INTERNATIONAL CONFLICTS OF LAW AND THEIR IMPLICATIONS FOR CROSS BORDER DATA REQUESTS BY LAW ENFORCEMENT

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

FEBRUARY 25, 2016

Serial No. 114–84

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

98–827 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
MIMI WALTERS, California
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
DAVE TROTT, Michigan
MIKE BISHOP, Michigan

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island
SCOTT PETERS, California

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM,

CONTENTS

FEBRUARY 25, 2016

INTERNATIONAL CONFLICTS OF LAW AND THEIR IMPLICATIONS FOR CROSS BORDER DATA REQUESTS BY LAW ENFORCEMENT

THURSDAY, FEBRUARY 25, 2016

HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY

Washington, DC.

The Committee met, pursuant to call, at 10 a.m., in room 2141, Rayburn House Office Building, the Honorable Bob Goodlatte, (Chairman of the Committee) presiding.

Present: Representatives Goodlatte, Chabot, Issa, King, Jordan, Poe, Marino, Gowdy, Collins, DeSantis, Walters, Buck, Ratcliffe, Bishop, Conyers, Lofgren, Johnson, Chu, DelBene, Jeffries, and Peters.

Staff Present: Shelley Husband, Chief of Staff & General Counsel; Branden Ritchie, Deputy Chief of Staff & Chief Counsel; Zachary Somers, Parliamentarian & General Counsel; Kelsey Williams, Clerk; Jason Herring, Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; (Minority) Perry Apelbaum, Minority Staff Director & Chief Counsel; Danielle Brown, Parliamentarian & Chief Legislative Counsel; Aaron Hiller, Chief Oversight Counsel; Joe Graupensperger, Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; and Veronica Eligan, Professional Staff Member.

Mr. GOODLATTE. Good morning. The Judiciary Committee will come to order, and without objection, the Chair is authorized to declare recesses of the Committee at any time.

We welcome everyone to this morning's hearing on "International Conflicts of Law and Their Implications for Cross-Border Data Requests by Law Enforcement," and I will begin by recognizing myself for an opening statement.

Today's hearing will examine international conflicts of law and how these conflicts impact law enforcement access to data both here and abroad. This is an extremely important issue that affects individuals, technology companies, law enforcement, and the economy. In the digital age, where the Internet knows no boundaries, U.S. technology companies have flourished internationally and provide services to customers and subscribers around the world, but there is a growing tension between U.S. law and foreign law, and U.S. technology companies are caught in the middle.

U.S. law places restrictions on access to data by foreign countries, making it difficult if not impossible in some instances to obtain evidence of crimes or terror plots carried out by their own citizens in violation of their laws. This has provided an incentive for foreign governments to enact their own legislation to address the problem. Some foreign governments have enacted laws requiring U.S. technology companies as a requirement for doing business there to comply with that government's requests for data.

Alternatively, other countries are considering legislation that would require U.S. providers to locate servers in that country to ensure that country's jurisdiction over the U.S. provider. This is sometimes referred to as data localization. The disparity between U.S. and foreign law has similarly created a conflict with regard to what law governs requests by the U.S. Government to U.S. companies for data stored in foreign countries.

Certain foreign countries prohibit the removal of data from their boundaries in contravention of their law. U.S. law, on the other hand, makes no distinction between data stored domestically versus data stored abroad, nor any distinction with regard to the nationality or location of the customer.

The result of these conflicts is that U.S. technology companies find themselves with a Hobson's choice: either comply with U.S. law, or comply with foreign law. But it is increasingly impossible to comply with both. This is an untenable situation for U.S. tech companies. This conflict also thwarts timely access to information by foreign governments, and has the potential to create additional barriers for U.S. law enforcement.

Current U.S. law requires foreign governments who want access to content maintained by a U.S. technology company to make a government-to-government request for the data.

This is generally accomplished through the mutual legal assistance treaty, or MLAT process, but frankly, the MLAT process is slow and cumbersome. It has been reported that an MLAT request takes, on average, approximately 10 months. This is clearly causing serious frustration from foreign governments who have legitimate interests in their own public safety.

For example, a foreign government may be investigating criminal activity that has occurred wholly within that government's borders by its own citizens, but because the perpetrators are utilizing the email services of a U.S. email provider, that foreign government cannot get access to email content for evidentiary purposes, except through the MLAT process, which takes entirely too long. The current arduous MLAT process likewise poses significant hurdles to the U.S. Government obtaining information stored abroad from U.S. companies, and is not designed to carry the heavy burden of these types of cross-border data requests.

It is abundantly clear that Congress must find a legislative approach that embraces the modern manner in which data is stored and acquired internationally.

One such approach could be bilateral agreements between the U.S. and foreign countries that work to resolve or waive these conflicts of law. Earlier this month, it was reported that the U.S. and the United Kingdom recently commenced negotiations on a bilateral agreement that would allow the U.K. Government to request

data directly from U.S. companies in criminal and national security investigations not involving U.S. persons. This type of agreement may serve as model for future agreements, and thus relieve some of the international pressure on U.S. tech companies, but we must closely examine important details, such as the legal standard for which the U.K. Government may make requests of U.S. tech companies, whether such requests would require an independent review, and what privacy protections should be implemented.

Such an agreement could also help alleviate any conflicts of law relating to requests by the U.S. for data stored abroad by U.S. companies. But any such agreements must preserve American civil liberties and privacy protections embodied in U.S. law.

Ultimately, in order for a bilateral agreement of this kind to have effect, Congress would first need to enact legislation enabling direct access to U.S. companies by foreign governments, and prescribing the criteria that must be met by the foreign government to receive such access.

Once again, the House Judiciary Committee finds itself at the forefront of a pressing issue that impacts personal privacy, national security, public safety, economic viability, and the rule of law. Members of this Committee have been dedicated to finding a legislative solution to address the issues raised by the current conflict of laws, and we will continue to examine all options presented to the Committee.

As always, we will not shy away from the heady task ahead of us in finding a thoughtful, balanced solution to this problem. I look forward to closely examining these issues today and hearing from our distinguished witnesses, and with that, I am pleased to recognize the Ranking Member of the Committee, the gentleman from Michigan, Mr. Conyers, for his opening statement.

Mr. CONYERS. Thank you, Chairman Goodlatte. And thanks to all of our witnesses on both panels for the time they are taking to be with us today. The House Judiciary Committee is the appropriate forum for a topic that never seems to leave the news: how government agencies access the content of our communications.

Over the past few years, we have explored this theme in various forms: government surveillance, the FBI's effort to build back doors into strong encryption, and our works to reform the Electronic Communications Privacy Act. Today, we discuss a different aspect of this theme: how law enforcement agencies attempt to access data stored beyond their jurisdictional reach.

Whatever your favorite policy solution may be, everyone in this room agrees that there is a problem that must be solved. Twenty years ago, a police officer in the United Kingdom investigating a routine crime would have had little reason to seek evidence stored in the United States, but today, on a daily basis, law enforcement agencies around the world request access to digital evidence stored in other countries. And the legal framework in place for making those requests is wholly inadequate to the task.

The mutual legal assistance treaty system was written for a different era, and struggles to keep pace with the scope and pace of modern communications. Our Members have also been outspoken in the need to modernize the Electronic Communications Privacy Act, and I hope we will do it soon.

I am also a co-sponsor of H.R. 1174, the "Law Enforcement Access to Data Stored Abroad Act." Now I signed onto this bill because it is an important vehicle for the discussion that we will have today, and I thank the gentleman from Pennsylvania, Mr. Marino, the gentlelady from Washington, Ms. DelBene, and Mr. Amodei, Nevada for their leadership on this issue. The LEADS Act takes a holistic view of the system.

It reforms ECPA to require warrants for content in the domestic content. It also provides one solution for Federal law enforcement to reach data that is stored abroad. And, it begins a much needed overhaul of the mutual legal assistance treaty framework, and even if we may reach consensus on a solution that differs from the LEADS Act, it will have been important legislation for having recognized early that we need to use every tool in our toolbox to update Federal law for the digital age.

One other possibility for reform that I would like to discuss today is the idea of bilateral agreements with our closest allies. Those Nations we trust most on civil liberties and due process issues. We should add this concept to the mix. In addition to amending the Electronic Communications Privacy Act, and updating our treaty system, these agreements could counter the trend toward data localization, incentivize our partners to set better standards for data protection, and help our closest friends investigate serious crimes that often impact the United States either directly or indirectly. I would add only two notes on this topic for our distinguished guests from the Department of Justice.

First, I hope to have your agreement today that no deal with the United Kingdom is better than a deal that does not honor privacy, due process, and free expression on both sides of the Atlantic.

Secondly, I hope that this will be a collaborative process. It is unfortunate that we learned about your discussions with the British from the Washington Post before we heard about them from you. I appreciate that the Department took the time to brief Committee staff earlier this week. It was important, I appreciate how candid the Department was about possible civil liberties concerns going forward. I am sure that working together, we can come up with a system of reforms that benefits each of the stakeholders in this discussion.

And so I thank the Chairman and yield back any time that might be remaining. Thank you.

Mr. GOODLATTE. Thank you, Mr. Conyers. And without objection, all other Members' opening statements will be made a part of the record.

[The prepared statement of Ms. Jackson Lee follows:]

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
2160 Rayburn House Office Building
Washington, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE:
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 861-4070

FIFTH WARD OFFICE:
3300 LYONS AVENUE, SUITE 301
HOUSTON, TX 77020

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
COURTS AND COMPETITION POLICY
IMMIGRATION, CITIZENSHIP, REFUGEES, BORDER SECURITY, AND INTERNATIONAL LAW
CRIME, TERRORISM AND HOMELAND SECURITY
CONSTITUTION, CIVIL RIGHTS, AND CIVIL LIBERTIES

HOMELAND SECURITY
SUBCOMMITTEES:
CHAIR
TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

FOREIGN AFFAIRS
SUBCOMMITTEES:
AFRICA AND GLOBAL HEALTH
MIDDLE EAST AND SOUTH ASIA
TERRORISM, NONPROLIFERATION, AND TRADE

SENIOR WHIP
DEMOCRATIC CAUCUS

CONGRESSWOMAN SHEILA JACKSON LEE OF TEXAS
Ranking Member
House Judiciary Committee
Subcommittee on Crime, Terrorism, Homeland Security, and Investigations

COMMITTEE ON THE JUDICIARY
FULL COMMITTEE HEARING ON
"INTERNATIONAL CONFLICTS OF LAW CONCERNING CROSS BORDER DATA FLOW AND LAW ENFORCEMENT REQUESTS"
2141 RAYBURN
10:00 A.M.

FEBRUARY 25, 2016

- Good morning. Thank you, Chairman Goodlatte and Ranking Member Conyers for holding this hearing.

