense reforms to improve the efficiency and transparency of that process. In particular, the Act requires creation of a new online intake form for MLAT requests from foreign governments, and requires the Department of Justice to publish annual statistics about the number of MLAT requests the Department has made and the time it takes foreign governments to process those requests.

* * *

In this paper, we first provide an overview of existing law under ECPA. We then discuss the problems of that framework and the goals that should be accomplished by reform legislation. We then analyze the LEADS Act and the Email Privacy Act in detail, and discuss the ways in which these legislative proposals would improve upon the status quo. Either the LEADS Act or the Email Privacy Act would be an important step in the right direction towards modernizing and improving the ECPA framework, although the LEADS Act is somewhat more ambitious in scope given that it addresses the territorial scope of the warrant power and the process for resolving inter-jurisdictional conflicts. We conclude by discussing ways in which this proposed legislation can be further improved.

Analysis

I. OVERVIEW OF CURRENT LAW REGARDING LAW ENFORCEMENT ACCESS TO EMAIL CORRESPONDENCE.

Congress enacted the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848, in 1986 to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986); *see generally* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 378-90 (2014) (summarizing history of ECPA). Preexisting law, such as the Wiretap Act of 1968, focused primarily on privacy protections for telephone calls, and was woefully inadequate to address the unique issues raised by new methods of electronic communications such as email. The Supreme Court had also held that information "voluntarily conveyed" to a third party was not protected by the Fourth Amendment, *see United States v. Miller*, 425 U.S. 435, 442 (1976), which suggested that email messages—information "voluntarily conveyed" from a customer to an email provider—were entitled to little or no constitutional protection.

ECPA was designed to establish a regulatory framework for the protection—and disclosure—of new types of electronic communications that were becoming increasingly popular at the time. The statute creates new privacy rights for users of electronic communications services, broadly providing that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

At the same time, however, ECPA contains several exceptions to this prohibition that allow federal, state, and local law enforcement officials to gain access to electronic communications. If an electronic communication has been in "electronic storage in an electronic communications system" for 180 days or less, then law enforcement officials may compel disclosure of that communication only through a search warrant. *Id.* § 2703(a). In contrast, law enforcement officials can compel disclosure of communications that have been stored for more than 180 days merely by obtaining a subpoena. *Id.* § 2703(b); *see id.* § 2703(d) (subpoena may be issued by a court if there are "reasonable grounds to believe" that the contents of the electronic communication are "relevant and material" to a criminal investigation).

When ECPA was enacted in 1986, email services typically did not retain emails for longer than six months, and a user would have to take affirmative steps to save and store a message. *See* H.R. Rep. No. 99-647, at 72 (1986). Congress thus concluded that "[t]o the extent that the record (including e-mail message) is kept beyond that point (180 days) it is closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection." *Id.* at 68.

II. THE CURRENT REGULATORY REGIME IS BADLY OUTDATED AND IN NEED OF REFORM.

Although ECPA was hailed as an important privacy protection when it was enacted in 1986, its framework has been significantly undermined by recent developments in technology and commerce. ECPA also has several critical omissions—such as a lack of any guidance about whether, and to what extent, it applies extraterritorially—that have led to confusion and spawned litigation.

180 Day Rule: As noted, ECPA requires a warrant to compel a provider to disclose electronic communications that have been stored for 180 days or less, but allows law enforcement to obtain older emails simply by obtaining a subpoena. 18 U.S.C. § 2703(a). That 180-day rule was questionable even when it was first enacted, but it makes no sense at all today. Consumers now have access to massive amounts of electronic storage at little or no cost, and the fact that an individual has retained an email for longer than 180 days hardly suggests that the communication should be entitled to a lesser degree of privacy protection. If anything, the fact that a consumer has retained an email rather than deleting it should indicate that it is *more* deserving of protection.

The Sixth Circuit has held that—wholly apart from ECPA—the Fourth Amendment requires a warrant to compel disclosure of *any* email correspondence, regardless of how long it has been stored. *See United States v. Warshak*, 631 F.3d 266, 282-88 (6th Cir. 2010). In light of *Warshak*, all major email providers have taken the position that a warrant is *always* required to compel disclosure of a customer's electronic communications. But *Warshak* is technically binding only within the Sixth Circuit, and law enforcement agencies have taken conflicting positions about whether that rule should apply on a nationwide basis.[1] It would be wholly untenable to have a legal regime in which search warrants may be required to compel production of emails in some, but not all, areas of the country. It is thus imperative that Congress address this issue through comprehensive legislation that will apply on a *nationwide* basis and will give all interested stakeholders clear notice of when a warrant is needed to compel the disclosure of email communications.

