Google

Digital Security & Due Process: **Modernizing Cross-Border Government Access Standards for the Cloud Era**	
Democratic countries around the world strive to keep their citizens safe. Those governments need access to digital evidence, which can often be held by foreign communication service providers. Today's international legal frameworks, however, were built for a gone-by era when the need for cross-border evidence collection was rare. As a result, countries struggle to find ways to get the information they need, and the solutions proposed often come at a high cost for privacy and security. The proposals in this document would allow law enforcement authorities to obtain the digital evidence they need to investigate legitimate cases in a more timely manner while protecting privacy.	
The Problem...	**The Solution...**
Governments that adhere to baseline privacy, due process, and human rights standards are encumbered in their ability to obtain electronic data that is held by service providers. These governments have legitimate law enforcement objectives, and they are often unable to obtain this data in a timely manner…	...**Digital evidence that is held by service providers should be accessible in a timely manner for legitimate law enforcement investigations.** Countries that commit to baseline privacy, due process, and human rights principles should be able to make **direct requests to providers** in other democratic countries. For other countries, existing mutual assistance frameworks should be reformed to improve response times.
Users' privacy rights are not adequately protected by current legal frameworks…	...Countries must **commit to baseline principles** of privacy, due process, and human rights in their domestic laws if they wish to make direct requests to providers in other democratic countries.

The Great Train Robbery of 1963 (and 2017)

In 1963, a train on its way from Glasgow to London was interdicted by a cohort of young men, who subsequently stole £2.6 million that they knew was being transported at the time. "The Great Train Robbery", as it became known, left an indelible mark on Britain as one of its most notorious crimes. The crime was meticulously planned and much of the stolen money was never recovered. Multiple investigations were launched using traditional investigative techniques at the time. Witnesses were interviewed, items were dusted for fingerprints, warnings about potential suspects were made to seaports, and most of the culprits were ultimately apprehended.

The investigation of a hypothetical Great Train Robbery in 2017 would involve some of the same investigative techniques used in 1963, but would also be different in significant ways. The availability of closed-circuit television (CCTV) footage could help identify the culprits and key witnesses. And the availability of data from email providers, social media services, communications services, and other providers could yield evidence identifying the culprits' whereabouts at the time of the crime and their communications about planning the heist.

And that's where things would get complicated. If a company in the United States (U.S.) provided an email service used to plan the robbery, the U.K. government would need to turn to the U.S. government for legal assistance to get the relevant emails. The U.S. might have grounds to open their own investigation, serve a warrant on the provider to get the emails, and then share them with U.K. officials. Absent the possibility of obtaining these emails from the U.S., the U.K. investigators would invoke a diplomatic process under the Mutual Legal Assistance Treaty (MLAT) between the U.S. and the U.K..

MLATs are critical treaties that allow one country to seek assistance from another to obtain evidence and investigative support. The MLAT process serves an important function. It allows countries to cooperate in investigations, while ensuring that the values important to each are respected. The treaties respect the sovereignty interests of each country and allow even countries with largely adversarial relations to work together where there is common ground.

In recent years, however, the volume of MLAT requests submitted to the U.S. has swamped the system, which is largely a manual one. This growth in the number of requests is in large part because so many investigations involve evidence held by U.S. communications service providers. The volume combined with other factors such as lack of automation, poor understanding of what is required to be in an MLAT application to the U.S., and other challenges, has rendered the MLAT process slow and cumbersome. And so the result is that today it may take many months before the U.K. government receives the communications content it sought. In the interim, the culprits would remain free, follow-on crimes may be committed, witnesses might move or become unavailable, and evidence could be destroyed. To reduce delays on its side, the U.S. may be able to expedite processing of the request, but of course that just comes at the expense of other pending requests that lose their place in the queue.

This state of affairs is untenable for governments with legitimate law enforcement interests. It leaves governments around the world looking for other ways to get the information they need for their public safety and security responsibilities. These alternatives can be unsavory, may cause collateral damage, undermine privacy and security protections for all of us, and may in the end be ineffective to get the information.