- And thank you to all of our witnesses who are here today.

- The topic of this hearing, assessing "International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests" is a critically important issue we need to address as we progress in the age of technology, innovation and highly sophisticated means of threatening our national security.

- As Ranking Member of the Subcommittee on Crime, Terrorism, Homeland Security and Investigations and a senior member of the Homeland Security Committee, I am gravely concerned about the legal implications as well as the national security implications of accessing data across international border lines.

- We must engage our allies on the topic of data protection and find common ground to move forward.

- The Internet is a global medium and enforcement of US laws requires the cooperation of the global community.

- Congress has moved to provide an equal level of data protection to European citizens as U.S. citizens to acknowledge the level of data protection provided to U.S. citizens by EU data protection laws.

- While the 1986 enactment of the *Electronic Communications Privacy Act (ECPA)* (which sought to govern how law enforcement agencies and private parties may access electronic communications, was meant to be forward looking as technologies began to rapidly advance), and various lower court decisions such as the 2010 Sixth Circuit case *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010), (which held that subscribers have a reasonable expectation of privacy in the content of electronic communications and that the government must obtain a warrant to access email stored by a third party), have attempted to clarify and govern electronic storage on third party servers, constitutional and legislative privacy safeguards for electronic

communications and other forms of developing digital media are wholly inadequate for modern times.

- The advent of Cloud Commuting services has only further broadened the question of third parties and communications due to the storage of not only emails, but digital photos, video, audio, electronic books, music preferences, political views, religious beliefs or the lack thereof.

- Smart devices in use by tens of millions of Americans allow for the collection, and retention of much more information - and that retention is outside of the control of the email user.

- Consumers, technology companies, law enforcement officials, related stakeholders and members of Congress on both sides of the aisle, all agree that reform is badly needed.

- Two viable options Congress has within its immediate purview to act upon are "the Email Privacy Act, (H.R. 699)" and "the Law Enforcement Access to Data Stored Abroad Act, or the LEADS Act (H.R. 1174)".

- The Email Privacy Act which I cosponsored along with 309 of my Democratic and Republican colleagues, and the LEADS Act, which I am also a cosponsor of along with 134 of my colleagues from both sides of the aisle, certainly set forth a necessary step in the right direction.

- Both the Email Privacy Act and the LEADS Act would unquestionably fix several of *ECPA's* long overdue deficiencies.

- Importantly, both bills will amend the 30-year old *ECPA* to prevent the government from accessing private electronic communications without a probable cause warrant.

- Both proposed statutes would eliminate the procedural delay of set forth by the 180-day rule and provide that law enforcement must *always* obtain a search warrant to compel disclosure of customers' private email communications.

- 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.

- While the LEADS Act and the Email Privacy Act differ in several other recommended routes to reform *ECPA*, both bills have broad bipartisan support and demand further action.

The Email Privacy Act (H.R. 699)

- Specifically, the Email Privacy Act will prohibit a provider of remote computing service or electronic communication service (including email communications) to the public from *knowingly* divulging to a governmental entity the contents of any communication that is in electronic storage or otherwise maintained by the provider, subject to exceptions.

- This bill will revise provisions under which the government may require a provider to disclose the contents of such communications.

- Importantly, the Email Privacy Act requires the government to obtain a warrant from a court before requiring providers to disclose the content of such communications *regardless of how long the communication has been held in electronic storage* by an electronic communication service, or whether the information is sought from an electronic communication service or a remote computing service.

- FBI Director Comey, has testified that the current practice of the FBI is to obtain a warrant for e-mail communications, and that this bill would not change their current practices.

- Moreover, the Email Privacy Act would not change any of the existing exceptions in ECPA that allow emergency requests for assistance to be processed in a timely manner.

- The Email Privacy Act is an important measure that directs the Comptroller General to report to Congress regarding disclosures of customer communications and records under provisions: (1) as in effect before the enactment of this Act, and (2) as amended by this Act.

The LEADS Act (H.R. 1174)

- "The LEADS Act, introduced by my Judiciary colleague Suzan DelBene (D-WA), would 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:

    - Emails that are physically stored within the United States; and
    - Emails of U.S. nationals that are stored outside the United States.

- The LEADS Act also 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.

- Lastly, the LEADS Act addresses the equally demanding need for reforming the *Mutual Legal Assistance Treaty (MLAT)* process by improving efficiency and transparency through the creation of a new online intake form, and further requests the Department of Justice to document statistics relating to the amount of time and the number of MLAT requests made.

- Both the LEADS Act and the Email Privacy Act, through overwhelming bipartisan support are making strides to make sure that citizens are secure and protected in their digital records and effects.

- Either proposal would be an important step in the right direction towards modernizing and improving the EPCA framework.

- Again, thank you for holding this important hearing and I look forward to the testimony of our distinguished panel of witnesses concerning these proposal and other considerations for reform.

- Thank you. I yield back the remainder of my time.

Mr. GOODLATTE. We welcome our distinguished witness of today's first panel. And if you would please rise, I will begin by swearing you in. Do you swear that the testimony that you are about to give shall be the truth, the whole truth, and nothing but the truth so help you God? Thank you very much.

And I will now introduce our witness for today's first panel. Mr. David Bitkower serves as the Principal Deputy Assistant Attorney General of the U.S. Department of Justice. Prior to joining the criminal division at the DOJ, Mr. Bitkower was an Assistant United States Attorney in the eastern district of New York.

He is a graduate of Yale University and Harvard Law School. Your written testimony will be entered into the record in its entirety, and we ask that you summarize your testimony in 5 minutes or less; and to help you stay within that time, there is a timing light on your table. When the light switches from green to yellow, you have 1 minute to conclude you testimony. When it turns red, that is it. Your time is up. Welcome. Please begin.

TESTIMONY OF DAVID BITKOWER, PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL UNITED STATES DEPARTMENT OF JUSTICE

Mr. BITKOWER. Thank you. And good morning 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 international conflicts of law, cross border data flow, and law enforcement requests. The Department recognizes that issues concerning cross border law enforcement access to data, while vitally important, can be complex and require balancing several sometimes competing goals.

Mr. GOODLATTE. Mr. Bitkower, you may want to pull that microphone a little closer to you.

Mr. BITKOWER. Certainly, thank you. Most importantly, we must fulfill the responsibility that Congress and the American people have entrusted to us by taking lawful steps to protect Americans from threats to their safety and security. But we must also do our best to meet legitimate public safety needs of other countries that require access to evidence that happens to be stored in the United States without compromising users' 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 Nations where they choose to do business; and we should seek to minimize those conflicts where possible.

Finding solutions that satisfy all of these goals will be difficult, and we welcome this hearing as part of an important discussion about how to do so. I will focus on two issues this morning.

First, I will discuss the increasingly important role that cross border access to data plays in the protection of the public, both for the United States and for our foreign partners. Second, I will discuss a potential new opportunity to build a framework for cross border access to data that would facilitate legitimate law enforcement requests for electronic information, help to alleviate conflicts of law as faced by service providers, and protect privacy and civil liberties.

Two related trends have significantly increased the need for U.S. law enforcement to be able to access electronic data that may be stored overseas.

First, the rapid growth of Internet use has meant that law enforcement increasingly relies on electronic data, such as the content of emails or text messages, in identifying perpetrators and bringing them to justice.

Second, while much of this information is stored within the United States, providers are increasingly storing information outside the United States as well. United States law generally does not require providers to store data here, and U.S. providers increasingly face tax or other business incentives as well as pressure by foreign governments to store data outside the United States.

In fact, many of the largest American providers now operate data centers abroad, and it is unusual for a major provider to store all of its data within a single country. For these reasons, although law enforcement access to data stored abroad is already a key issue for the United States, its importance is likely to grow over time. Under United States law, when a provider is subject to the jurisdiction of U.S. courts, U.S. law enforcement may use the Stored Communications Act, or SCA, to obtain this data.

The SCA's efficient and privacy protecting process is critical to successful investigations. When SCA process is unavailable, U.S. law enforcement may attempt to obtain information stored abroad through international cooperation mechanisms, such as mutual legal assistance treaty, or MLAT requests, but the MLAT system can be cumbersome and is overburdened, and the United States does not even have MLAT treaties with half the countries in the world.

As a result, criminals may remain free to commit serious crimes against Americans. The United States is of course not alone in confronting these challenges. Many of our foreign partners, including close allies such as the United Kingdom, find themselves in an even more difficult situation reliant on evidence stored outside their borders, often within the United States, to protect public safety and national security. The difficulty arises in part because the SCA not only serves as the mechanism for U.S. law enforcement to require a provider to disclose information, but also precludes providers from disclosing the contents of communications unless certain exceptions are met; and the SCA contains no exception permitting a provider to disclose the contents of communications in response to a foreign production order.

Thus, when a foreign country makes a request under its own law for an American provider to disclose data stored in the United States, the provider may face conflicting legal demands, compulsion to disclose under foreign law, and simultaneous preclusion of that disclosure under American law. This is so even if, for example, the order relates solely to a crime committed by the country's national within its own territory.

The result may be to stymie legitimate investigations, motivate foreign countries to require data to be stored within their own borders, and expose American companies and their employees to potential enforcement actions abroad. There is widespread acknowledgement that this status quo is untenable. To address these prob-

lems, the Administration is currently considering a framework under which U.S. providers could disclose data directly to the United Kingdom in response to a lawful U.K. order. The agreement would not permit the targeting of U.S. persons or persons within the United States, and would not be used for bulk collection. The agreement would also secure reciprocal access for the U.S. to data located in the United Kingdom. We recognized that any such agreement would require legislation, both to lift conflicts of laws in carefully specified circumstances, and also to set forth base line standards to project privacy and civil liberties.

We look forward to working with Congress as we continue to explore this approach. Should the approach prove successful, we would consider it for other like-minded governments as well. We believe the framework I have described rather than legislation that would unilaterally restrict U.S. law enforcement authority, offers a path forward to efficient and privacy protecting cross border law enforcement access to data. Thank you, and I look forward to answering your questions.

[The prepared statement of Mr. Bitkower follows:]

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.

Mr. GOODLATTE. Thank you. We will now begin the questioning, and I will recognize myself. Mr. Bitkower, what will happen if Congress fails to implement legislation to facilitate international agreements such as the one currently being negotiated with the United Kingdom?

Mr. BITKOWER. Thank you for the question, Congressman. And I think it goes to the heart of why such a framework is so helpful. As we said, the status quo today is untenable, both for our close allies and for our companies. If there is no agreement or path forward, then our companies will increasingly face conflicts of law situations when foreign countries, including close allies such as the United Kingdom, have legitimate requests for data related to legitimate investigations under their own law, the only connection to the United States of which is that the data happens to be stored here, and the provider is precluded under United States law from complying with that request.

