Department of Justice

STATEMENT OF
DAVID BITKOWER
PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE
COMMITTEE ON THE JUDICIARY
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"INTERNATIONAL CONFLICTS OF LAW CONCERNING CROSS BORDER DATA FLOW AND LAW ENFORCEMENT REQUESTS"

PRESENTED
FEBRUARY 25, 2016

Statement of
David Bitkower
Principal Deputy Assistant Attorney General
Criminal Division
Department of Justice

Before the
Committee on the Judiciary
United States House of Representatives

At a Hearing Entitled
"International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests"

February 25, 2016

Good afternoon Chairman Goodlatte, Ranking Member Conyers, and members of the committee. Thank you for the opportunity to testify on behalf of the Department of Justice concerning law enforcement access to data stored abroad. This topic is particularly important to the Department for two reasons. First, timely and lawful access to electronically stored information is critical to both criminal and civil law enforcement; and second, electronic communications service providers, including American providers, are increasingly storing data outside the United States. If the Department is unable to obtain access to information stored abroad in a timely manner when authorized by a court, its ability to fulfill its missions of protecting public safety and obtaining justice for victims of crime will be impaired. Our citizens rightfully demand that we be prepared for the rapidly evolving challenges of combating crime in the digital age, and we must therefore ensure that we maintain efficient and effective mechanisms for access to evidence stored across borders. We are thus pleased to engage with the Committee in discussions on legislation in this area.

I will address three topics in my testimony. First, I will discuss the increasingly important role that cross-border access to data plays in the protection of the public, for both the United States and our foreign partners. Second, I will address existing U.S. law related to obtaining access to information across borders, including the role of the Stored Communications Act ("SCA") and Mutual Legal Assistance Treaties ("MLATs"), which affect the ability of both the United States and other countries to successfully investigate and prosecute serious crimes. Third, I will address possible legislation, including the opportunity to build a new framework for effective, efficient, and privacy-protecting cross-border access to data — as well as the need to avoid legislation that would erect new obstacles to our ability to protect Americans, without adding any meaningful protections for privacy.

I. Cross-Border Access to Data Is Increasingly Important to Protecting Public Safety – Both for the United States and for our Foreign Partners

Electronic information is critical to investigations of serious offenses, including terrorism, financial fraud, drug trafficking, child sexual exploitation, human trafficking, and computer hacking. The Internet has brought tremendous new opportunities for Americans and American industry — it has become nearly ubiquitous in our lives, and we use it to communicate, to learn, to collaborate, and to store our private information. At the same time, the Internet has created new ways for criminals to target and harm Americans and American companies. To a degree that was difficult to imagine only a generation ago, it has become an easy thing for perpetrators to commit serious crimes within the United States without ever setting foot here — and perhaps even easier to commit crimes against Americans when we travel or do business overseas. Given the unparalleled threats the United States faces from abroad, Congress has wisely enacted criminal offenses targeting such conduct, and the Department has expended substantial efforts in investigating and prosecuting those crimes. Our experience has shown that in both purely domestic cases and cases involving threats from overseas, data stored by communications providers, such as the content of email or text messages, IP connection records, or even subscriber and billing information, can be crucial to identifying perpetrators, tracing their steps, and bringing them to justice.

Because of the pioneering role played by American companies in electronic communications services, it is not unusual for this type of electronic information to be stored in the United States – whether the information relates to an American, or to a foreign citizen who happens to use an American service. Increasingly, however, American providers and other providers subject to the jurisdiction of United States courts are storing such information outside the United States, and not always at rest and in the same location. For example, one major American provider has said that it has begun to store the contents of many accounts in data centers located abroad. That provider indicated that it chooses whether to maintain data in the United States or abroad based solely on the user's selection of her country of residence at the time the account is created. Accordingly, even Americans who live in the United States can effectively choose to have their account data stored abroad by doing no more than choosing a desired country from the drop-down menu on the sign-up form. In fact, many of the largest American providers now operate data storage centers abroad and it is unusual for a major provider to store all of its data within the United States.