Notice: ECPA requires the government to provide notice to an individual whose emails are searched pursuant to a *subpoena*. *See* 18 U.S.C. § 2703(b)(1)(B). But the statute also expressly provides that law enforcement need not provide notice to the subscriber if electronic communications are disclosed to the government pursuant to a search warrant. *Id.* § 2703(b)(1)(A). Thus, under current law, many consumers may never know if their email provider has given government officials access to their private correspondence.

Geographic Scope: When ECPA was enacted in 1986, most internet communications occurred within the United States, and thus "the territorial scope of ECPA was not the focus of attention." Kerr, *Next Generation Privacy Act*, at 406. But this issue has subsequently become "tremendously important," especially as U.S. companies serve an increasingly foreign customer

[1] *See, e.g.*, Declan McCullagh, *DOJ: We don't need warrants for e-mail, Facebook chats*, CNET.com (May 8, 2013) (noting that Department of Justice and IRS have taken different positions about whether search warrants are needed to obtain email correspondence), *available at* http://cnet.co/1MK7SeF.

base. *Id.* With the rapid globalization of the Internet and email communications, it is untenable that there is no clear statutory framework for resolving the inter-jurisdictional conflicts that will inevitably arise when law enforcement officials in one country seek access to records stored in another country.

For example, there have been sharp disputes over whether ECPA allows law enforcement to compel a provider to disclose email correspondence that is stored on a foreign server. In a case currently pending before the Second Circuit, the Department of Justice is seeking to compel Microsoft to produce emails that are located on servers in Dublin, Ireland. *See United States v. Microsoft*, No. 14-2985 (2d Cir. filed Aug. 12, 2014). Underscoring the importance of this issue, a diverse array of stakeholders—including Verizon, AT&T, AOL, Amazon, Apple, the Chamber of Commerce, the ACLU, the government of Ireland, and many others—have filed *amicus* briefs to express their position on the issues before the court.

The far better view of the law is that ECPA does not apply to emails stored in foreign countries because nothing in the statute *explicitly* provides for extraterritorial application. The Supreme Court has repeatedly held that "'[w]hen a statute gives no clear indication of an extraterritorial application, it has none.'" *Kiobel v. Royal Dutch Petroleum*, 133 S. Ct. 1659, 1664 (2013) (quoting *Morrison v. National Australia Bank*, 561 U.S. 247, 255 (2010)). This rule reflects a longstanding "presumption that United States law governs domestically but does not rule the world." *Id.* And there is a significant risk that foreign governments would view extraterritorial application of ECPA as impermissible meddling in their internal affairs.

In all events, regardless of which party is ultimately correct about whether ECPA has extraterritorial application, the very existence of this dispute only underscores the need for clear guidance from Congress about the territorial scope of the government's power to compel the disclosure of emails. The rules governing this critical issue should be established by Congress through comprehensive, nationally uniform legislation, rather than being addressed piecemeal on an *ad hoc* basis through judicial decisions.

III. ANALYSIS OF LEADING LEGISLATIVE REFORM PROPOSALS.

In this section, we analyze the proposed LEADS Act and Email Privacy Act, which are two of the leading proposals for reforming the outdated ECPA regime. The LEADS Act (S. 2871) was introduced on September 18, 2014 by Senators Orrin Hatch, Christopher Coons, and Dean Heller. The bill was reintroduced in the 114th Congress as S. 512 in the Senate and H.R. 1174 in the House. The Email Privacy Act was introduced in the House (H.R. 699) and Senate (S. 356) on February 4, 2015. That legislation was introduced by Senators Mike Lee and Patrick Leahy and Representatives Kevin Yoder and Jared Polis. Although the LEADS Act is somewhat more ambitious in scope and provides a more comprehensive solution than the Email Privacy Act, either would be a significant step in the right direction and would resolve several key problems of the ECPA regime.