There is an urgent need for action to address these issues in a way that recognizes legitimate law enforcement interests, respects the sovereignty and political process of representative democracies, and lifts privacy, due process, and human rights standards throughout the world. In our view, such actions should:

- Provide an alternative to MLATs for democratic countries to use to seek information directly from foreign providers;
- Protect privacy based on who the user is, not based on where the data is stored; and
- Modernize the MLAT process and implement other practical improvements.

****

The rules governing law enforcement access to data are becoming obsolete in two critical, but different ways.

First, they do not ensure that countries with respect for the rule of law and human rights can obtain digital evidence – accessible and available in the cloud – in a manner that reflects the gravity of the law enforcement equities at stake.

Second, they do not adequately protect the privacy rights of users in light of technological innovation.

The adverse consequences of failing to update the law are now materializing — the result of mounting frustration from countries who are hampered in their ability to access digital evidence in a timely manner in order to prevent or investigate criminal and terrorist acts. This is manifesting itself in the form of:

- the extraterritorial assertion of one country's laws in the face of clear conflicts of law;
- data localization proposals;
- aggressive enforcement efforts (e.g., imprisonment, substantial fines, garnishment of wages) targeted at employees of U.S. providers in countries outside the U.S; and
- proposals to enhance government access powers, including increased and aggressive government hacking efforts.

As concerns about crime and terrorism grow, we have seen proposals that would invariably create a conflict of laws between different countries. For example, as noted above, U.S. law generally prohibits U.S. companies from disclosing electronic communications content to foreign governments. As frustrations mount over the inability to obtain this data through sovereign channels in a timely manner, some foreign governments are resorting to other tactics — including the extraterritorial application of their own laws — that conflict with U.S. law.

Such conflicts between countries trying to protect their respective interests potentially put companies in the untenable position of deciding whether to risk violating the law of the requesting country or to risk violating the law of the country in which it is headquartered. Conflicts also significantly reduce the likelihood that law enforcement authorities will receive data from service

providers, who become hamstrung in their ability to respond in light of such conflicts. It is in the interest of all stakeholders to work toward solutions that avoid conflicts of law, enable the production of digital evidence for legitimate law enforcement investigations, and incentivize the improvement of privacy and due process standards.

Two Fundamental Challenges

(1) Governments Are Encumbered in Their Ability to Obtain Data for Legitimate Law Enforcement Investigations in a Timely Manner

- **Democratic Countries That Respect the Rule of Law Are Encumbered in their Efforts to Obtain Communications Content in a Timely Manner for Legitimate Law Enforcement Investigations**

Companies that provide communications services largely arose in a world where the services offered were for local users, and were mainly telephonic. Naturally and understandably, laws were created based on that reality. This factual assumption is reflected in the key U.S. laws, such as the Electronic Communications Privacy Act of 1986 (ECPA). ECPA has worked well for many years, and much of it remains vibrant and relevant, even in 2017. But it is also clear that some of its underlying technological assumptions are increasingly outmoded and ill-equipped to address a world in which data moves seamlessly and ubiquitously across borders. Understandably, the U.S. Congress in 1986 did not contemplate a world in which U.S.-based Internet companies would provide services to billions of users around the world. Because some of the biggest Internet communication service providers are located in the U.S., ECPA is a particularly important law, not just in the U.S., but throughout the world.

ECPA has created significant challenges in cross-border investigations where the production of digital evidence may be critical for solving or prosecuting crimes that take place outside of the U.S. ECPA contains a "blocking" provision that generally prohibits U.S. companies from disclosing communications content to foreign law enforcement agencies. In the absence of emergency circumstances, foreign governments — regardless of their adherence to baseline privacy, due process, and human rights standards — cannot receive communications content without relying on the MLAT process or other diplomatic channels, which often inhibit timely access to data for legitimate law enforcement purposes. In recent testimony before the Senate and House Judiciary Committees, Paddy McGuinness, the United Kingdom's (UK) Deputy National Security Advisor, observed that this prohibition puts U.S. companies in the "invidious position of having to withhold information that could protect public safety."