Moreover, there is no guarantee that communications service providers that have traditionally stored information in the United States will continue to do so. United States law generally does not require providers to store data in the United States, whatever the nationality of the user. The Administration has advocated against such requirements globally in order to ensure the free flow of information that is the foundation of the Internet. However, U.S. providers increasingly face tax or other business incentives, as well as pressure by foreign governments, to operate data storage centers outside the United States. For these reasons,

although law enforcement access to data stored abroad is already a key issue today, its importance for the United States is likely to grow.

Consider the following examples, each of which involves persons outside the United States charged with significant United States crimes. Evidence gathered from American service providers pursuant to the Stored Communications Act — evidence that providers may choose to store abroad based on solely the individual's citizenship or location — was critical to investigating these crimes and ensuring that the perpetrators faced justice.

- A child exploitation group dedicated itself to producing and distributing images and videos of infants and toddlers being sexually abused. Although the ringleader of the group was a citizen of, and resided in, a Western European country, many members of the group were American, and many of their victims were American children — including children inside the United States who were being actively abused in order to produce new child pornography. The ringleader of the group used an email account operated by a U.S. provider, and U.S. law enforcement officers obtained and executed an email search warrant on that provider pursuant to the SCA. The results of that search led to the identification of scores of dangerous sex offenders around the globe. It also led to the rescue of more than a dozen children, many in the United States. Ten offenders, including the ringleader, were charged in the same district and convicted in the United States for their roles in the conspiracy.

- In 2009, a Tunisian suicide bomber carried out an attack on U.S. forces in Iraq and killed five American servicemen. Law enforcement suspected a Canadian citizen of having facilitated the recruitment and travel of the suicide bomber and several associates from Tunisia to Iraq in order to conduct attacks on U.S. military personnel on behalf of the Islamic State of Iraq, currently known as ISIL. The Canada-based defendant communicated with alleged members of his terrorist network through email accounts operated by U.S.-based providers. U.S. law enforcement officers obtained and executed search warrants on several of those accounts pursuant to the SCA, and the results of those searches yielded significant evidence about the conspiracy and about the suicide attack. The United States sought the defendant's extradition from Canada to face charges of murdering U.S. nationals and providing material support to terrorists, and the defendant has been extradited to face trial in the United States.

- A Nigerian citizen traveled to Yemen to join al-Qaeda in the Arabian Peninsula ("AQAP"), and received weapons training and money from former AQAP leader Anwar al-Awlaki before returning to Nigeria, where he was suspected of plotting an attack against U.S. interests in Nigeria or the U.S. homeland. The defendant and a co-conspirator used email accounts operated by U.S. providers to communicate with other AQAP members about their plot. While in custody in Nigeria, the defendant and his co-conspirator provided U.S. law enforcement officers with consent to search their email accounts, but not the correct passwords, and a consensual search could not be

executed. Instead, U.S. law enforcement officers obtained and executed search warrants pursuant to the SCA. Those searches yielded significant evidence about the conspirators' contact with AQAP. After his extradition to the United States, the defendant pleaded guilty to providing material support to AQAP and was sentenced to 22 years' imprisonment.

- In connection with the investigation of an organization that allegedly laundered more than $10 million stolen from the bank accounts of U.S. companies, U.S. law enforcement obtained more than 30 warrants to search email and social media accounts used by the conspirators to communicate and facilitate the fraudulent scheme. These records played a significant role in developing evidence of the scheme, which resulted in charging four Ukrainian nationals with conspiracy to hack into computers in the United States, money laundering, and other crimes. One of the defendants has been successfully extradited from Poland, and the remaining three are in extradition proceedings.

- A dual U.S./foreign citizen accepted more than $5 million in bribes to influence the awarding of more than $2 billion in contracts from a foreign government. U.S. law enforcement officers obtained and executed email search warrants for accounts relating to both a U.S. person and a non-U.S. person; the results of those searches included emails regarding the details of the bribery scheme and foreign bank account information showing the flow of illicit funds. Based primarily on the search warrant evidence and its fruits, law enforcement was able to arrest the defendant, and he subsequently pleaded guilty to mail fraud, money laundering, and tax fraud.