I think we will see that situation continuing to grow as crime becomes more international and as data can move around more easily, and if we do not resolve those questions, then we will face both continuing pressure from our allies as well as continuing pressure on our own companies.

Mr. GOODLATTE. Do you agree that the Stored Communications Act is silent as to whether its procedures apply to data stored outside the U.S. or to non-U.S. persons outside the U.S.?

Mr. BITKOWER. Again, thank you for the question, Congressman. So, the U.S. Stored Communications Act is a form of compulsory process. And U.S. law at the time the SCA was enacted and in fact, for many decades has provided the compulsory process, if served on a company within the jurisdiction of the United States, can require that company to produce materials, even if those materials happen to be stored abroad. This has been the law of the United States for many decades and in fact many countries have similar laws. I think we saw, in fact, even in the case involving Microsoft in Ireland.

Mr. GOODLATTE. Yeah, can you answer the question though? Is it silent with regard to these parties?

Mr. BITKOWER. So the text of the law does not particularly mention where the data is stored and does not turn one way or the other in where data is stored.

Mr. GOODLATTE. So, what guidance do U.S. providers have as to the application of the Stored Communications Act to data or customers that are outside the U.S.?

Mr. BITKOWER. So again, we think that since this SCA was legislated against a backdrop of U.S. law, which applies across a variety of contexts, not just in electronic communications contexts.

Mr. GOODLATTE. Is your answer that it does not give guidance to this?

Mr. BITKOWER. No, to the contrary, sir. My answer is that it operates like other forms of compulsory process where the law is clear that companies may be required to retrieve data from abroad in response to a lawful request.

Mr. GOODLATTE. Okay. Should a bilateral agreement such as the one under consideration with the U.K. also ameliorate any conflicts

of law with regard to U.S. requests for data held by U.S. companies in that other country that is a party of the bilateral agreement?

Mr. BITKOWER. Yes, Congressman. One of the primary benefits in an agreement of this nature would be to have reciprocal benefits for the United States in lifting any conflicts of law that might be present in the other country from where we request data.

Mr. GOODLATTE. And in your written testimony, you say that a successful bilateral framework must establish adequate base lines for protecting privacy and civil liberties, both through the agreement and implementing legislation. And you also go on to say that, for example, legislation should require the foreign country's law to have in place appropriate substantive and procedural protections for privacy and civil liberties. What does that mean?

Mr. BITKOWER. So thank you, Congressman. That is an area where we had hoped to work very closely with Congress and in particular with this Committee in establishing what those base lines ought to be. Our goal is that when we choose a country to conclude such an agreement with, we would want to ensure that that country has adequate substantive and procedural base lines to ensure that the orders that they are submitting and serving on our providers are ones based on a rule of law framework, they provide protections for civil liberties, they provide protections for privacy. And so that way our companies can be sure they are complying with legitimate requests.

Mr. GOODLATTE. Thank you very much. I now recognize the gentleman from Michigan, Mr. Conyers for his questions.

Mr. CONYERS. Thank you, Mr. Chairman. And welcome to our hearing, sir. In the case pending before the Second Circuit right now, the Department of Justice and Microsoft differ on the application of the law to data stored on servers outside the United States.

I would like to focus on some areas that I think we may be in agreement on. Do you believe that companies like Microsoft face a difficult decision when U.S. laws like the Electronic Communications Privacy Act dictates one outcome, and the law of a different country dictates another? That is a pretty difficult situation, is it not?

Mr. BITKOWER. I absolutely agree, Congressman. Our companies currently can be caught in difficult conflicting legal obligations, in particular when foreign countries seek access to data that is stored here in the United States.

Mr. CONYERS. Do you believe that the Electronic Communications Privacy Act should be reformed to address this issue?

Mr. BITKOWER. So, thank you, Congressman. I am aware this Committee held a hearing in December on the subject of the Electronic Communications Privacy Act. The Department was privileged to submit testimony to that hearing, and obviously we stand by that today. We recognize that certain aspects of the Electronic Communications Privacy Act have not kept date with the way technology is used, and the Department is open to certain changes in that statute, provided contingencies are made to protect important civil and criminal law enforcement functions.

Mr. CONYERS. Now, in February, the Washington Post reported that the Department of Justice had entered into negotiations with the British government on an agreement that would allow British

agencies to serve wiretap orders directly on United States companies. Do you think it might have been appropriate for us to learn about this activity from the Department of Justice rather than the Washington Post?

Mr. BITKOWER. Certainly, Congressman. We believe that close collaboration with Congress is essential in this area as in many others. I do not want to overstate any progress we have made. The negotiations began just very recently. We only very recently received, in fact, the authorization to begin those negotiations, at approximately the time that that Washington Post article was published. We obviously did look forward to the opportunity to brief this Committee and other Committees of jurisdiction and we hope to work with you in the future as well.

Mr. CONYERS. Well, is it your position that our government should be able to obtain data stored abroad by applying the Electronic Communications Privacy Act to any company based in the United States?

Mr. BITKOWER. Thank you, Congressman. We think it is essential that the United States be able to obtain data without regard to its location, if the provider is subject to U.S. jurisdiction. As I noted in my testimony, there are numerous examples of cases where individuals who may be outside the United States, who may not be United States citizens, whether they are in the United States or not, commit very serious crimes against Americans, and if we do not have access to data and evidence, then those crimes could continue. So we do take seriously potential conflicts of laws that our companies may face.

We do everything in our power to minimize those and see if there are work arounds we can engage in. But at the end of the day, if the United States does not have the authority to gather evidence simply based on the location of that evidence, then not only will our citizens suffer, but in fact, an agreement of the type we are talking about today, would have no reciprocal benefit for the United States.

Mr. CONYERS. All right. Is there some way we can speed up the negotiations and the conferences and all this business so that this does not take months and months, and jeopardize the interest of a lot of individuals and companies? How would we react if the Chinese government, for example required, a Chinese company like Alibaba, which maintains the data center in the United States, to produce account information that belongs to a U.S. citizen or citizens?

Mr. BITKOWER. So thank you, Congressman. Again, that is I think one of the key conflicts of laws that our companies may face. That is they receive requests from other companies in other countries, for data that our companies may store in the United States. Sometimes those are requests that they very much want to respond to. Legitimate requests from close allies to resolve crimes in their territory; and sometimes they come from countries who do not have the same human rights record and where the request is not as obviously legitimate.

We do not believe the solution to that problem is to enact legislation that would unilaterally strip U.S. authority to investigate serious crimes, but we do think a framework of the type I am talking

about today, under discussion between the U.S. and the U.K., which allows us to pick and choose likeminded countries and circumstances in which we would reduce those conflicts is a path forward.

Mr. CONYERS. Well, I hope we work more closely together in this area, and I thank you for your response to my questions. And I thank the Chair.

Mr. BITKOWER. Thank you.

Mr. GOODLATTE. The Chair recognizes the gentleman from California, Mr. Issa, for 5 minutes.

Mr. ISSA. Thank you, Mr. Chairman, Mr. Bitkower. Is it Bitkower?

Mr. BITKOWER. Yes.

Mr. ISSA. Okay. Sometimes, here from the dais, the best way to deal with a new problem is see if the problem is new or not. So let me ask you a few questions just to see if the problem is new. The country of Ireland decides that, in fact, you committed a crime, and they want you back there. Should they be able to simply unilaterally go to an Irish court, issue a warrant, and come get you?

Mr. BITKOWER. So if the country grounds had an extradition request for me?

Mr. ISSA. No, no. They just want to come haul your ass in.

Mr. BITKOWER. I would oppose that, sir.

Mr. ISSA. Okay. So, in the tangible world, that is an example where we have absolutely no authority whatsoever to take a person—by the way, U.S. or otherwise, from another sovereign country. We have had a long tradition—and I just left the Foreign Affairs Committee—I have got Secretary Kerry there so I apologize I am going back and forth between the two most important people I will see today—so, for all these years we have set up a list of countries in which we do business on extradition.

We want tangible evidence. Let's just say an M-16 used in a crime, but it left the country. Or, an M-16 was found in Ireland being used, but we believe it is from the U.S. When you want that tangible property, you do not go to a U.S. court order alone. You go to a U.S. court to plead your case, and then you go to a foreign jurisdiction, and you negotiate with the foreign jurisdiction whether or not, as to that person, as to that equipment, as to that evidence, they are willing to, through their court system, allow you access or, in fact, removal from their country. Correct?

Mr. BITKOWER. So the question is—Congressman, I do appreciate the question, I think, across a wide variety of contexts. We face a wide variety of situations where we—there may or may not be a conflict of law.

Mr. ISSA. Right, but let's just look at the intangible world, the piece of paper reduced to a PDF. Because that is really what we are talking about. We are talking about something that could be tangible fairly quickly but happens to be in electronic format, correct?

Mr. BITKOWER. Certainly.

Mr. ISSA. Okay, and you want us to assume that somehow, as to U.S. corporations, Microsoft, Apple, whoever it happens to be, that in my opinion the bully—is being bullied by the Justice Department today in some ways. You want us to believe that you should

throw out all the history of extradition, all the history of you do not get it, you get to ask another country for it. And you want to have an absolute right to demand it and get it if a U.S. court says it, and you have jurisdiction over the entity who could control the bringing of it back electronically to you. Is that correct?

Mr. BITKOWER. That is not precisely correct.

Mr. ISSA. It is pretty close though, is it not?

Mr. BITKOWER. Well, respectfully, sir, the U.S. courts do have a long tradition of balancing——

Mr. ISSA. I am not asking what the U.S. court is. I am asking what you are asking for. You are asking for the U.S. courts to summarily order U.S. corporations or any entity that you believe the court has jurisdiction over, to deliver to you something from another country and circumvent that other country's opportunity to tell you yes or no. And that is essentially what you are asking for.

So let me ask it in another way, and I will be asking the next panel. Should we not fashion legislation that treats intangible evidence exactly the same as we treat tangible evidence? That treats the summoning of something from somewhere else to the United States substantially similar to how we would do so if, in fact, it was tangible, like a person, M-16, or a piece of paper? Is that not where—not your position. Your position is rightfully so, self-serving, that you would like the evidence as quickly and easily as possible. But from our standpoint, our Founding Fathers saw 200 years evolve without this sort of an idea that you can order an U.S. entity to bring back something to the United States.

Can you give me a good reason as the time expires—I will give you the rest of the time and as much as the Chairman gives us—can you give me the good reason why I should treat this intangible substantially different than we have treated tangible for 240 years?

Mr. BITKOWER. So thank you, Congressman. We do not believe that our position either in the Microsoft case or with regard to the SCA treats tangible and intangible objects differently. As I said before, there is a long tradition where corporations and banks, for example, subject to U.S. jurisdiction, may be required by lawful process in the United States to retrieve documents from abroad. If after that order is given, the provider can show, or the company can show that there is legitimate competitive laws we work every with companies in that context, in our financial investigations, in trade secret investigations, and so on.