Indeed, the blocking provision in ECPA is a source of enormous frustration for democratic countries that respect the rule of law and maintain substantive and procedural protection of civil liberties, and who need to investigate local crimes involving local users of U.S. services. In a letter sent to the Presidency of the Council of the European Union, French and German Interior Ministers opined that

"all too often, Member State authorities are faced with a refusal by service providers to provide information on legal grounds that we must be able to override. Electronic communication service providers must be able to contribute more to the successful outcome of investigations by being authorised to provide data linked to users' connections; in addition, data for European customers must be stored in a jurisdiction where direct cooperation with competent authorities of [EU] Member States is authorized." A recent French-British Action Plan also calls for cooperation to "ensure that data and content of communications can be rapidly accessed for law enforcement across borders, wherever it is stored."

These countries are often unable to obtain timely access to digital evidence solely because it is retained by a U.S. service provider subject to ECPA, even for crimes that are wholly domestic in nature. The inability to obtain this data creates incentives for these countries to seek other techniques to get the information, including enforcement of their laws extraterritorially, even in the face of conflicting U.S. law. It also creates incentives for enactment of data localization laws and aggressive investigative efforts that undermine security in general and redound to the detriment of users' privacy.

The U.S. is not the only country with such blocking provisions. A recent survey of the European Commission highlighted that the majority of European Member States' laws "do not cover/allow that service providers established in a Member State respond to direct requests from law enforcement authorities from another EU Member State or third country." In fact, it appears that "only 2 Member States" allow for such cooperation. Such restrictions also exist for law enforcement authorities, who are often prevented by law from making requests for direct cooperation to service providers in any other country. It is quite clear that the challenges created by blocking provisions are international in scope and not merely confined to the U.S.

There are legitimate reasons that a country may wish to limit how a provider headquartered in its jurisdiction behaves, including to whom the provider discloses data. A country may, for example, want to prevent its local providers from disclosing the content of communications to governments with poor human rights records. A broad blocking statute that is divorced from policy implications and lacks nuance, however, can leave countries with a legitimate need for information looking for alternative means, some of which can be unsavory, aggressive, and unsafe.

- **Improving Public Safety and Civil Liberties Through Alternatives to Diplomatic Channels and Procedures Such as MLATs**

As discussed above, ECPA's blocking provision imposes a barrier to law enforcement agencies outside the United States and often prevents them from obtaining information held by U.S. providers, even where the agencies are in democratic countries that respect the rule of law and are investigating entirely domestic matters. Typically such agencies will need to go through diplomatic channels with the U.S. government to obtain the content of communications. This can take many different forms, including letters rogatory and, where there is a treaty or executive agreement, through Mutual Legal

Assistance Treaty (MLAT) requests. MLAT requests are a primary legal mechanism by which foreign governments obtain electronic communications content from U.S. service providers. MLATs enable foreign governments to request and obtain such communications content by making a request through the U.S. Department of Justice.

The MLAT process, however, is often slow and cumbersome. In part this is because the number of MLAT demands have grown as evidence is more commonly held by companies in other jurisdictions, even if the crime itself is entirely local. In its 2015 Fiscal Year budget request, the Department of Justice noted that "[o]ver the past decade the number of requests for assistance from foreign authorities handled by the Criminal Division's Office of International Affairs (OIA) has **increased nearly 60 percent**, and the number of requests for computer records has **increased ten-fold.** While the workload has increased dramatically, U.S. Government resources, including personnel and technology, have not kept pace with this increased demand." (emphasis added). In 2013, the President's Review Group on Intelligence and Communications Technologies reported (p. 229) that MLAT requests "appear to average approximately 10 months to fulfill, with some requests taking considerably longer."

The problem is not entirely with the U.S., however. The MLAT process is also often hindered by the requesting country's lack of understanding of what is required to satisfy U.S. legal standards, or inefficiencies in the system of the requesting country. These diplomatic channels are critical tools and need to work efficiently.