- A drug trafficking organization obtained heroin, methamphetamine, and precursor chemicals from Pakistan for illicit importation into the United States. The primary target of the investigation was based in Europe. U.S. law enforcement served search warrants pursuant to the SCA to multiple providers in the United States, resulting in critical evidence that led to the identification of the target, his location, and information about bank accounts used to collect illicit proceeds. The target was subsequently arrested and pleaded guilty, and he received a 15-year prison sentence.

- A Kosovo citizen allegedly stole personally identifiable information belonging to U.S. service members and other U.S. Government employees. This information was later posted online with encouragement for ISIL supporters to conduct terrorist attacks against the identified individuals. Investigators used SCA process to a U.S. service provider to obtain the contents of communications by ISIL members. The Kosovo citizen was ultimately charged with providing material support to ISIL and with computer hacking and identity theft violations, and he has been extradited to face trial in the United States.

As these examples illustrate, the U.S. Government's ability to use domestic legal process to obtain information about persons committing crimes both inside and outside the United States is critical to enforcing U.S. law and protecting U.S. citizens and is likely to grow more critical in

the future. The Government does not know where the providers in each of these cases had stored this critical data, yet it may well have been outside the United States. As mentioned above, there is generally no requirement that American providers store data in the United States. Preserving the ability to investigate regardless of the physical location where data may be stored is essential to the Department's mission and ensuring the safety of the American people.

II. Current Rules Governing Cross-Border Access to Data

A. Access by United States Investigators to Data Stored Outside the United States

Before considering potential legislation regarding law enforcement access to data stored abroad, it is valuable to understand the current legal framework under which U.S. investigators obtain such data. Sometimes, if the company is subject to U.S. jurisdiction, investigators can use the SCA to obtain the data, regardless of where the company chooses to store it. In other circumstances, investigators may seek the assistance of a foreign government through mechanisms such as an MLAT request. Which of these mechanisms is available can have a big impact on how quickly evidence is collected, and sometimes whether the evidence can be successfully collected at all. And as I will discuss later, similar mechanisms also constrain the ability of foreign governments to obtain access to data stored in the United States.

U.S. law enforcement relies on the SCA to obtain access to electronic information stored by service providers subject to the jurisdiction of United States courts. Under the SCA, law enforcement uses legal process — warrants, court orders, or subpoenas — to require service providers to disclose information pertaining to electronic communications. This information can include both content and non-content information. Under the SCA's comprehensive framework, the Government must satisfy a standard of probable cause to obtain disclosure of some categories of information and may satisfy a lesser standard with regard to others. For example, law enforcement will generally obtain a warrant, issued by a magistrate judge and based on probable cause, to compel disclosure of the contents of communications, such as a text message relating to a gang murder or an email that includes an image of sexual abuse of a child. To obtain non-content information about the routing of communications, such as email or IP address information demonstrating that communications took place between criminals and their co-conspirators, law enforcement may use a court order based on a showing that the information sought is relevant and material to an ongoing criminal investigation. Finally, the Government may use a subpoena to obtain certain basic information relevant to an investigation, such as a subscriber's name and address.

Whether the Government obtains a subpoena, court order, or warrant, investigators can serve that process on a service provider in the same manner. The provider then gathers the information specified in the legal process and provides it to the investigators. Even when law enforcement obtains a search warrant under the SCA, the effect of the warrant is to compel the

disclosure of information within a provider's control, not to authorize agents to conduct a direct search of a provider's premises in the United States or abroad.

Courts have ruled that a communications service provider's duty to produce information in response to SCA process extends to information stored by the provider in a foreign country. This is as true of electronic information as it is of paper documents. Indeed, the Second Circuit Court of Appeals declared nearly fifty years ago that "[i]t is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has *in personam* jurisdiction of the person in possession or control of the material." *United States v. First Nat. City Bank*, 396 F.2d 897, 900-01 (2d Cir. 1968). As that court later stated, "[t]he test for the production of documents is control, not location." *In re Marc Rich & Co.*, 707 F.2d 663, 667 (2d Cir. 1983). Applied to the SCA, the Department has argued that this principle requires a communications service provider to disclose information in response to SCA process regardless of where the provider has chosen to store the information.