A. Both the LEADS Act and the Email Privacy Act Would Update and Clarify Several Aspects of the ECPA Framework.

The LEADS Act and the Email Privacy Act both address several of the key shortcomings of ECPA. First, both statutes would update the ECPA framework by expressly eliminating the oft-criticized 180-day time limit for when a warrant is required instead of a subpoena. Section 3(a)(2)(A) of the LEADS Act provides that "[a] governmental entity may require the disclosure by a provider … of the contents of a wire or electronic communication that is in electronic storage … *only pursuant to a warrant*." Section 3(a)(1)(a) of the Email Privacy Act similarly provides that "[a] governmental entity may require the disclosure by a provider … of the contents of a wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider only if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Civil Procedure (or, in the case of a State court, issued using State warrant procedures)." Thus, consistent with the Sixth Circuit's *Warshak* decision and the current practice of major email providers, the government would *always* be required to obtain a warrant to compel the disclosure of email correspondence, and could not force a provider to disclose the contents of emails pursuant to a mere subpoena. The length of time that the emails had been stored would no longer be relevant to this inquiry. And there would no longer be a risk of having different standards for disclosure in different parts of the country.

Second, both the LEADS Act and the Email Privacy Act would remedy a critical deficiency in ECPA—and promote constitutional values of notice and due process—by ensuring that individuals receive notice whenever their electronic communications are disclosed to law enforcement officials. If a customer's emails are disclosed to the government pursuant to a warrant, the LEADS Act would generally require the government, within 10 days, to send the person a copy of the warrant and a notice that the person's emails have been provided to law enforcement. The Act would extend the notice period to 90 days if a court determines that there is "reason to believe that notification of the existence of the warrant may have an adverse result" on the investigation. The Email Privacy Act similarly requires that notice be provided to the subscriber within 10 days of the execution of a warrant, although it provides that the time for notification may be extended up to 180 days upon a showing that notification would threaten a person's physical safety, result in the destruction of evidence, or otherwise "seriously jeopardize" the investigation. Either one of these notice provisions would be a significant improvement over ECPA, which expressly provides that the government is *not* required to notify a user when his or her emails have been disclosed pursuant to a warrant. *See* 18 U.S.C. § 2703(b)(1)(A).

B. The LEADS Act Addresses the Territorial Scope of the Warrant Power in a Manner That Is Consistent With Longstanding Principles of U.S. and International Law.

In addition to eliminating the 180-day rule and providing greater notice to affected individuals, the LEADS Act also expressly addresses the *territorial* scope of the warrant power. That legislation would authorize the disclosure of: (1) electronic communications that are physically stored by the provider within the United States; and (2) communications that are stored within a foreign country but belong to a U.S. national. Section 3(a)(2)(A) provides that "a warrant issued pursuant to this subsection may be used to require the disclosure of contents of a wire or electronic communication that are in the provider's electronic storage within the United States or

otherwise stored, held, or maintained within the United States by the provider." And Section 3(a)(2)(B) provides that law enforcement can compel disclosure of the contents of an electronic communication with a warrant, regardless of where the communication is stored, if "the account-holder whose contents are sought by the warrant is a United States person."

These provisions regarding the territorial scope of the LEADS Act are grounded in longstanding principles of both U.S. law and international law. It is beyond dispute that a nation has jurisdiction over persons or things *physically present* within its territory. As the Supreme Court has recognized for more than two centuries, "[t]he jurisdiction of the nation within its own territory is necessarily exclusive and absolute," and is "susceptible of no limitation not imposed by itself." *The Schooner Exchange v. McFaddon*, 11 U.S. 116, 136 (1812). International law similarly recognizes that a nation may apply its law to "conduct that, wholly or in substantial part, takes place within its territory" and to "persons, or … things, present within its territory." Restatement (Third) of Foreign Relations Law § 402 (1987).

Every electronic communication must be physically stored *somewhere*, even if it can be accessed from anywhere in the world. For example, a company that provides an email service would typically store user data on hard drives in servers that are stored in large data centers. If data is stored on a server *physically located within the territory of the United States*, then law enforcement officials should be able to access that data pursuant to a duly issued warrant. Any other rule would be inconsistent with longstanding principles of territorial sovereignty and would undermine critical law enforcement prerogatives.