- **ECPA's Limitations Frustrate the U.S. Government in its Efforts to Obtain User Data in Legitimate Law Enforcement Investigations**

Out-of-date concepts in ECPA also plague government agencies in the U.S. A unanimous panel of the United States Court of Appeals for the Second Circuit held last year that a search warrant issued under ECPA, as written, only permits U.S. government entities to compel a provider like Google to search for, seize, and produce records that are stored in the U.S. The ruling underscored the challenges of interpreting a 1986 statute and applying it to modern-day technological realities and cross-border law enforcement investigations.

At the time ECPA was passed, this limitation on warrants may have made some sense. Times, and more importantly networks, have changed since then. The limitation on ECPA warrants to data stored in the U.S. has presented challenges to law enforcement, which service providers appreciate. And it has spawned litigation in other parts of the U.S. This is not to criticize the Second Circuit's decision, which is based on well-established and long-held principles of statutory construction. Rather, it is to underscore the importance of Congressional intervention to update the law. The cases pending around the country have judges working to understand what Congress intended in this statute enacted in 1986, well before providers like Google and Facebook existed.

But these challenges can be best addressed only by the U.S. Congress. Rather than imposing limits under ECPA based on the location of data at the moment data is sought, a criterion applicable to traditional warrants, legal process under ECPA should be modified to consider the underlying user's nationality and location. Let's pay attention to the user, not to where the data is stored.

(2) Users' Privacy Rights Can Be Improved

- **Any Framework for Cross-Border Law Enforcement Requests Should Establish Baseline Privacy, Due Process, and Human Rights Standards**

For many years, we have called upon the U.S. Congress to update the Electronic Communications Privacy Act (ECPA) and codify a warrant-for-content standard. As we noted in previous testimony before the U.S. Congress, a warrant-for-content standard is effectively the law of the land today. This standard is observed by governmental entities and providers alike and has been embraced by courts as necessary to satisfy U.S. constitutional standards. In 2016 and 2017, the House of Representatives passed the Email Privacy Act, which would codify a warrant-for-content standard. But it hasn't been enacted into law, despite the clear consensus that has emerged in support of this standard.

Currently, some of the world's largest Internet companies are headquartered in the U.S. and thus subject to U.S. jurisdiction. Policy reform in the U.S., such as codifying the warrant-for-content standard, is thus critical to engender and incentivize the types of international reforms that can improve global privacy and due process standards while addressing legitimate law enforcement needs.

This is all the more important as many countries still lack such robust safeguards and standards for government access to data in the cloud. Even among like-minded countries, standards vary greatly, despite the fact that users' reasonable expectations of privacy vis a vis government access do not. A broader, international framework for cross-border law enforcement requests necessitates changes in the domestic statutes of countries that do not adequately protect privacy, due process, and human rights. This is core to any fundamental realignment of government access laws; it must reflect modern law enforcement needs and the privacy expectations and rights of Internet users.

This will undoubtedly require time and significant change for many countries. It also means that the MLAT process will be the primary mechanism that many countries will rely upon for the foreseeable future. However, adherence to baseline privacy, due process, and human rights standards are and should be no less compelling than law enforcement interests in obtaining electronic evidence stored in the cloud.

Proposed Solutions — A Blueprint for Reform

In debates about government access standards, there is an understandable tendency to view solutions as a balancing act, where improving governments' postures to obtain user data necessarily entails a trade off with user privacy (or vice versa as the case may be). But the goals of creating more efficient

government access standards and stronger privacy and due process standards are not mutually exclusive. Indeed, by updating the law to reflect the new realities, we will be creating new approaches that are better for law enforcement and civil liberties. We can and should endeavor to achieve both without searching for a balance that necessarily suggests a trade-off.

The proposed solutions set forth below aim to address the two fundamental challenges outlined above. We believe these ideas can make significant progress towards addressing these challenges, but we also recognize that workable international frameworks will require input and contributions from a broader group of stakeholders.