Historically, case law regarding the reach of compulsory process arose in the context of subpoenas, but the rule that "the test for production of information is control" extends to all forms of compulsory process under the SCA: subpoenas, court orders, and warrants. This approach makes sense. United States law generally does not tell American companies where they have to store the data that they control, but by the same token an American company's decision to locate data overseas does not insulate that data from U.S. legal process. Furthermore, SCA court orders and warrants ultimately function like subpoenas with respect to how information is gathered: they are served on a communications service provider, which is then required to disclose information in its custody (as opposed to having government agents enter and search the service provider's facilities for the requested information). The higher evidentiary threshold required to obtain SCA court orders and warrants is designed to protect the privacy interests of account holders; it does not free service providers from a duty to produce responsive information simply because that data has been stored abroad. Thus far, courts have agreed with the Justice Department that the SCA extends to information stored abroad. *See In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (M.J. Francis Opinion), *aff'd*, No. 13-mj-2814, Dkt. No. 80 (S.D.N.Y. Aug. 11, 2014). This issue is currently pending before the Court of Appeals for the Second Circuit. *See In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, No. 14-2985 (2d. Cir.).

Federal courts have also addressed concerns expressed by recipients of lawful process that compliance with that process would expose them to a conflict of laws. When the recipient establishes that there is a genuine conflict between U.S. law requiring production of information stored in a foreign country and the laws of that foreign country, U.S. courts balance several factors, including sovereignty concerns, the governmental interest in obtaining the information, and the potential hardship from compliance to the subject of the order. Courts have, however, expressed "great reluctance" to excuse the compelled disclosure of records simply because of competing directives from foreign sovereigns. *First Nat. City Bank*, 396 F.2d at 903.

Particularly in the criminal context, U.S. courts have generally found that, even where foreign law prohibits the production of the relevant records, the powerful interest of the government in enforcing criminal laws outweighs the foreign prohibition. *See, e.g.*, *In re Marc Rich & Co.*, 707 F.2d at 665 (production ordered despite claim that it would violate Swiss law). Thus far, no cases have needed to explore this doctrine in the SCA context, as no service provider has alleged, much less established, the existence of a genuine conflict between the law of a foreign nation and SCA warrants.

The MLAT process, by contrast, involves requests between countries, made on behalf of prosecutors, judicial authorities, or investigators. When a U.S. law enforcement agency requires records or information that must be obtained by MLAT, the investigative agent must first consult with a federal prosecutor, who will in turn consult with a prosecutor at the Department of Justice's Office of International Affairs (OIA). OIA serves as the Central Authority of the United States, responsible for implementing the MLATs to which the United States is a party, including by making and receiving such requests, as well as handling similar requests made pursuant to letters rogatory and letters of request. The prosecutor, with the assistance of OIA, will draft a formal request to the foreign government that meets the requirements of the MLAT, explains the facts of the underlying investigation that justifies the request, and seeks the foreign government's assistance in using its own domestic laws to fulfill the request. Typically, such requests require discussions between OIA and the Central Authority of the foreign government regarding legal sufficiency and other issues that may affect their execution. These discussions may be complicated by the fact that many countries' Central Authorities lack sufficient standing to function effectively or are not adequately staffed and must relay any questions to other parts of their government, including local officials. When a request is ready for transmission (including formal translation of the request, if necessary), OIA sends it to the foreign Central Authority, which is then responsible for conveying the request to the appropriate authority in that country for execution. Once the request has been executed, any results are conveyed back to the law enforcement agency through a similar process: to the foreign country's Central Authority, from that Central Authority to OIA, and from OIA to the relevant U.S. prosecutor.