Courts and commentators have also recognized that a sovereign nation may retain power over its nationals wherever they go in the world. *See, e.g.*, *Kiobel v. Royal Dutch Petroleum*, 133 S. Ct. 1659 (2012) (Breyer, J., concurring) (Alien Tort Statute may apply extraterritorially if "the defendant is a U.S. national"). As the Restatement explains, each nation has jurisdiction "to prescribe law with respect to … the activities, interests, status, or relations of its nationals *outside as well as within its territory*." Restatement (Third) of Foreign Relations Law § 402 (emphasis added). Indeed, given that the U.S. Constitution *protects* U.S. nationals even when they travel outside the United States, *see Reid v. Covert*, 354 U.S. 1 (1957), it makes sense as a basic matter of symmetry that the *responsibilities* of U.S. citizenship should also attach when U.S. nationals travel abroad.

There are numerous instances in which the United States exercises jurisdiction over the activities of its nationals in foreign countries. For example, U.S. nationals must generally pay taxes on income earned abroad and must file annual reports documenting their foreign holdings. *See* IRS, *Report of Foreign Bank and Financial Accounts*, *available at* http://1.usa.gov/1bDYARp (explaining reporting and disclosure requirements for U.S. nationals who hold foreign bank accounts). The Supreme Court has also found a U.S. citizen in contempt of court for failing to comply with a subpoena issued in the United States, even though the defendant was residing in Paris at the time. *Blackmer v. United States*, 284 U.S. 421 (1932). And, in an effort to crack down on "sex tourism," Congress has made it a crime for any U.S. national to "travel[] in foreign commerce … and engage[] in any illicit sexual conduct with another person" anywhere in the world. 18 U.S.C. § 2423(c).

Even more to the point, the United States has also compelled multinational *companies* to disclose information stored abroad that pertains to U.S. citizens. For example, the Department of Justice has reached landmark settlement agreements with several major Swiss banks that require those banks to disclose "account information about thousands of … U.S. taxpayers who maintain secret Swiss bank accounts." *See* DOJ, *Offshore Compliance Initiative*, *available at* http://1.usa.gov/1BZzLdJ. DOJ has also served "John Doe" summonses on a number of other multinational banks, seeking information about U.S. taxpayers who may hold undisclosed offshore accounts. *Id.*

It is thus hardly anomalous for the LEADS Act to allow law enforcement to seek disclosure of U.S. nationals' emails pursuant to a warrant, even if those communications are stored overseas. Just as a U.S. citizen must disclose—and pay taxes on—foreign bank accounts, the LEADS Act ensures that U.S. nationals cannot evade the jurisdiction of U.S. authorities merely because they have an email account that is stored on a server in a foreign country. The geographic scope of the LEADS Act is entirely consistent with longstanding principles of both U.S. and international law.

C. The LEADS Act Respects Foreign Nations' Sovereignty and Recognizes That Inter-Jurisdictional Disputes Should Be Resolved in the First Instance Through the Well-Established MLAT Process.

As noted above, there are ongoing disputes in the courts over whether ECPA authorizes law enforcement officials to seek disclosure of foreign citizens' email correspondence that is stored in foreign countries. The LEADS Act expressly addresses this issue in a manner that respects the sovereignty of foreign nations and ensures that cross-border disputes will be addressed on a sovereign-to-sovereign basis through the MLAT process.

1. Critically, the LEADS Act does *not* authorize law enforcement officials to compel the disclosure of emails belonging to foreign citizens that are stored in foreign countries. *See* LEADS Act § 2(4) ("[T]his Act authorizes the use of search warrants extraterritorially only where the Government seeks to obtain the contents of electronic communications belonging to a United States person."). The Act thus promotes international comity by reasonably presuming that when a foreign citizen's information is stored on a server in a foreign country, it is the foreign government—*not the United States*—that should exercise principal law enforcement authority. The United States would view it as an egregious breach of its sovereignty if a foreign government compelled a multinational corporation to produce information belonging to U.S. citizens that was stored on servers in the United States. The LEADS Act ensures that the United States will extend the same respect to other countries as well.