Mr. ISSA. So you go to the court, you get an order, and then with the threat of the order and the financial loss to them you negotiate. Is that right?

Mr. BITKOWER. That is correct.

Mr. ISSA. But only if they file an opposition and they are tying it up in court. Then you negotiate because you want it faster. Is that right?

Mr. BITKOWER. That is not correct. They do not have to file an opposition. They simply have to tell us there is a conflict of laws and we will talk to them right away. I will point out in the Microsoft litigation you are referring to, there has been no claim or allegation by Microsoft of any conflict of law.

Mr. ISSA. Thank you. Thank you, Mr. Chairman.

Mr. GOODLATTE. The Chair recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Well, thank you, Mr. Chairman, and thank you for scheduling this and a series of hearings on this important topic before our country. You know, I will just join with the other Members' concern with the negotiations with Britain with the newspaper instead of from the Department. I just do not think that is the way this should work. And looking at that, I just got to express some concerns.

Yes, Britain is our ally, but they do not have a First Amendment. I mean, they do not protect speech. And they do not have judicial review. I mean, they do not have a magistrate that oversees the issuance of warrants. And they do not have a probable cause standard either. So to think that just because they are our ally, they meet our standards I think is completely mistaken, and I have very grave concerns about what is going on.

Obviously this is not the focus of this hearing, but I will just get that out there. I have very grave concerns. And certainly Britain is moving in a direction away from what we would consider basic liberties that are guaranteed by our Constitution. So their direction in our negotiation I think is cause for grave concern in this country. And I will—we are going to have to get further into that later.

Since you are here, I would like to ask a couple of questions about ECPA reform, because I think what we do with ECPA reform will greatly impact the conflict of laws issues that is the subject of this hearing. We have a bill that has, I think, hundreds of co-sponsors. I am for that bill. But what the bill does not have in it is protection for geolocation. Now, our Supreme Court is moving in the direction of projection geo location, so it may be that our Supreme Court is going to solve that, even though the legislation does not include it, but I am interested in the Department's policy.

Now, it is my understanding that the Department recently enacted a policy requiring a warrant before deploying a cell site simulator, sometimes called a StingRay, to locate a suspect using their cell phone. Does that mean that the Department of Justice is going to require a warrant for all other means of obtaining real time geo location information of a person or mobile device? And if not, what technologies and techniques require a warrant and which do not?

Mr. BITKOWER. Thank you, Congresswoman for raising two different but both very important issues. Initially, with respect to the U.K., I do want to emphasize we are at an early stage in the negotiations. We fully recognize and appreciate that Congress will have to legislate in this area, and we hope to work with this Committee and others in order to establish the appropriate base line standards for the protection of privacy and civil liberties.

And I will also note, as you note, that the U.K. has introduced substantial reforms to its Investigative Powers Act. Any determination with respect to any country, including the U.K., will only be made after there is legislation in place at that time. With respect to geo location, I will note also at the beginning we follow the law, whether it is in the statute or created by court decisions, including the Supreme Court. So we will follow it, obviously no matter what the circumstance is.

There is no single category of geo location data that law enforcement can obtain from third parties. There are various types of data and various types of technology. It depends whether you're looking at prospective information or historical information, information provided voluntarily by an individual, or information collected without their consent. And they vary in terms of precision. So our practices vary depending on the type of information, and the type of technology, and we make the showing that is required under law for any of those.

Ms. LOFGREN. So, let me ask you this. If you are requiring a warrant for—which I must say, apparently the U.S. Marshals Service is not—to deploy StingRay for real time geo location would you require a warrant generally to obtain historical geo location?

Mr. BITKOWER. So, again Congresswoman, it depends on what you mean by geo location information.

Ms. LOFGREN. Where you are.

Mr. BITKOWER. Well, again, that can be determined with different degrees of precision. That could be as precise as are you in this room? It could be more generally, are you in the city? Or are you in this country? When you get more precise, generally speaking the law does require a higher showing, often including a warrant based on probably cause. When you are less precise, often the law requires a lower showing and we will follow that law.

Ms. LOFGREN. Well, in some cases there is a void in terms of the law, in terms of where the court has so far acted. So it sounds like, Mr. Chairman, that as we take this up, we may want to include some geo location protection and precision to guide the Department in the future, and I see my time has expired, and I would yield back.

Mr. GOODLATTE. The Chair thanks the gentlewoman and recognizes the gentleman from Iowa, Mr. King, for 5 minutes.

Mr. KING. Thank you, Mr. Chairman. Thanks for your testimony, Mr. Bitkower. I would like to ask you about the broader picture of this. I mean, we are bouncing this back and forth between the United States and the U.K., and it is far more complex than this as I understand it. And the several hundred countries there are in the world, that would seem to me that that is several hundred different bilateral relationships that need to be negotiated. Could you paint this big picture on what would be the optimum here? I mean, if we had the picture of what's optimum, perhaps then, as we move the pieces around on this jigsaw puzzle, we might be able to get that picture eventually put together, or at least have a target?

Mr. BITKOWER. Sure, and thank you, Congressman. And I will do my best. I think we all start from the recognition that the current situation is untenable, and the optimum would be to move in the right direction, which means both to facilitate legitimate requests from countries to solve crimes and protect public safety, but also to take our companies out of the middle when they are stuck between conflicting legal obligations, both of which they respect.

We do not believe that we will wind up with 181 bilateral agreements. I think that is not even close to being contemplated. There are not that many countries, I think, that share our values in that sense that would be willing to conduct such an agreement with. If it proves successful with the U.K., however, we would be amenable

to exploring it with other countries with whom we have similar close relationships, and who have similar values and have similar rule of law respecting systems.

So I think the approach that we want to take is one that solves the problem that we see, the problem being lack of access because of conflicting laws and our country is caught in the middle. The approach we want to avoid is one that would unilaterally strip U.S. law enforcement of its authority to protect Americans, even in cases where there are no conflicts.

Mr. KING. I would add to that, that by some of the memos here I have in front of me, there is an indication that perhaps just valuable evidence in a criminal investigation might be delayed as long as 10 months. It would seem to me that that would be a big discouragement from the prosecutors in whichever country was waiting for 10 months. How much is that a consideration of your initiative here?

Mr. BITKOWER. That is an everyday consideration, sir, for the most serious crimes we face, ranging from terrorism to child sexual exploitation to computer crime, and I will add the 10 months is an estimate of the time it takes us to respond to requests from foreign countries.

When we are talking about situations where the Department of Justice is required to request information—I am sorry, the 10 months is when we produce information. When we are talking about situations where we are required to request information from foreign countries, 10 months may be a best-case scenario. In many cases we will never see that evidence at all, and in many cases we do not even have a mutual legal assistance treaty, as I said, with about half the countries in the world.

So, if we are required to pursue international cooperation mechanisms to gather evidence, that is going to stop many important investigations dead in their tracks.

Mr. KING. So that would imply that there are many criminals going free because of these delays.

Mr. BITKOWER. There is no question that that is true, sir.

Mr. KING. And also, what about intelligence purposes? Say investigations of radical Islamic terrorists? How much of this proposal is contemplated that would be gathering that kind of intel?

Mr. BITKOWER. So that is a core consideration. So, if, for example, the United Kingdom was investigating a U.K. citizen who had gone off to Syria to fight with ISIL, and was communicating with his co-conspirators through a U.S. provider, and that data was stored in the United States, right now the U.K. would have to come to us for an MLAT, and we would have to go through all those same procedures.

By the same token, when we investigate Syria's terrorism offenses—and I have a couple in my written testimony—quite often terrorists are non-U.S. persons who are located overseas, and that might be exactly the type of data that our providers store overseas. If we have to go through MLAT procedures to obtain that evidence, and if any conflicts of law are automatically resolved against the United States, those investigations will automatically suffer.

Mr. KING. Let me just suggest then that if we are contemplating a degree of change in our foreign policy, that Mr. Issa referenced

foreign policy and foreign affairs—a change in our foreign policy that we were committed to actually defeating ISIS and doing so in a comprehensive way, not only tactically in the Caliphate, but throughout our initiation of a global war against terrorists, and using data as a component of that as well as finances, would you say that this is a critical element that we are addressing here today?

Mr. BITKOWER. When it comes to the fight against terrorism by both us and our allies, access to evidence stored abroad is a key part of that. Absolutely.

Mr. KING. And right now we are handcuffed to a degree?

Mr. BITKOWER. Yes.

Mr. KING. Thank you. I appreciate your testimony, Mr. Bitkower, and I yield back the balance of my time.

Mr. MARINO [presiding]. The Chair now recognizes Mr. Johnson from Georgia.

Mr. JOHNSON. Thank you, Mr. Chairman. Sir, thank you for your testimony today. In what ways, if any, would a bilateral or series of bilateral agreements be preferable to a mutual legal assistance treaty?

Mr. BITKOWER. Thank you, sir, for the question. So let me say from the very beginning, the mutual legal assistance process is a vital part of international cooperation. We rely on it all of the time on a daily basis, and I do not by any means mean to suggest that that is not a key element going forward, but the mutual legal assistance process can be burdensome, because it requires essentially a diplomatic request from one country to another, the need for a country to translate its documents not only in terms of language but also in terms of legal process.

Mr. JOHNSON. Well, that is within the current framework of—yeah.

Mr. BITKOWER. Exactly, exactly. And the idea of a new framework of the type I am talking about today between the U.S. and the U.K. is that it would permit direct requests from the U.K. under U.K. law to providers that are doing business in the U.K. And that would circumvent the need to go through all the procedures in the MLAT process that are not privacy protecting, that do not enhance investigations, but simply add time and delay.

Mr. JOHNSON. A new MLAT process or framework could incorporate the features of the bilateral agreement that is being negotiated with the U.K. Is that not correct?

Mr. BITKOWER. So, in a sense the U.S.-U.K. framework is one of mutual legal assistance, but it is not mutual legal assistance in the type contemplated by our current treaties, which require requests to go through those diplomatic channels.

Mr. JOHNSON. Well, I guess I am getting to the issue of whether or not it is better to try to, for this country, to address its cross-border access to data issues—and other countries that have the same issue—whether or not it is better to negotiate within a treaty format as opposed to a series of bilateral agreements. Why would a bilateral agreement process with at least 190 different Nations in this world—why would that be a superior route as opposed to a treaty?

Mr. BITKOWER. So, I absolutely agree with you. We should continue to work and reform the MLAT system, and there are a number of steps that we are taking in that regard. And we are happy to work with this Committee and others to continue to do so. That is an essential step as well.

Mr. JOHNSON. It seems like that is on the back burner though.