It is worth emphasizing the significant advantages — for preventing crime and achieving justice for victims — of using SCA process instead of the MLAT process to obtain information stored abroad by American service providers: speed and reliability. Many investigations, including investigations involving terrorism, financial fraud, drug trafficking, child sexual exploitation, human trafficking, and computer hacking, must move quickly to be successful and to prevent ongoing harm. When using SCA process, the Government typically obtains information in a matter of days or weeks. In contrast, it usually takes many months for law enforcement to receive the information sought from a foreign country through the MLAT process. The MLAT procedures described above — many of which, like transmission of requests from central government authorities to foreign prosecutors responsible for executing the requests for evidence, are unavoidable — generally lack the requisite efficiency for time-sensitive investigations and other emergencies. In less experienced or less cooperative countries, the process can take even longer. Sometimes we never receive a response at all.

And this type of inefficiency may be a best-case scenario. The United States does not have MLATs with approximately half of the countries in the world. And even in cases where we are parties to MLATs, some countries entirely exclude certain categories of evidence from their MLATs: the United States' agreements with some Caribbean nations, for example, do not require assistance with investigations regarding the evasion of U.S. taxes. And some countries, despite being parties to MLATs with the United States, do not cooperate or barely do so.

Finally, even where we have a functioning treaty relationship with a country that is eager to assist, MLATs are not perfectly adapted to modern communications and electronic storage services. Reliance on an MLAT request assumes that data is at rest in a single country. But with modern communications and cloud services, that is often not the case. Data can be moved across jurisdictions or stored in multiple locations for any number of business reasons. The location of the data could change day-by-day or hour-by-hour. In such cases, sending an MLAT request to a country could result — after months of delay — in notification that the data is no longer there. Moreover, one major U.S. provider told investigators that it could not determine in which country requested data resided. For these reasons, requiring U.S. law enforcement to rely solely on the MLAT process to obtain data stored overseas by providers would, in many cases, effectively place that data out of reach of U.S. authorities. This would result in perpetrators of crimes like the ones described above escaping justice, in many cases free to continue targeting Americans.

B. Access by Foreign Governments to Data Stored in the United States

The United States is, of course, not alone in confronting new challenges to gathering the evidence necessary to enforce essential laws in an increasingly international and digital age of crime. And just as we face challenges when we are required to rely on the MLAT process to obtain critical evidence from abroad, many of our foreign partners find themselves in an even more difficult situation, reliant on evidence stored outside their borders — often, indeed, within the United States — to protect their own public safety and national security. In part, this is because the SCA plays two different functions with regard to digital information. As described above, it provides a mechanism for U.S. law enforcement to require a provider to disclose information pursuant to specified legal standards, such as a probable-cause based search warrant. But the SCA also plays a privacy-protecting role, precluding providers from disclosing the contents of communications to law enforcement or anyone else, unless certain exceptions are met. And the SCA contains no provision permitting a foreign government to compel a provider to disclose the contents of communications stored in the United States.

The experience of the United Kingdom illustrates why this scenario can be so problematic. A significant portion of the electronic communications service providers used by the U.K. public are based in, and store their data in, the United States (or elsewhere outside the United Kingdom). As a result, U.K. authorities must frequently come to the United States to access data located here, even if it is relevant to the investigation of conduct taking place entirely

outside of the United States and is not related to any U.S. persons. For instance, U.K. authorities might be investigating a British citizen who has traveled to Syria to fight with ISIL and uses email services provided by a U.S. company to communicate with his co-conspirators back in the United Kingdom. In such cases, if the data happens to be stored in the United States, U.S. law would control the manner in which that data is available to U.K. authorities, even though only British citizens are involved, the threat is directly to the United Kingdom, and the conduct is taking place entirely outside the United States. Thus, U.K. investigators may find their investigations delayed by the cumbersome MLAT procedures described above, even despite the U.S. Government's best efforts to process requests expeditiously.

Countries like the United Kingdom are adapting their laws to fit this reality. To facilitate its cross-border access to data, in 2014 the United Kingdom enacted a law that would compel a provider to disclose evidence regardless of where it is stored. Under this law, the United Kingdom can serve a production order on a U.S. company that provides communications services in the United Kingdom, and that company could be obligated under U.K. law to comply, even with respect to data located in the United States.