The LEADS Act also attempts to minimize inter-jurisdictional conflicts by ensuring that providers are not forced to violate the laws of a foreign country. Countless companies offer electronic communications services to users in multiple countries. What if U.S. law enforcement officials served a warrant on a multinational company seeking emails stored on a server in Germany, but disclosure would violate German law? Section 3(a)(2)(B) of the LEADS Act expressly provides that "[a] court issuing a warrant pursuant to this subsection, on a motion made promptly by the service provider, shall modify or vacate such warrant if the court finds that the warrant would require the provider of an electronic communications or remote computing service to violate the laws of a foreign country." Without this critical safety valve, a company could be

faced with competing legal obligations, and could be forced to choose between violating U.S. law (by refusing to comply with the warrant) and violating foreign law (by disclosing emails that are protected by local law). The LEADS Act's provision that allows a warrant to be vacated if it would require violation of the laws of a foreign country *both* respects the sovereignty of foreign nations *and* ensures that providers of electronic communications services are not forced into an impossible position.

These concerns about inter-jurisdictional conflicts are not just hypothetical. For example, Article 25(6) of the European Union's Data Protection Directive prohibits providers from transferring personal data outside the E.U. unless the European Commission determines that the target nation provides an adequate standard of data protection. *See* Council Directive 95/46, art. 25(6), 1995 O.J. (L 281) (EC). There are serious questions about whether a provider would violate this provision if it produced data stored in the E.U. in response to a U.S. subpoena. A member of the European Parliament who sits on the committees that oversee data privacy has emphasized that this situation could "give rise to a conflict of jurisdiction," that is "not only offensive to the sensitivities of European citizens but also reinforces the already strong sentiment of many EU citizens that their data is not 'safe' when they use IT services offered by U.S. corporations." Br. of *Amicus Curiae* Jan Philipp Albrecht at 9-11, *Microsoft v. United States*, No. 14-2985 (2d Cir. Dec. 19, 2014). The LEADS Act would eliminate this risk of inter-jurisdictional conflict and promote international comity by allowing a subpoena to be quashed if it would violate the laws of a foreign nation.

2. The LEADS Act further recognizes that when there is a need for information about a foreign citizen stored in a foreign country, the proper way to handle this request is through the well-established process under Mutual Legal Assistance Treaties. The United States currently has MLATs with more than 50 other countries, including Australia, Canada, Brazil, France, Germany, India, Japan, Mexico, Russia, and the United Kingdom. The purpose of these treaties is to provide a mechanism for the exchange of evidence and information in criminal cases and other government investigations.

When there is a dispute over a criminal investigation that crosses national borders, it should be handled on a government-to-government basis through the MLAT process—not by inserting an email provider into an international dispute between two sovereign nations. The MLAT process respects each nation's sovereignty by allowing a country to reject a request for information or cooperation if it would violate that nation's laws or public policy objectives. For example, the MLAT between the United States and France provides that "[l]egal assistance may be denied if the Requested State considers that . . . execution of the request would prejudice its sovereignty, security, public order, or other essential interests." U.S.-France Mutual Legal Assistance Treaty, Article 5 (Dec. 10, 1998). The MLAT process thus promotes international cooperation in law enforcement while also ensuring that signatory nations are not forced to violate their domestic laws or take actions that would undermine their policy interests.

The LEADS Act includes several provisions that are designed to make the MLAT process more efficient and transparent. For example, Section 4(a)(1) of the Act attempts to modernize and streamline the MLAT process by creating an online intake form and online docketing system for MLAT requests from foreign governments. Although these provisions would not be binding on other countries, they would create examples of "best practices" for other countries to emulate.

Section 4(a)(2) also requires the Department of Justice to publish annual statistics about the number of MLAT requests the Department has made and the time it takes foreign governments to process those requests.

In sum, the LEADS Act takes an appropriately circumscribed approach to law enforcement information requests that cross jurisdictional lines. When a country needs information about a foreign citizen that is stored in a foreign country, the proper way to obtain that information is to file a request *with the other government* through the well-established MLAT process—not to go directly to a private company with a warrant or subpoena for customer records. The United States would view it as an egregious breach of protocol (and its own sovereignty) if a foreign government forced a multinational company to produce information about a U.S. citizen that was stored in the United States. Other countries will inevitably look to U.S. law in crafting their own policies regarding privacy and disclosure of electronic communications, and the United States should follow the golden rule of treating other countries' citizens the same way it would want U.S. citizens to be treated by foreign governments.

IV. CONSIDERATIONS TO FURTHER IMPROVE THE LEGISLATIVE PROPOSALS

For all the reasons set forth above, either the LEADS Act or the Email Privacy Act would be an important step in the right direction toward improving the outdated ECPA regime. But there remains room for improvement with respect to both pieces of proposed legislation.