- ***Enable Certain Democratic Countries to Obtain Electronic Data From U.S. Service Providers***

It is increasingly clear that solutions complementary to MLATs must be developed to address the challenges to cross-border law enforcement investigations created by the advent of the Internet era. This is long overdue. Countries that commit to baseline privacy, human rights, and due process principles should be able to make requests to U.S. providers in serious cases without the intervention and participation of the U.S. government. Making such an avenue available would have the salutary effect of incentivizing foreign countries to raise their privacy and due process standards so that they can avail themselves of this new and more efficient process.

Such a framework would also have the ancillary benefit of giving citizens of those countries a real stake in the outcome of legislative processes that address government access to data. Currently, U.S. law often governs the circumstances under which the data of non-U.S. persons is disclosed to their governments. A German law enforcement agency seeking communications content about a German Gmail user, for example, would have to meet U.S. legal standards to obtain such data in most cases. Amending U.S. law to lift the prohibition on disclosing communications content to certain foreign governments in serious cases shows deference to the democratic processes of representative governments and their citizens, many of whom may prefer the privacy protections afforded under their domestic laws to those afforded under U.S. law.

In July 2016 and again in May 2017, the U.S. Department of Justice (DOJ) unveiled legislation that would amend ECPA to authorize, but not require, U.S. providers to disclose communications content to foreign governments that adhere to baseline due process, human rights, and privacy standards. This legislation would authorize the U.S. government to enter into executive agreements with foreign governments that meet minimum requirements of substantive and procedural protection of rights. Under such agreements, a qualifying foreign government could make legal requests to U.S. service providers in certain types of criminal investigations involving serious crimes without going through diplomatic channels, such as the MLAT process. DOJ and the Department of State would be required to determine and certify that a country adheres to baseline privacy, due process, and human rights principles before U.S. companies could disclose the content to that country. Foreign governments would be required to afford

reciprocal rights to the U.S. government in obtaining access to electronic data that a foreign country may prohibit service providers from disclosing.

The U.S. and U.K. governments are in the process of negotiating this type of agreement, the first of its kind. The U.K. for its part has enacted legislation to implement what are key components of this agreement, including a requirement that legal demands for communications content have a strong factual basis and are reviewed by a judicial commissioner that is independent of the UK government. The expectation is that other democratic countries with a commitment to privacy, due process, human rights, and the rule of law will be candidates for future bilateral or multilateral agreements.

A framework of this kind can help set expectations about the types of changes that foreign governments will need to make in order to satisfy baseline privacy, due process, and human rights standards. Providing a pathway for these countries to obtain electronic evidence directly from service providers in other jurisdictions, where such jurisdictions have no appreciable equity to block disclosure, will remove incentives for the unilateral, extraterritorial assertion of a country's laws, data localization proposals, aggressive expansion of government access authorities, and dangerous investigative techniques, which are ultimately bad for us all.

The changes to U.S. law described above will provide powerful incentives for foreign countries to update their government access statutes in ways that comport with baseline privacy, due process, and human rights standards. There is no international consensus about what concrete measures governments must take to meet such standards, but there are different models that can inform this undertaking.

First, the legislation unveiled by DOJ last year describes the types of human rights norms that other countries must observe to receive certification for the types of executive agreements that the legislation envisions. For example, countries must demonstrate "respect for the rule of law and principles of non-discrimination", and adhere to international human rights norms that include, but are not limited to "protection from arbitrary and unlawful interference with privacy; fair trial rights; freedoms of expression and peaceful assembly; prohibitions on arbitrary arrest and detention; and prohibitions against torture and cruel, inhuman, or degrading treatment or punishment." Legal orders from such governments must be "based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation". Such orders issued by foreign governments "must be subject to review or oversight by a court, judge, magistrate, or other independent authority".

Second, the Necessary and Proportionate Principles can also be a useful lodestar. In 2013, the United Nations' Human Rights Council initiated a process to develop and articulate principles that governments could emulate in fashioning government access statutes that comport with international human rights law. The result of that process is the Necessary and Proportionate Principles, a set of thirteen guideposts developed by privacy and human rights non-governmental organizations across the world. The Necessary and Proportionate Principles — as the prefatory text notes — can provide

governments with a "framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights."