As a result, U.S. companies may find themselves confronted by a conflict of laws — between the U.K. law that compels the disclosure of electronic evidence stored in the United States and the U.S. law that may prevent a U.S. provider from complying. Such conflicts can pose unique challenges. Providers may risk violating U.S. law if they comply with U.K. orders and disclose communications data subject to U.S. law. If so, they could be subject to civil liability, criminal sanctions, or both. But if they refuse to comply, they could be subject to U.K. enforcement actions and fines.

The effects of such conflicts are felt acutely by many of our foreign law enforcement partners, whose ability to access data in the United States is generally constrained to the MLAT process. Similarly, it can be felt acutely by U.S. providers who wish to compete for overseas customers, but store data in the United States. Both our foreign partners as well as prominent voices among U.S. communications providers have indicated that the status quo is unsustainable in the long term. It undermines efforts by our foreign partners to protect their citizens, just as it would for U.S. authorities to protect Americans. It gives other countries strong incentives to require that their citizens' data be stored within their borders, where it is accessible under that country's law, a policy referred to as data localization. Such policies threaten to Balkanize the Internet, raise the costs to American providers of doing business abroad, and render data inaccessible to U.S authorities. And it exposes U.S. providers to potential enforcement actions and fines by foreign countries for adhering to U.S. law.

III. Possible Legislation

The Department recognizes that issues involving access to data stored in foreign countries can be complex and create difficulties for all stakeholders involved. We must strive to balance several, sometimes competing goals. Most importantly, we must fulfill the responsibility

Congress and the American people have entrusted to us by taking lawful steps to protect Americans and American companies from threats to their safety and security. But we must also do our best to meet the legitimate public safety and justice needs of other countries that require access to evidence that happens to be stored in the United States, without compromising users' legitimate privacy interests. And we must recognize that U.S. service providers seeking to compete in a global marketplace may, in some instances, face conflicting legal obligations from the many nations in which they choose to do business, and minimize those conflicts where possible. Finding solutions that satisfy all of these goals will be difficult, and we are committed to an open conversation among stakeholders about how to do so.

Nevertheless, some measures could potentially improve current processes for access to data stored abroad, for both the United States and our law enforcement partners.

In particular, the United States has begun considering a framework under which U.S. providers could disclose data directly to the United Kingdom for serious criminal and national security investigations when the United Kingdom obtains authorization to access the data under its own legal system, while protecting privacy and civil liberties. The framework would not permit bulk data collection and would not permit foreign-government targeting of any U.S. persons or persons known to be located in the United States. Moreover, it would not impose any new obligations on providers at all under U.S. law; instead, any requirement to comply with the foreign order would derive solely from the requesting country's law. The framework would, in turn, permit reciprocal access for U.S. law enforcement to data stored in the United Kingdom, which will become increasingly important for data located beyond U.S. borders and subject to foreign law. If the approach proves successful, we would consider it for other like-minded countries as well.

This approach would require amendments to U.S. law, in the form of new exceptions to the SCA and similar U.S. laws governing access to electronic data. These exceptions would lift the statutory prohibition on disclosure of communications data for lawful requests from a foreign partner with which the United States has a satisfactory executive agreement. The general parameters of a satisfactory agreement would be legislated by Congress, and we would welcome the opportunity to work closely with Congress in developing the legislative parameters for such agreements.

To succeed, any framework must establish adequate baselines for protecting privacy and civil liberties, both through the agreement and implementing legislation. For example, legislation should require the foreign country's law to have in place appropriate substantive and procedural protections for privacy and civil liberties; it should prohibit use of the agreement for bulk data collection; and it should require robust targeting and minimization procedures to prevent the targeting of and ensure the protection of U.S. person data. In this way, the framework would ensure that there are sufficient protections for privacy and civil liberties, while permitting countries to maintain appropriate checks and balances for doing so within their existing legal framework. The framework would not require our foreign partners to mirror the

American legal system. However, we expect that the benefits of securing such an agreement could encourage interested countries to improve their legal protections for communications data to a satisfactory level.