The Email Privacy Act could be improved by expanding its scope to address the territorial reach of the warrant power and the process for resolving inter-jurisdictional conflicts over access to electronic communications. ECPA's failure to address these issues has led to heated disputes such as the one now pending in the Second Circuit. Given the rapid globalization of commerce and communications, it likely makes sense for Congress to address these issues in a single piece of comprehensive reform legislation rather than addressing them on a piecemeal basis.

As to the LEADS Act, some commentators have correctly noted that the MLAT process—which is central to the LEADS Act's framework for resolving inter-jurisdictional disputes—can be somewhat costly and cumbersome. We thus believe that the LEADS Act can be further improved if both Congress and the executive branch take additional common-sense steps that would improve the workings of the MLAT process.

As noted in a recent report by the President's Review Group on Intelligence and Communications Technologies, foreign countries seeking information from the United States through an MLAT request "can face a frustrating delay in conducting legitimate investigations."[2] These delays may "provide a rationale for new laws that require e-mail and other records to be held in the other country, thus contributing to the harmful trend of localization." *Id.* The LEADS Act would take several steps to address such delays by, for example, creating an online intake form

[2] *Liberty and Security in a Changing World, Report and Recommendation of the President's Review Group on Intelligence and Communications Technologies*, at 227 (Dec. 12, 2013), *available at* http://1.usa.gov/1bK0q7x.

and an electronic docketing system for requests from foreign governments. *See supra* Section III.C.

But a more fundamental problem is that the office within the Department of Justice that responds to MLAT requests has regularly suffered from "flat or reduced funding," despite the "large increase in the international electronic communications that are the subject of most MLAT requests." President's Review Group Report at 227-28. Increased funding and staffing for this office would enable DOJ to respond more quickly to foreign countries' MLAT requests, which would, in turn, incentivize those countries to respond more promptly to requests from the United States.

Moreover, MLAT response times are often delayed because the requests may be sent back and forth several times between DOJ headquarters and the local U.S. Attorney's Office. Response times could likely be reduced significantly if DOJ "[s]treamline[d] the number of steps in the process," and designated "a single point of contact" for each MLAT request. *Id.* at 228. Similarly, under current procedures, an email provider typically forwards responsive records to DOJ, which then sends them to the requesting foreign government. But "[i]t may be possible to streamline this process by permitting the provider to send the records directly to the requesting country, with notice to the Justice Department of what has been sent." *Id.*[3]

Finally, another recent report on MLAT reform has noted that "[p]erhaps the lowest-hanging fruit, from the standpoint of policy changes to the existing MLAT regime, is better training for requesting law enforcement officials."[4] Many MLAT requests from both the United States and foreign countries are "incomplete, overbroad, and ill-informed about the relevant legal requirements." *Id.* As a result, the receiving country often needs to go back to the requesting country for clarification or additional information, resulting in delays for both sides. Providing additional training for the government officials who both make and respond to MLAT requests would help ensure that such requests are presented in a manner that will promote a quick response.

In sum, the LEADS Act appropriately treats the MLAT process as the primary vehicle for resolving inter-jurisdictional disputes over law enforcement access to electronic communications. The LEADS Act would take several important steps to improve the workings of that process, but even more can be done. We encourage both Congress and the executive branch to take additional common-sense steps to improve the efficiency and transparency of the MLAT process. The better the system works in the United States, the more it will encourage other countries to adopt similar reforms that will expedite the processing of information requests from the United States.

[3] A previous attempt to resolve some of these inefficiencies, the Foreign Evidence Request Efficiency Act of 2009, has not been fully implemented due to inadequate funding. *See* 18 U.S.C. § 3512; DOJ, *FY 2015 President's Budget & Performance Submission*, at 22, *available at* http://1.usa.gov/1EJ3P1G.

[4] Global Network Initiative, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, at 9 (Jan. 2015), *available at* http://bit.ly/1zyXqGq.

Conclusion

Reform of ECPA's 30-year-old statutory framework is long overdue. Although the LEADS Act provides a more comprehensive solution than the Email Privacy Act, either proposal would be a significant step in the right direction toward updating and modernizing the statutory framework that governs law enforcement access to electronic communications.