Provided that countries can meet baseline privacy, due process, and human rights standards, the bilateral agreements authorized by the legislation unveiled by DOJ provide the most promising avenue to appreciably improve global privacy standards and create a pathway for foreign governments to obtain digital evidence for legitimate law enforcement investigations.

Of course, bilateral agreements are not the only path for improving privacy standards and enabling foreign governments to obtain digital evidence in legitimate law enforcement investigations. The same objectives may be better and perhaps more efficiently served through multilateral agreements that accomplish the same objectives. The current U.S.-U.K. agreement, however, is the best practical example thus far of addressing the various equities at stake. In light of the adverse consequences of inaction, it is critical that governments move quickly to address challenges that have been apparent for years and that are only growing more acute with the passage of time.

- ***Enact the International Communications Privacy Act (ICPA)***

Relatedly, it is also critical that countries begin to refashion their domestic statutes to take into consideration the legitimate privacy interests of both individuals outside of their country and the comity interests of the countries in which those individuals are citizens. ICPA is a framework that takes into consideration both of these equities. While we appreciate that ICPA will require refinements, it can be a useful model for other governments as they consider ways to adapt their domestic statutes to modern-day realities, where digital evidence is often vital to criminal investigations and often implicates the privacy rights of non-citizens and the comity interests of foreign countries.

Modern Internet networks increasingly store data intelligently, often moving and replicating data seamlessly between data centers and across borders in order to protect the integrity of the data and maximize efficiency and security for users. This technological reality underscores the importance of legislative solutions that eschew data location as a relevant consideration in determining whether a particular country can exercise jurisdiction over a service provider.

Notably, all of the judges who issued pertinent rulings in the Second Circuit case (including both the original 2016 panel opinion and a 2017 ruling denying rehearing before the entire Second Circuit) urged Congress to consider appropriate changes to ECPA that would resolve the policy questions at the heart of the case. Judge Lynch's concurrence in the 2016 case is notable in this regard:

> Although I believe that we have reached the correct result as a matter of interpreting the statute before us, *I believe even more strongly that the statute should be revised*, with a view to maintaining and strengthening the Act's privacy protections, rationalizing and modernizing the provisions permitting law enforcement access to stored electronic communications and other data where

compelling interests warrant it, and clarifying the international reach of those provisions after carefully balancing the needs of law enforcement (particularly in investigations addressing the most serious kinds of transnational crime) against the interests of other sovereign nations." *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 233 (2d Cir. 2016) (Lynch, J., concurring) (emphasis added).

Inaction means that important policy decisions about electronic privacy and government access fall by default to the courts. Courts are being asked to resolve individual disputes in ways that are divorced from sound policy solutions, without the robust opportunity for debate among a variety of stakeholders, and indeed potentially entirely in closed courtrooms. This is hardly the path for appropriately addressing the equities of users, law enforcement agencies, service providers, and foreign sovereigns.

The U.S. Congress has an opportunity to update ECPA for the Internet age, and to consider how the application of domestic U.S. government access laws affects the equities of foreign countries and the privacy rights of non-U.S. persons. A legislative framework that addresses the equities of relevant stakeholders is far preferable to a protracted litigation battle that is missing critical voices and perspectives. This is a job for Congress, not the courts. In the last Congress, Representatives Marino and DelBene, and Senators Hatch, Coons, and Heller, introduced the International Communications Privacy Act (ICPA). With some further refinements, ICPA can provide the right framework for cross-border law enforcement demands for user data. The following principles should inform further changes to ICPA. We believe it is important, however, to remain flexible in devising solutions to the broad array of challenges and wide array of equities at stake.

- **Warrants for Content:** Congress should codify a warrant-for-content standard. This has already passed the House of Representatives twice with no opposition, and this reform enjoys widespread support across the political spectrum.

- **Data Location:** Subject to the following additional principles, the location of data held by a U.S. provider should not in and of itself determine whether legal process issued under the stored communications chapter of ECPA can reach that data.