Mr. BITKOWER. Not at all, sir. That is actually on the front burner for the Department of Justice, and it is an area where we put a lot of resources and intend to continue to do so. In fact, we think a framework of the type—a bilateral framework with the U.K. of the type I have discussed would actually contribute to reforming and improving the MLAT process, because it would take certain high volume countries like the U.K. out of that system to a degree and free up resources for uses for all other countries, even those that are not part of the framework. But the reason we would go through a bilateral framework is for certain close allies with particularly—with legal systems that have adequate substantive and procedural protections for privacy and civil liberties, the idea is that this would be an expedited method, that they would not have to go through the normal MLAT procedures for crimes that are of particular concern to them, and do not involve U.S. persons, they have not targeted at U.S. persons or persons located in the United States.

So we would get the best of both worlds in a sense of expediting process that have privacy protecting features and favor our close allies, but also lifting all boats by freeing up resources for people who are not part of that process.

Mr. JOHNSON. So, I presume that you are working under the assumption that British legal standards are acceptable with respect to U.S. legal standards?

Mr. BITKOWER. So, again, we are not working on any assumptions. We recognize the need to and we look forward to working with this Committee and others to establish exactly what those standards ought to be and only then would be evaluate the U.K. as an applicant for such a process.

Mr. JOHNSON. And, last question: would a bilateral agreement with the U.K. waive U.S. Fourth Amendment protections with respect to requests from British for electronic data stored here in the U.S.?

Mr. BITKOWER. So, any agreement obviously would require MLAT legislation and that legislation would have to be consistent with the Fourth Amendment. We certainly recognize that. The Fourth Amendment, of course, takes particular views with regards to investigations by foreign governments as opposed to our own. Or data that does not belong to U.S. persons or persons who are in the United States.

Mr. JOHNSON. Thank you. And would a bilateral agreement be subject to congressional approval?

Mr. BITKOWER. So Congress would have to enact legislation to make this entire process possible, sir.

Mr. JOHNSON. Thank you, and I yield back.

Mr. MARINO. The Chair now recognizes the gentleman from Texas, a former judge, Congressman Poe.

Mr. POE. I thank the Chair. I am over here on the far right. Let me just go back to the basic, what the law is right now. Under current law, information that is stored in the cloud that is over 6 months old, the Department of Justice, on behalf of some law enforcement agency, makes a request or a demand to the provider for that information in the cloud such as an email that belongs to Bubba down in Texas. Is that a fair statement of what the law is right now?

Mr. BITKOWER. Yes, sir. For the content of email, we would generally proceed with a warrant.

Mr. POE. Okay. You would get a warrant from a judge.

Mr. BITKOWER. Yes, sir.

Mr. POE. When is it you do not get a warrant, but you get a subpoena or a request made by some person in the Department of Justice?

Mr. BITKOWER. So we would proceed by subpoena with—under the SCA with respect to certain non-content information, such as metadata, or subscriber information.

Mr. POE. So that is not a law enforcement agency, though. Is that correct?

Mr. BITKOWER. That would be on behalf of law enforcement agencies, sir, yes.

Mr. POE. Oh, a law enforcement agency. So when do you request the subpoena and when do you have to get the warrant?

Mr. BITKOWER. So the Department's practice is to seek a warrant when content of the communications are at issue, sir.

Mr. POE. But to get the data, you issue a subpoena.

Mr. BITKOWER. For certain types of non-content information, that is correct, sir.

Mr. POE. Okay. And, right now, Congress, for the last 4 years, has been discussing and trying to update ECPA to deal with the issue of content and information that is stored in the cloud that is over 6 months old. Is it the Department of Justice's position that a warrant should be required to get that information, whether it is data or whether it is content?

Mr. BITKOWER. So the Department is open to a warrant requirement for that type of data if exceptions for certain limited contingencies involving civil investigators are made.

Mr. POE. Okay. All right. And just so you are clear, I think that the—you ought to have a warrant for all of that. And the reason that the SEC wants to have an exception is exactly the reason that the SEC should have a warrant requirement as well. Its content I think is—or data I think is protected under the Fourth Amendment. That is one of the bills that we are debating here. And regardless of what we eventually come up with, do you think it is important that Congress actually make a decision on reforming ECPA?

Mr. BITKOWER. So again, the Department is certainly open to that change that you are describing, and I would agree with you that any access to data has to comply with the Fourth Amendment. There are ways other than warrants to comply with the Fourth Amendment, and we think those ways might be available to civil investigators.

Mr. POE. And I think it ought to apply to the civil agencies in the Federal Government as well. That is my personal opinion. Do you think that Congress—I am asking your opinion if you are open to it, are you open to it now, or do you think we ought to wait to figure out some deal with the British on what they are doing? Or should we go ahead and make that decision as our responsibility in Congress?

Mr. BITKOWER. So certainly, we do not see one process as dependent on the other. Our concern is when, for example, DOJ civil investigative agencies or civil components, such as the Civil Rights Division, do need to seek information for an important civil rights investigation, and they are not able to get a warrant because it is not a criminal investigation. And in that case there ought to be some mechanism for them to get access to data from the provider, but with full privacy protections, and we are open to a variety of solutions in that regard.

Mr. POE. I did not ask you that. I asked you about dealing with the British. I did not ask you about civil rights. Do you think that we ought to wait to deal—make a treaty with the British on content that is stored in the cloud, and what they think and what we think and come up with some agreement, treaty, whatever it is called, or should we act on behalf of the American public now?

Mr. BITKOWER. We do not think there is any need to wait to act on ECPA, but to resolve the situation with the U.K. either, no.

Mr. POE. All right. Well I agree with you on that. That is Congress' responsibility, and it is long overdue that we deal with storing information in the cloud, and I think the Fourth Amendment ought to apply to the information stored in the cloud, over 4 months or over 6 months old, whether it is civil process or criminal process. And maybe we will get that legislation that is now pending with over 300 sponsors of Congress to the House floor soon. Thank you very much; I will yield back the balance of the time.

Mr. MARINO. Chair now recognizes the congresswoman from the great State of Washington, Congresswoman DelBene, who is a coauthor with me on the LEADS Act.

Ms. DELBENE. Thank you, Mr. Chair, and you thank you, Mr. Bitkower, for being with us today. The DOJ argued in the Microsoft Ireland case that congressional inaction with respect to updating the Electronic Communications Privacy Act is evidence of legislative intent, and that Congress generally think the law is fine, but the courts should feel free to apply it to all of the unique situations that arise given the way technology works today, including international data storage. Now as was mentioned by my colleague from Texas moments ago, are you aware that this Committee has held hearings and announced plans to mark up the Email Privacy Act, and there are over 300 cosponsors on that very basic reform bill waiting for this Committee to take it up, and over 100 on the LEADS Act that addresses the international question?

Mr. BITKOWER. I am aware of those facts, yes.

Ms. DELBENE. So, you have indicated that DOJ's position is that in all cases, the Electronic Communications Privacy Act as written reaches data oversees. So where it is stored does not matter.

Mr. BITKOWER. With respect to the government's ability to compel a provider to disclose information, it does not matter where the provider chooses to store that information, that is correct.

Ms. DELBENE. Now, you know, Congress is looking at a number of ways to update the Electronic Communications Privacy Act to account for the global nature of cloud computing, and the needs of law enforcement to access critical evidence, but some of the threshold questions that we have discussed include the citizenship of the account holder, the location of the data, or the headquarters of the company holding the data. Would you say that the DOJ's position is that ECPA as written already addresses questions about how to handle data stored abroad, and that all these questions are essentially superfluous to—and we should not be asking them?

Mr. BITKOWER. So I think ECPA today currently does not make distinctions that restrict the government's ability to investigate based on the nationality of the account holder, and does not make distinctions about the DOJ's ability to investigate based on where the data is stored. We think that is a wise course to continue with, because there are many investigations where we need to take action where the individual may be abroad and the individual may not be an American. So obviously we are concerned with legislation that would unilaterally strip our authority to investigate in those cases.

Ms. DELBENE. So if we follow the model that says it is based on a company, then—and I think this was mentioned earlier as well—China could make subsidiaries of Chinese companies in the U.S., turn over whatever information it wants, is that a desirable outcome?

Mr. BITKOWER. That is certainly not a desirable outcome, and that is in fact why we are looking for a creative way forward that would address conflicts of laws in targeted ways that lower those conflicts in case we have legitimate requests from companies that respect—countries that respect rights. But we can pick and choose which country to make a deal with.

Ms. DELBENE. So, many of us would agree though that the MLAT system is in need of modernization to function officially in a digital age. Could you share with the Committee how many times an MLAT has been used to obtain data stored overseas versus a warrant stored under the Stored Communications Act?

Mr. BITKOWER. So it is difficult to answer that question, because for the most part, if you are talking about the context of the SCA, the government is not aware where the data is stored. So if a company complies with an SCA warrant, we will not know one way or the other where the company got that data from, Seattle, San Francisco, or Ireland. So I cannot give you an answer to that question. I can only give you answers based on the information we have received from companies when we serve that process on them.

Ms. DELBENE. But can you give us your best estimation of that answer then? Or is that a different——

Mr. BITKOWER. So this may not be a scientific answer, but to our knowledge, in the history of serving SCA warrants on U.S. providers, we have never been told that they cannot comply because of the conflict of law.

Ms. DELBENE. It is my understanding that before the Microsoft Ireland case, standard practice in these circumstances was to use the MLAT process. So if the MLAT process is broken, it is—you know, I would urge the DOJ to start working with Congress on reforms, rather than coming up with new legal theories that apparently you have relied on in the past to get there, and I really would love to get more information on the difference of these numbers, if you can provide those to us.

Mr. BITKOWER. So we would be happy to work with you on that. I guess the one area where I think that it is important to clarify, is that there was no change in DOJ policy for—or in the law. For upwards of three decades, it has been the clear law of the United States that lawful process served under an American company cannot require that company to bring data back from abroad.

We have never heard from an SCA provider to my knowledge that they cannot comply with one of those warrants because of a conflict of law. If we were ever told so in a given situation, we would take that very seriously. We would work with a provider and endeavor to see what that conflict of law is. If there is a true conflict, we would try to see if there are ways around that. That situation has not actually occurred yet, including in the Microsoft Ireland case, whereas I said before, Microsoft has not alleged any conflict of law. In fact, Microsoft submitted a declaration on behalf of itself, and Ireland submitted a declaration on behalf of itself, and neither one have alleged a conflict of law in that situation.

So we take very seriously conflict of laws, we do it across a variety of investigative contexts. Nearly every one of our financial investigations involving banks and the like involve claims with conflicts of laws. We work through those processes. If we do proceed to a compulsion action in court, the court is then empowered to balance important considerations, including comity, including the value to the investigation, including the burden that might be facing the company, and we take all of those very seriously.