There are a number of benefits to such a framework. Importantly, it would secure reciprocal access for the United States to data in the United Kingdom in an efficient, effective, and privacy-respecting manner. It would support our partner's ability to investigate serious crime as well as terrorism and other transnational crimes – threats that may, in turn, also affect us. It would decrease the existing burden on the MLAT process, thereby freeing resources for all other MLAT requests; in other words, it would improve cross-border access to data even for countries that did not join the framework. It would reduce the impetus for foreign countries to implement data localization policies, which would be harmful to U.S. commercial interests and public safety, while encouraging them to develop stronger privacy protections. And it would help obviate a potential obstacle to U.S. communications service providers' ability to compete for global business by reducing the risk that providers face from potential international conflicts of laws.

This approach would be a complement to and not substitute for reform of the MLAT process, which the Department is pursuing as well. For example, the Department has undertaken efforts to reform the way in which we take in and address the myriad requests for assistance we receive from foreign governments through the mutual legal assistance process. The Department has done so taking into account the significant technical, financial, administrative, and security needs that accompany such a reform effort. We would welcome congressional efforts to provide appropriate resources for this effort. Reform of the MLAT process must take into account the complexity of MLAT intake procedures and the Department's associated administrative needs.

At the same time, the Department also believes it is critical to public safety that Congress avoid legislation that would erect new obstacles to the ability of U.S. law enforcement to investigate criminal activity in cases where a provider has stored the data abroad, either for its own business reasons or pursuant to pressure by foreign governments. Here, I will discuss proposals such as those contained in the Law Enforcement Access to Data Stored Abroad Act ("LEADS Act"). To be sure, the LEADS Act raises a number of different issues. Aspects of the bill seek changes similar to those contained in other proposals to reform the Electronic Communications Privacy Act ("ECPA"), and I would refer you to the testimony submitted on behalf of the Department at this Committee's December 1, 2015 hearing on that subject. For example, the Department has stated that proposals that would create a requirement to obtain a warrant based on probable cause to compel disclosure of stored email and similar stored content information from a service provider have considerable merit, provided that Congress considers contingencies for certain, limited functions, such as civil law enforcement, for which this may pose a problem. We look forward to continued discussions on how to accommodate these different interests.

However, the Department is concerned that other aspects of the LEADS Act would impair our ability to investigate crimes ranging from national security cases to human and drug trafficking to cyber intrusions and child sexual exploitation. Moreover, the changes the LEADS Act calls for are unnecessary, in that current law already contains safeguards to preclude inappropriate access by U.S. law enforcement to data stored abroad. In contrast to the framework outlined above, we believe that bills like the LEADS Act would be highly counterproductive to the law enforcement interests of the United States and our foreign partners and potentially to the privacy interests of users of American providers as well.

First and most importantly, the Department strongly opposes legislation that would require U.S. investigators to rely exclusively on MLAT requests for important categories of evidence located in foreign countries. Doing so will inevitably slow — and in some cases end — the investigation of serious offenses against Americans. For example, the LEADS Act would require investigators to rely on mutual legal assistance requests to obtain electronic evidence from overseas when the account holder is not a U.S. person. But successful investigation of crimes of the type I discussed previously — including child sexual exploitation and terrorism — often requires obtaining information from accounts of non-U.S. persons abroad. If the evidence at issue in those cases had been stored abroad, and SCA process had been unavailable, those investigations may well have failed.

As a practical matter, if SCA process is not available, U.S. law enforcement may be unable to obtain evidence in many cases. As previously noted, while mutual legal assistance requests can be useful, receiving evidence from foreign governments takes several months at best. In the worst cases, foreign countries take years, or never respond at all. Indeed, countries generally are not obligated to cooperate with one another unless they are party to an MLAT, and the United States has MLATs only with about half the countries of the world. Even with our treaty partners, swift action, or the will or ability to cooperate quickly, is not guaranteed. While assistance without an MLAT is possible, cooperation based on a foreign partner's domestic law, or comity and reciprocity, is discretionary. Thus even with seemingly cooperative counterparts, assistance can be delayed or ultimately refused.