- **Notice:** When a government agency in one country endeavors to obtain, through lawful process, from a provider in its own jurisdiction, the electronic data of a user who is a national of or located in a different country, that agency should provide notice to that other country. There will be understandable exceptions and limitations to this notice requirement, but a country that has established diplomatic mechanisms (e.g., a Mutual Legal Assistance Treaty (MLAT)) with another country for the production of data in cross-border investigations, and that observes shared, baseline principles of privacy, due process, and human rights, should honor this notice principle. This affords the other country an opportunity to raise concerns, through diplomatic channels for

example, about the request in light of the legitimate privacy interests of its citizens and the comity interests and values of that country.

- **Redress and Comity Factors:** A jurisdiction that receives the notice contemplated above should have the opportunity for redress in the requesting country's jurisdiction. This may include the opportunity to initiate a legal challenge in the requesting country's jurisdiction. Courts that hear such challenges should conduct a comity analysis to help weigh the equities of the countries. Factors to be considered under that analysis could include: (i) the location and nationality of the customer or subscriber; (ii) the location of the crime; (iii) the seriousness of the crime; (iv) the importance of the data to the investigation; and (v) the possibility of accessing the data via other means.

- **Reciprocity**: Countries that extend the aforementioned rights (i.e., notice and redress) to other countries under their domestic laws should expect reciprocity. Countries should not be required to provide notice or redress mechanisms to other countries that are not obliged to reciprocate. And no country, of course, should be required to extend the aforementioned rights to countries that fail to adhere to baseline privacy, due process, and human rights standards.

The basis for a legislative framework that addresses the various equities at stake exists, and we are eager to work with interested stakeholder to update ECPA in this manner.

- ***Modernize the MLAT Process***

There is no panacea for the range of challenges presented by aging legal regimes that are ill-equipped to address technological innovation, modern law enforcement needs, and strong privacy, due process, and human rights standards. MLAT improvements remain critical to instill confidence in the ability of the U.S. to provide data to foreign law enforcement agencies in a timely manner. The vast majority of countries are going to rely on MLATs and comparable diplomatic mechanisms for the foreseeable future, which underscores the importance of moving quickly to fully fund and implement the necessary reforms to the MLAT process.

There are a number of ways that the DOJ could modernize its response procedures for MLAT requests.

- **Develop a Standard Electronic Form and Online Docketing System for MLAT Requests:** DOJ should create a publicly available, standardized online form for the submission of MLAT requests. Separately, DOJ should create an online docketing for receipt of MLAT requests accessible only to those MLAT partners. Foreign governments should be able to utilize this online docketing system to track the status of outstanding MLAT requests.

- **Streamline Review of MLAT Requests:** DOJ could streamline the handling of MLAT requests

for content data by eliminating the need for duplicative review by both its Office of International Affairs (OIA) and a local U.S. Attorney's Office. This could be accomplished in multiple ways, using existing statutory authorities. For example, OIA attorneys could review the MLAT request, prepare the U.S. legal documents needed to execute that request, and file those documents directly with a U.S. court, without the need to work through a local U.S. Attorney's Office. Second, OIA attorneys could prepare the U.S. legal documents needed to execute the MLAT request and then provide those documents to an Assistant U.S. Attorney in the District of Columbia or another appropriate district who has been specially designated to file those documents on behalf of OIA. The second option would expand on a highly successful pilot project OIA recently conducted with the U.S. Attorney's Office for the District of Columbia for requests for § 2703(d) orders. Both options, which are not mutually exclusive, would significantly streamline the MLAT process by eliminating the delay caused by having multiple DOJ attorneys in different offices review and process the same MLAT request.

- **Engage Foreign Partners and Improve Training:** The Justice Department, in conjunction with other agencies, should keep an ongoing line of communication with their MLAT counterparts across borders and establish single points of contact so there is no confusion about where requests or orders should be sent. The U.S. government should also work to increase and standardize education and training of law-enforcement ministries, the U.S. judiciary, and other interested parties on how to utilize MLATs effectively. This will require further coordination with the U.S. Department of State, the Federal Bureau of Investigation's Legal Attache offices, and other relevant U.S. federal and private sector entities to host overseas training sessions at U.S. Embassies. These sessions could focus on best practices relating to the use of MLATs, applicable U.S. legal requirements such as probable cause, guidance on electronic forensics, and overviews of modern electronic data technologies relevant to criminal investigations.