Our concern is with legislation that in every single case, if there was a conflict, resolve that conflict against law enforcement and in favor of the foreign country.

Ms. DELBENE. My time has expired. I think we need laws that work the way the world works today, and that is going to be critical for us all to follow up on. Thank you. I yield back.

Mr. MARINO. Thank you. I now my recognize myself for my questioning, and thank you for being here, sir. Assume that I am back down near in my position where the Marino thing is, and the gentleman to my left, Trey Gowdy, former Assistant U.S. Attorney. The gentleman to my right, the former judge from Texas, Judge Poe and myself. And I am going to include you in this because you would not be where you are at if you were not. There is no one in this room that is more law enforcement than the four of us in our careers, and I thank you for your service to this country in law enforcement and prosecution. I read your statement, thoroughly, and I agree with you.

Your first issue, cross border access. We all know how incredibly important that is. Your second issue, current rules governing access to data in other countries. Again, another complicated issue that we must deal with, and your third issue of the possible legisla-

tion. While it is not possible legislation from my perspective, it is going to be legislation from my perspective. We are talking about dealing with 2016 issues based on a 1986 law, ECPA, which we are talking about data collection when we did not even—when that law was implemented, we barely had these. We did not have this, we had such a model that my mother still likes to use, just the flip one with the big buttons.

So let me ask you this, if you would please? You talked about treaties, and of course the SCA. Would legislation not make life simpler if we got a consensus on the legislation, instead of having 194 different agreements with countries or referring to a law that is, what, 30 years old?

Mr. BITKOWER. So certainly, sir, we would not contemplate 194 different agreements. We think this agreement would be available to a very small set of countries, at least at the beginning.

Mr. MARINO. Okay. At least in the beginning. But okay, you start out with two countries, and then you go to six, and then you go to 16, and then you go to 60. These countries are not going anywhere, and the electronic age is going to continue to explode. So why not have definitive legislation? Do you think that justice should be legislating or interpreting a 1986 law, instead of a 2016 Congress legislating what is important to law enforcement, without tying the hands of law enforcement, but also with having a law—a rule of law that we can agree on with other countries once we get established here in the legislature.

Mr. BITKOWER. So I fully agree with you that there is an important role for legislative change here and legislative change would absolutely be necessary to enable us to take down these conflicts of laws in carefully targeted ways. The way we anticipate it working is that Congress would act by establishing the parameters for an agreement, and then we would be able to fit particular countries in that agreement if they qualify.

Mr. MARINO. I do not get that from reading DOJ information. I am getting that DOJ does not like the LEADS act.

Mr. BITKOWER. Well so, to be clear sir, even under the context of a bilateral agreement of the type we are discussing in the United Kingdom, that sort of agreement presupposes both the United States and for the United Kingdom the ability to compel the production of data that might be stored abroad.

Mr. MARINO. My point exactly then. Would legislation not simplify that matter? And when you have a direct source of law that we could point to when we need to. Let me pose a scenario to you. Assume there is a company with a presence in Brazil. One of our companies, a presence in Brazil. And the Brazilian Government wants some of that information, they issue a warrant, but that warrant would violate U.S. law. What do we do?

Mr. BITKOWER. That is a serious situation of course. That is one we face in real life. That is not a hypothetical situation.

Mr. MARINO. Okay. But would legislation not then address that issue? Good concise legislation working closely with justice and the private sector from a law enforcement perspective. Would that not be the approach to take?

Mr. BITKOWER. Yes. I do not want to speak to any particular country obviously, because there is a wide variety of——

Mr. MARINO. Neither do I. That is why I keep going back to legislation. And it is Congress' role to legislate. And looking back at a 30-year law based on where we are today, I do not think is logical. So at no time I do not think, at least I do not know that Justice even called my office, called Ms. DelBene's office, called the Chairman to discuss LEADS. We would like to do that; we want input from Justice on these issues.

So again, I thank you for your service, but the point I want to get across is Congress legislates, and I yield back my time. The Chair now recognizes Congressman Jeffries from New York.

Mr. JEFFRIES. I thank the Chair for yielding, and for your leadership in putting forth the LEADS Act and on this very important issue. And I thank you for your testimony here today. The law is currently silent as to whether the DOJ can compel a U.S. company to produce the email content of a non-U.S. citizen when the server is in another country. Is that correct?

Mr. BITKOWER. So, we would not agree with that, sir.

Mr. JEFFRIES. Okay. But the Stored Communication Act is silent on this issue, correct?

Mr. BITKOWER. So, we would agree that the Stored Communication Act does not address that through tax, that is correct.

Mr. JEFFRIES. Okay. And in light of this silence, the Department of Justice has chosen to take the broadest possible interpretation as to what its authority can be. Is that right?

Mr. BITKOWER. Well respectfully sir, there are court decisions on the matter, and we are following those decisions.

Mr. JEFFRIES. Okay. Now do you agree that Congress, in light of the silence that you have acknowledged at least as it relates to the Stored Communications Act, should step into the void to clarify the situation for all parties involved?

Mr. BITKOWER. So again sir, we think Congress did act, and Congress legislated against a backdrop of which the government could compel the production of documents from abroad. So we think that already occurred. Obviously we will see how the courts come out on these issues, and it may be the case that for the legislation might be helpful.

Mr. JEFFRIES. So at the end of the day, in the absence of congressional action, at least as it relates to the specific circumstance that I laid out, is it fair to say that we could put a United States company in the position of providing email content located internationally as it relates to a non-U.S. citizen in violation of another country's laws. Is that a possibility, sir?

Mr. BITKOWER. That is a possibility.

Mr. JEFFRIES. Okay. Now in the 21st century we live in a global economy. Is that right?

Mr. BITKOWER. Yes, sir.

Mr. JEFFRIES. Okay. And compelling United States companies to violate, potentially as you have acknowledged, United States law by disclosing email content of non-U.S. citizens could possibly place United States businesses at a competitive disadvantage. Is that correct?

Mr. BITKOWER. Sir, the way I would answer that question is to say, again, for many decades ,we have engaged in the enforcement of our laws, and that often results in us trying to compel records

from companies which store those records abroad. This is not a new issue, it is not unique to the SCA. It is not unique to the United States. In fact most countries, or many countries at least, have similar provisions in their law that authorize them to seek evidence that may be stored abroad.

Mr. JEFFRIES. There is at least a possibility that by compelling a United States company to violate international law, as you have acknowledged, is potentially the case here, that that could place a United States company as a competitive disadvantage. Yes or no?

Mr. BITKOWER. So to be clear, I did not say to violate international law, I said it is possibly the conflict with the law of another country.

Mr. JEFFRIES. The law of another country.

Mr. BITKOWER. Yes.

Mr. JEFFRIES. Correct.

Mr. BITKOWER. So that is correct. It could absolutely put companies in a situation conflict to legal obligations.

Mr. JEFFRIES. Okay. Now, and that could in my view I think in the view of many reasonable people place them at a competitive disadvantage, which I think could undermine the United States' national interest economically. And in fact I would just point out that Article I, Section 8, Clause 3 of the United States Constitution states that Congress shall have the power to regulate commerce with foreign Nations. Are you familiar with that clause?

Mr. BITKOWER. Yes, sir.

Mr. JEFFRIES. Now I think that the Founding Fathers in their great brilliance understood that Congress should be the entity to decide how to properly balance United States' interests across the legal, economic, constitutional spectrum. True?

Mr. BITKOWER. Congress certainly has that authority, sir.

Mr. JEFFRIES. So is it not correct that Congress should act in this specific circumstance where you have acknowledged at least that there is silence? Some ambiguity in order to clarify this very complex situation.

Mr. BITKOWER. So, again sir, I do not think there is ambiguity in terms of how the statute works today. Certainly we do welcome the opportunity to work with Congress in addressing the very conflicts of laws you were talking about. Our concern is simply if we address them in a way that unilaterally strips U.S. law enforcement authority and does not address the situation of foreign law enforcement authority, that is not the approach we are seeking, but we do think there is definitely options that Congress can work on here.

Mr. JEFFRIES. Okay. Lastly I would point out, and I think my colleague Darrell Issa began this line of inquiry, I think it was very important, the U.S. has a history of respecting the sovereignty of other Nations when conducting criminal investigations in the context of extradition treaties. Correct?

Mr. BITKOWER. Yes, sir.

Mr. JEFFRIES. And we have got extradition treaties with about 120 Nations. True?

Mr. BITKOWER. I do not know the exact number.

Mr. JEFFRIES. Including Mexico, correct?

Mr. BITKOWER. That is certainly true.

Mr. JEFFRIES. Are you familiar with El Chapo?

Mr. BITKOWER. I am, sir.

Mr. JEFFRIES. He is an international drug dealer. Correct?

Mr. BITKOWER. Yes, sir.

Mr. JEFFRIES. Seven United States jurisdictions have currently criminal charges pending against him, including murder. True?

Mr. BITKOWER. Yes, sir.

Mr. JEFFRIES. Would you conceive of a circumstance where the United States, in violation of its treaty with Mexico, would go across the border, snatch El Chapo, and bring him back to justice, notwithstanding the serious United States interest? Would you conceive of that circumstance?

Mr. BITKOWER. No, sir, I could not.

Mr. JEFFRIES. Okay. And if we would not do it in such a serious situation, for the life of me, respectfully, I cannot figure out why Congress should not step into this vacuum that exists as it relates to email content and respecting the principles of comity and the competitive disadvantage that will replace the United States companies and which would undermine our national economic interests. I yield back.

Mr. MARINO. Thank you. The Chair now recognizes the congressman from Georgia, Mr. Collins.

Mr. COLLINS. Thank you, Mr. Chairman. I think at this point I am just going to have a few questions. But I do not agree with the Chairman. I mean, from my background, I think this has become the new discussion over the years, as, you know, yes, there are many Members who are prosecutors on those, judges on this. I take it from a little different perspective.

I am the son of a State Trooper from Georgia. As I have jokingly said, I have fought the law on many occasions, and I lost most of the time, but the issue here is not an issue of law enforcement. This is an issue of where are we at in 21st century privacy, where are we at in a 21st century and digital environment, and why do we continue many times to continue to hold to issues that really need to be updated? I would agree with my friend from Texas, the judge, and I would agree with my friend from New York and also Washington. The LEADS Act, although it seems to be in some of the questions and some here tends to denigrate this LEADS Act, I think that something needs to be done and something that we need to put our companies and the world on notice on how we are going to do this.

ECPA also was another issue which is again baffling to me. And I know it has been said that well 300 Members could be wrong. Well yeah, I agree, this is Congress, but I think 300 Members also have a pretty good idea that something is not right too. And to continue to hold this out is a frustration, but especially from DOJ's position.