Some of our foreign partners have similar concerns with relying on MLAT requests when they seek to obtain electronic evidence located in the United States. The framework outlined above is one approach to addressing some of these concerns with the MLAT process, but more needs to be done to improve the process on all sides. Legislative proposals should enhance ongoing efforts to improve the way that the Department of Justice handles MLAT requests. At the same time, the Department believes that we must avoid unworkable provisions that would complicate the strides that have been made to reform the MLAT process, particularly with regard to how the United States responds to requests from our foreign partners seeking electronic records held by U.S. providers.

Second, the Department opposes legislation that would forbid law enforcement from using a warrant to investigate people living in the United States. Some proposals have suggested

that officers should be permitted to use warrants only where the account holder is a "United States person," but define the term to extend only to U.S. citizens and permanent residents. Narrow definitions like this would exclude, for example, foreign nationals engaged in criminal activity within the United States. The majority of the 9/11 hijackers were in the United States on tourist visas; their email accounts could have been protected under such legislation depending solely on where their data was stored. It makes no sense to accord such individuals greater protections than Americans, and such restrictions would in some cases end or significantly impede investigations of crimes committed by foreigners within the United States.

Third, in the Department's view, legislation should not prevent law enforcement from using a warrant where the citizenship of the account holder cannot be adequately established. Some proposals condition law enforcement's ability to obtain a warrant on proof that the account holder is a U.S. person. But law enforcement officers often investigate crimes before they know the identity and nationality of the perpetrator. In fact, they may need the information from the service provider for the very purpose of determining the identity and nationality of the target. As a general matter, investigators often do not know the nationality or identity of hackers or those sexually exploiting children online until near the end of an investigation. Requiring investigators to know the nationality of criminals before they can investigate would often make it impossible to bring offenders to justice.

Fourth, in the Department's view, legislation should not delegate power to foreign legislatures to determine whether U.S. law enforcement should be able to access evidence using U.S. search warrants. Some proposals would require U.S. courts, upon motion of the provider, to "modify or vacate" an otherwise valid U.S. search warrant — even a warrant seeking data belonging to a U.S. citizen — if the data is stored abroad and complying with the warrant would conflict with the law of a foreign country. We are concerned that, under this sort of rule, any country whose interests are adverse to the United States could pass a law that would bar use of U.S. warrants — even if the data were not stored in that country. And even countries whose interests are not adverse would face pressure from their own citizens and companies to take advantage of this new statutory loophole in U.S. law enforcement authority. Addressing conflicts of law is a complex issue, and we believe the framework discussed above is one example of how to strike the right balance. Conditioning U.S. law on foreign law is not the right balance.

Fifth, the Department believes that legislation should not promote foreign data storage, potentially at the expense of user privacy. Although the United States has some of the best privacy protections of any legal system in the world, our system increasingly faces mistaken and misinformed criticism from abroad. U.S. providers have reported that this criticism has created market incentives for companies to advertise that they store data in ways that are inaccessible to U.S. law enforcement. Passing laws that would bar U.S. law enforcement access to certain categories of data stored abroad (other than potentially through the MLAT process) could thus incentivize U.S. providers to store user data overseas so as to render the information unavailable to U.S. law enforcement and place competitive pressure on companies that wish to continue

storing data in the United States. The result would be that many users' data could potentially be subject to the less protective laws of other countries rather than the strong protections of U.S. law. In the Department's view, such legislation would thus hamstring U.S. law enforcement while, in many cases, risk decreasing user privacy at the same time.

Moreover, as described above, the LEADS Act would in no way affect the authority of foreign governments to demand data stored in the United States by U.S. companies. More and more countries have been demanding such access, placing U.S. companies in a difficult position. Rather, the LEADS Act operates only to restrict the authority of U.S. investigators. Given the criminal and national security threats currently facing Americans, this approach, quite simply, makes no sense. By contrast, the framework currently under discussion with the United Kingdom would address the legitimate public safety needs of other countries, minimize conflicting legal obligations faced by our companies, and protect users' privacy interests, while permitting our law enforcement officers to fulfill their responsibility to protect the safety and security of the American people.

* * *

The Department appreciates the opportunity to discuss this issue with you, and we look forward to continuing to work with you. This concludes my remarks. I would be pleased to answer your questions.