- **Increase Transparency:** The Departments of Justice and State should work together to increase transparency and provide online and searchable treaty documents, compliance guidance, FAQ's, aggregate metrics, and other materials to international law enforcement and, where appropriate, to the public. This will improve the documentation available concerning the submission of MLAT requests and facilitate greater understanding of U.S. legal standards for foreign counterparts/agencies, which often struggle to formulate MLAT requests that meet the U.S. standard of probable cause. Providing this type of guidance in an accessible manner will contribute to higher-quality submissions to OIA, which in turn should help reduce review and processing time for those requests. In addition, public reporting on improved response times and other progress would increase trust by foreign law enforcement officials in the MLAT process as a reliable mechanism for law enforcement requests.

- **Increase Resources:** The U.S. government should allocate significant new resources to OIA in order to enhance its personnel and to implement the other recommendations outlined above for improving the MLAT process. Given its current constraints and the significant increase in volume

of requests it handles, it is unreasonable to expect OIA fully address these challenges without a surge in personnel and other resources.

This is by no means an exhaustive list of policy options available to governments. Indeed, the Global Network Initiative's report, entitled "Data Beyond Borders — Mutual Legal Assistance in the Internet Age," provides additional recommendations for improving the MLAT process. Foreign governments should also consider practical ways to improve cooperation with U.S. authorities. For example, the European Commission's recent efforts, which includes financial support for the exchange of best practices and training for EU practitioners on relevant U.S. law, is a good start. Foreign governments are often slowed by their own internal inefficiencies in transmitting MLAT requests to the U.S.

- ***Develop Practical Solutions for the Near Term***

Bilateral frameworks that can facilitate the production of digital evidence in cross-border investigations, while lifting global privacy standards, are undoubtedly ambitious undertakings. In the interim, there are practical steps that governments and service providers can take to make the provisioning of data in cross-border law enforcement investigations more efficient, which can help reduce the likelihood that governments will resort to more aggressive measures that will invariably weaken privacy and due process standards.

Based on our experience, there are meaningful and practical steps that improve cooperation between law enforcement and providers and help relieve some of the pressures of the problematic proposals described elsewhere in this document.

- **Single Points of Contact (SPOCs)**. Law enforcement authorities should designate officials to serve as dedicated points of contact for working with foreign communication service providers. The officials would be responsible for understanding the legal requirements and know how to submit legal process to a provider, what to expect in return, and how to deal knowledgeably and quickly with errors and misunderstandings that inevitably arise. We have seen that such points of contact help ensure that the requests are appropriately formulated and facilitate verification by providers that the requests are authentic. It would also consolidate (and limit) the number of requests concerning the same investigation. SPOCs have achieved meaningful improvements in the effectiveness of cooperation in many countries that have adopted this posture, and this is a promising avenue for improving the MLAT process in other countries as well.

- **Train the Trainer**: International and regional organizations should work on consolidated train-the-trainer programs in which providers should participate. Such systems are particularly effective in systems where there are SPOCs as discussed above. .

- **Clarity on Applicable Law**: International and regional organizations should work to collect, translate and keep up-to-date national legal requirements related to access to data, including both primary and secondary legislation. This would ensure that providers and authorities have a common understanding what these procedures and legal requirements are.

****

Government access laws are due for a fundamental realignment and update in light of the proliferation of technology, the very real security threats to people, and the expectations of privacy that Internet users have in their communications. This is not merely an aspiration, but a necessity.

If the current trajectory does not change, there will be an even more chaotic, conflicting world of expansive government access laws and overly-aggressive investigative techniques that will weaken privacy protections for users and exacerbate existing tensions between governments and service providers. This could undermine the global Internet that is driving economic and social progress around the world and would ultimately undermine cooperation between law enforcement authorities and service providers. We are confident that the solutions outlined above can accelerate the development of international legal frameworks that reflect sound policy judgments.