And in the Second Circuit Court of Appeals, I think it is the Microsoft case, as we work on this, the DOJ lawyer argued in the case that it does not—that ECPA does not apply to disclosure of information abroad. Even if the information to be disclosed is private email correspondence of a U.S. citizen.

In other words, the Department argued that U.S. citizens' emails have no privacy protection under ECPA outside the U.S. They were

pressed on this issue by the court, and the court—the DOJ attorney said the result should be of some concern to U.S. technology users, but suggests this is the norm, was his words. Or their words. I am concerned about the Department's position. I reject this notion that this is the new norm, and in fact, I think Congress is speaking in to say Congress the silence on this is not accurate in this environment. But I just want a clarification.

Do you agree that ECPA does not provide or protect email communications even if sent and received within the U.S. from disclosures abroad?

Mr. BITKOWER. Thank you, Congressman. So I think it is important to distinguish between two different provisions of ECPA. The provisions at issue in the Microsoft case generally are the provisions in 2703, which relate to the United States government's authority to compel a provider that is already subject to our jurisdiction to compel records that are in its custody or control. The provisions I think you are talking about now are the ones contained in 2702, which prevent a provider from disclosing content except in certain limited circumstances.

Mr. COLLINS. Well, let's go there, because there is a concern there, because what it seems to be, and again, you—it is your time to clarify. It seems that what the Department of Justice is not seeing is that they are trading private emails of technology users as a business record of a service provider. That is a leap.

Mr. BITKOWER. So, certainly, sir, that is not the standard that we are applying. The standard we are applying when it relates to our ability to compel——

Mr. COLLINS. But you have taken that position in litigation.

Mr. BITKOWER. No, that is not precisely correct, sir.

Mr. COLLINS. Okay. Elaborate.

Mr. BITKOWER. I would be happy to clarify, sir. So, the precedent we have taken is that a long line of cases stretching back over 30 years allows us to compel companies that are subject to our jurisdiction to produce responsive materials pursuant to lawful process, even if they may be stored abroad. Now if that production produces a conflict of laws, there is further work to be done. There is further work to be done both by us in discussing it with the company and by the courts if applicable.

The question I think that you are raising now about whether a company is free to disclose information is a slightly separate question. And that is if a company, American or otherwise, stores data abroad, then the protections of 2702 may not apply. That is, that company, irrespective of what DOJ does one way or the other, may be free to disclose that information to a foreign government or to any other person. The provisions of ECPA have simply been interpreted not to apply as it regards to 2702, which protects the information.

Mr. COLLINS. I think at this point in time, in the effort to defend the what if, I think DOJ has had some contorted positions in this. And I think understandably you have a job to do, you feel this is the best way to do your job. I think this panel, if you have heard today, has some very different opinions on how that actually is playing out in the real world, dealing not only with businesses and the cross country data flows and other issues, but also just the

issues of privacy and the issues of when this is. And again, when you get that to a point of, you know, whether the company can disclose or not, and it being a business record of a company which has nothing, there is some concern there.

So we are going to continue this hearing, I appreciate your service, but the LEADS Act and ECPA need to move forward, and this needs to be—have a debate. It is not up to an executive agency to determine law or intent. It is up to this Congress to do so. We are doing that, and I think that is where it needs to go. And with that Mr. Chairman, I yield back.

Mr. MARINO. Chair recognizes Congresswoman Jackson Lee from Texas.

Ms. JACKSON LEE. Thank you very much. I was very pleased to listen to a sizeable part of the exchange, and Mr. Bitkower, I thank you for your service representing this Nation and the Department of Justice. But as I listen to the series of back and forth, I think one of the things that I want to restate for the record is the large gap of response by Congress, in particular the passage of the Electronic Communication Privacy Act in 1986.

I guess I am in awe, and I might use the term appalled, that there is that large, enormous gap that has lasted on a number of issues. Then a state for the record that the SCA was not designed for international application, and ECPA does not permit providers to disclose information directly to a foreign law enforcement agency, even when the agency is investigating one of its own citizens. I think we had as an example what a police officer would do, 20 years ago in the United Kingdom, what they might need to do now, which is to ask for the information.

I also want to put into the record the dilemma that Microsoft faced. Their case is now pending. They answered part of it, Microsoft produced a non-content information. But they made the argument I think legitimately when the other material was stored in Dublin, Ireland. And so we find ourselves in a dilemma that must be answered. And what I would like to see is that we answer it with DOJ, even as we move legislation forward.

And so I am going to ask process questions, and what you are seeing in the day-to-day operations of the Department of Justice. So I will just ask the question. One, is it obvious that you are seeing a massive increase of requests for data internationally?

Mr. BITKOWER. Thank you, Congresswoman. We are seeing a massive increase of requests for——

Ms. JACKSON LEE. Well if massive takes you back, you are seeing an increase in requests coming in.

Mr. BITKOWER. I would say massive, Congresswoman.

Ms. JACKSON LEE. All right. I had the right——

Mr. BITKOWER. We have seen a massive increase in this, particularly for digital evidence.

Ms. JACKSON LEE. And as I see, part of the process in particular, some of the processes under the DOJ requires a request to come into the international office, and then it gets spread out to U.S. attorneys across the Nation. Already I am overwhelmed by just the process of it having to leave you, headquarters, and reach to places beyond and find offices of varying sizes that have to respond.

So let me just get a more detailed response from you. Do foreign law enforcement officers ever attempt to obtain data through faster, informal channels? Do they call their colleagues in the FBI or the NSA for a faster result?

Mr. BITKOWER. So there are a range of methods of international cooperation. Each one of them must obviously follow the law, but certainly there are occasions where we can share information on a more informal basis. If consistent with the law, of course.

Ms. JACKSON LEE. The question implied that maybe there was the normal collegiate responses, and so you cannot attest here today that that does not happen. I hear what you are saying, in compliance with the law, but——

Mr. BITKOWER. That is correct.

Ms. JACKSON LEE [continuing]. Because the law is so—I would say it does not answer the questions, it could be possible that relationships and people's interpretation of the law, information could just be given or access could be given.

Mr. BITKOWER. Well again, certainly Congresswoman, information relating to law enforcement threats is shared every day by police forces around the world. When it comes to compelling data from a provider, then there needs to be a legal process, and that legal process has to be obtained either under the law of the United States pursuant to if it is content a probable cause standard, or if under the law of a foreign jurisdiction. What we are trying to do here is eliminate some of the obstacles and burdens that are created when one country has to go through the processes of another country in order to get that information.

Ms. JACKSON LEE. And particularly when it involves the providers. Let me ask, one of the chief concerns underlying this discussion is the move toward data localization laws in other countries. And so, would you explain why the current environment has motivated some countries to try to balkanize the internet in this way, with respect to the data localization?

Mr. BITKOWER. Yes, thank you very much. So one of the concerns we have seen with regard to the new world of cloud computing and international data storage is that countries make requests that may be legitimate under their own laws for data that happens to be stored in another country, perhaps in the United States. If they cannot get those requests fulfilled in an efficient manner under their own law, then there is an incentive for them to mandate that that data be stored in their own country, so they do not have to go through these cumbersome processes, whether it is with U.S. or another country.

So one of the goals of the framework we are discussing today is to try to eliminate those incentives, but in a very carefully targeted way that protects privacy and civil liberties, and only for countries with an established rule of law system.

Ms. JACKSON LEE. Would you say that legitimate major companies, many of them creating genius through intellectual property, created here in the United States, become the tennis ball, the batting ball, and they become batted from one place to another? I hesitate to say that they are victims, but in essence, are they batted from one place to the next under the present structure that we now have?

Mr. GOODLATTE. The time of the gentlewoman has expired, but the witness will be permitted to answer the question.

Mr. BITKOWER. Thank you. So yes, in particular, the requests by foreign countries for data stored within the United States, that is correct.

Ms. JACKSON LEE. And so we need a fix.

Mr. GOODLATTE. The gentlewoman's time has expired.

Ms. JACKSON LEE. I yield back, thank you, Mr. Chairman.

Mr. GOODLATTE. The Chair recognizes the gentleman from Colorado, Mr. Buck, for 5 minutes.

Mr. BUCK. Thank you, Mr. Chairman. Mr. Bitkower, I assume that as a United States citizen, you would agree with me that I am afforded certain protections by our Constitution and laws.

Mr. BITKOWER. That is correct, sir.

Mr. BUCK. And that an individual in Ireland would be also afforded certain protections by their laws?

Mr. BITKOWER. Yes sir.

Mr. BUCK. And we have a treaty between the United States and the United Kingdom that recognizes those protections, and both countries agreed to.

Mr. BITKOWER. Both the United Kingdom and with Ireland, yes sir. Separate treaties.

Mr. BUCK. Excuse me. And when the Department of Justice goes around that treaty, you have made a decision that—and I assume it is fair to say that you went around the treaty by getting information in the Microsoft case outside of the processes created by that treaty.

Mr. BITKOWER. So I would actually disagree with that, sir. The treaty between the United States and Ireland, first of all—let me back up. At the time the request was made in the Microsoft case, the Department of Justice had no knowledge that the data was stored in Ireland. Typically we would not be aware of that information unless we were told by the provider after it happens.

Mr. BUCK. Did you withdraw your request when you learned that the information was stored in Ireland?

Mr. BITKOWER. So that brings me to the second point, sir, which is that many mutual legal systems treaties do not require that they are the exclusive mechanism for getting data from one country to another. They are one option.

Mr. BUCK. Well, is there a just kidding clause in that treaty? Is there something in the treaty that says, "Well you do not really have to follow the treaty? You can do anything you want, this is just one way of getting information."

Mr. BITKOWER. Well, so in essence, sir, the treaty does state as one way of getting information necessary. It is not the only way of getting information.

Mr. BUCK. And so, does the Department of Justice recognize the situation you have put American corporations in across the world when you go around treaties and use a completely separate process? Why would any country want to do business with an American corporation if America has access to that information all across the world?

Mr. BITKOWER. So again sir, I have to emphasize that we do not go around treaties if those treaties do not require that they have the present mechanism.

Mr. BUCK. You said you used a different process to get information.

Mr. BITKOWER. That is correct. That is correct.

Mr. BUCK. Now that is not going around the treaty?

Mr. BITKOWER. It is not, sir. The treaty does not require that it be the exclusive mechanism for the transfer of data.

Mr. BUCK. So answer my question. Do you recognize the situation you have put American corporations in across the world?

Mr. BITKOWER. So if our actions did create a true conflict of laws, we would recognize that as a serious problem, yes sir.

Mr. BUCK. I did not ask about conflict of law. We are trying to do business with other countries. And if the Department of Justice has a way of going around a treaty and getting information from an American corporation for an Irish citizen on an Irish server, why would any country want to do business or any citizens of any country want to do business with American corporations?

Mr. BITKOWER. So again sir, I need to specify. The discussion in terms of the Microsoft case did not necessarily involve an Irish citizen or a person in Ireland. It is data that happens to be stored in Ireland. It could belong to—as far as the record is clear, a citizen of any country, including an American citizen. That is said, the only fact we know about it from the record of that case is that the company has chosen to store that information in Ireland.

If, for example, it belongs to an American citizen, or a citizen committing a crime who is located in America, I think we would all agree that the United States has legitimate interest in obtaining that information as expeditiously as possible so long as it follows——

Mr. BUCK. Are you going to answer my question? Why would an American company—why would anybody want to do business with an American company overseas if the United States has access to any information it so chooses by going around a treaty?

Mr. BITKOWER. So again, sir, if there is a conflict of laws, we would take that seriously. And if that is brought to our attention, we absolutely will do everything we can to avoid a——

Mr. BUCK. I am not talking about the laws, though. I am talking about the competitive disadvantage you are placing American companies in.

Mr. BITKOWER. So my understanding is of what we have heard from companies is certainly the competitive disadvantage, if any, comes from the fact that they are placed in conflicting legal obligations. That is one country tells them to do one thing, another tells them to do another. If that comes to our attention, we take it seriously, and American law already also takes that seriously.

The situation we are talking about now is, however, where data may be stored in a country with no connection to that country other than the fact that it is chosen to be stored there. It could be the information of vital importance to the United States, and information with very little connection to Ireland. And in that case, we just need to have a mechanism to make sure we can get that data to the United States to protect American citizens.

If it turns out there is a conflict of law at any point, if that is brought to our attention by the company or by the country itself, then obviously we would have further work to do and further discussions to be had. I want to clarify, that has not happened in the Microsoft case.

Mr. BUCK. If Microsoft is put in a position where—or any American company—and frankly what is most bothersome to me is Microsoft has the resources to battle with the Department of Justice. A startup company, a company with 10, 12 employees in a similar situation would just cave. The coercive effect of the government would be placed on a company like that, and they could not—they do not have the resources to fight the Department of Justice. But in this situation, a foreign citizen would not want to do business with a U.S. company if that U.S. company is forced by the U.S. Government to turn over information that is located in that foreign country. And I am concerned about that.

Mr. BITKOWER. So again sir, that is the very purpose of the U.S.-U.K. framework that we are trying to explore now, is to find the ways of eliminating those conflicts of laws, prevent any competitive disadvantage to our companies, but do it in a careful way that allows the different investigations to take place, both on our behalf and on behalf of foreign governments in a way that it respects privacy.

Mr. BUCK. I yield back, thank you, Mr. Chairman.

Mr. GOODLATTE. The gentlewoman from California, Ms. Chu, is recognized for 5 minutes.

Ms. CHU. Mr. Bitkower, the process to exchange data under the MLAT process has been criticized as being slow and cumbersome, with requests taking average 10 months to fulfill. You argue that the MLAT is also unreliable, given that our country does not have MLATs with about half of the countries in the world. And some countries exclude certain categories, or do not cooperate at all. Is this occurring because they believe the MLAT process is too slow, or do they not believe in this process at all?

Mr. BITKOWER. So again, the MLAT process faces a variety of challenges. You have identified some of them. That is, even if we have a fully functioning MLAT relationship with another country, it will take many months at best to get that information. And as you point out, we may never get it at all, and that is even when we have a treaty, and as you point out again, for about half the world, we do not even have such a treaty, so in those cases, the requirement to rely exclusively on MLAT channels would end investigations.

Ms. CHU. Well, you have referred to the proposed deal between the U.S. and the U.K., and providers under this deal could disclose data directly to the U.K. for serious criminal and national security investigations when the U.K. obtains authorization to access the data under its own legal system. While the courts may have provisions to protect individuals' privacy rights, other countries may not. If we use the U.K. agreement as a model, what steps will the Department of Justice take to ensure that there are sufficient protections for privacy and civil liberties moving forward?

Mr. BITKOWER. Thank you Congresswoman. So that is an area where we would hope to work very closely with Congress in setting

up exactly what those adequate baselines are for protecting privacy and for protecting civil liberties, and we want to make sure that any country we choose to negotiate an agreement with fits into that category based on its own legal framework. It does not require that it exactly mirror the American framework certainly, and if it did require it, then no country would quality, but it does require that the country have those adequate protections.

Ms. CHU. And what kind of enforcement mechanisms could you put in place to ensure that that they would comply with, with privacy terms as well as other terms of the bilateral agreement?

Mr. BITKOWER. So again, we are obviously at the early stages of discussing what these agreements would look like and what the legislation would look like. We would certainly anticipate that there would have to be a mechanism to provide oversight of the agreement to make sure that it is being applied correctly.

Ms. CHU. And if the bilateral agreement approach is taken by the U.S., how do we determine whether or not a country is an appropriate partner? For example, how many of the witnesses have discussed about a country's policy on human rights. How do we evaluate that consideration and whether the country meets that requirement?

Mr. BITKOWER. So that would be a topic for close and ongoing conversation, I think, between us and Congress certainly. There are a number of factors we would look at. We would look at the system as a whole certainly, but with particular regard to its surveillance laws. We would want to make sure that there is a rule of law framework in place and appropriate procedural and substantive protections for privacy and civil liberties.

And these are areas of course, it is easier in cases like the U.K. where it is a longtime ally with a long democratic tradition with whom we have actually had a very long MLAT relationship as well. So we have a certain knowledge and visibility about how their system works, and I think that would be helpful in the process.

Ms. CHU. And with a country that is not as clear as the U.K., what would you do?

Mr. BITKOWER. So a country that is not as clear as the U.K. might not qualify at the end of the day, and that is just a fact. So we would have to make sure that the country, whatever its laws are, that we get good visibility into what those laws are. Not just what the laws are on the books, but how they are applied in practice, and to make sure there are those appropriate protections in place before we would consider such an agreement.

Ms. CHU. Okay. Thank you. I yield back.

Mr. GOODLATTE. The Chair recognizes the gentleman from Rhode Island, Mr. Cicilline, for 5 minutes.

Mr. CICILLINE. Thank you Mr. Chairman. Thank you, Mr. Bitkower. I want to just pick up on something you just said. You said in your testimony that the MLAT is not the only way of getting information. It is not the exclusive way. I just want to challenge you on that for a moment. It is in fact the agreement by which we set out a procedure for the sharing of information. That is the purpose of the treaty.

Mr. BITKOWER. So all MLATs are different, and some of them have different provisions, but MLATs are generally one method of

exchanging information. They are not typically the exclusive mechanism.

Mr. CICILLINE. But I mean, is not the purpose of the treaty so that both parties to a treaty have an understanding about a process that will be followed for a particular activity? And that is the whole purpose of it, otherwise what would be the purpose of having an MLAT if it were not in fact the expectation of both parties that this process be followed in the sharing of information?

Mr. BITKOWER. Well, so again, sir, every treaty is different. Typically the treaties make sure that a process is available to be followed in the case of a need in the requesting country.

Mr. CICILLINE. And with respect to the negotiations with the United Kingdom, what is the exact status of that negotiation, and what action will be required by Congress according to you, if any, if that agreement is successfully concluded?

Mr. BITKOWER. So, thank you, sir. The negotiations began, I think as you know, fairly recently, where we received formal authority to begin those negotiations within the last month or so. We have been hard at work in seeing what an agreement would look like, but we absolutely recognize that action by Congress would be necessary to make this project feasible in the first instance, both to lower in a targeted fashion the legislative bars that are present in our own law, and also to set up the framework to determine which countries would be eligible to join such an agreement.

Mr. CICILLINE. And so, to use this example again of British law. As you know, British law is not always compatible with U.S. law, particularly in the areas of due process and probable cause determinations. And if you think about the requirements we have in this country in terms of judicial review, a concept which is not omnipresent in the British system, how do you square some of those standards and practices? And that is a country that I think most people would agree might have more compatibility than many other countries. How do you make those determinations so that we can be certain those very deeply held values are reflected in this process?

Mr. BITKOWER. So I think that is the key question, and it is one that we will be grappling as we go forward. I think it is important on the one hand that we do not require that the other countries' legal processes exactly mirror our own, or else no country would ever qualify of course. We have some of the highest privacy protections in the world, and we are proud of those, and justifiably so, and we want to make sure that other countries have substantial protections and legitimate protections, but we cannot demand that they have the exact same legal standards for every sort of process along the way. Some of them have lower standards in one area and higher standards in another, and they have their own checks and balances within their own system.

So the U.K. is a country with which we have a great familiarity. As I said before, a very long democratic tradition, a tradition of rule of law. We are comfortable with understanding how their system works. As I mentioned earlier, they have also introduced a new investigative powers bill which would introduce further reforms. So we will have to keep looking at that as it goes forward. We will make any evaluation at the time when the legislation is prepared.

Mr. CICILLINE. But Mr. Bitkower, I think it is very clear that most of us on the Committee recognize that there is an important role for Congress to play in this. And if you have already answered this, I apologize, but it seems particularly disturbing that in light of the complicated nature of this and the important role of Congress should be playing that many of us learned about this from reading it in a news account. And I am just wondering, what was the reason that you would not have engaged Congress more as you developed or thought about the development of framework, so that we might have some alignment of what ultimately Congress might intend to do in this area?

Mr. BITKOWER. So again sir, I want to make clear that we only very recently began negotiations with the U.K., and only very recently, in fact, we received permission to do so through the intergovernmental process. So we tried to notify this Committee as soon as we possible could once those negotiations started. It was approximately the same exact week, I believe, that the Washington Post article came out.

We have tried to make ourselves available to brief this Committee and others. We expect to continue to do so, and there is no question that we fully respect the essential role that Congress has to play in these agreements.

Mr. CICILLINE. Thank you. I yield back.

Mr. GOODLATTE. The Chair thanks the gentleman. The gentleman from California, Mr. Peters, is recognized for 5 minutes.

Mr. PETERS. Thank you, Mr. Chairman. I want to thank you, sir, for your patience and for hanging in there. I think you have answered the questions very clearly. As I understand it, you are following the law as was passed in 1986 and interpreted by the courts. I am not sure what else we would ask you to do. You have been admonished or exhorted by a number of Members of Congress, that Congress should act.

I am not sure what you are supposed to do about that either. These are all Members of Congress, maybe they are responsible for amending the laws if we see a need to do so, but I appreciate how you have illuminated the issues. But it was a little bit Alice in Wonderland-y to hear them lecturing you about why Congress should take some action, because they are Congress Members.

But I would say your testimony spells out pretty long detail of some concerns about the LEADS Act. I apologize, I do not have the testimony that you refer—cross reference about the ECPA amendments that are proposed, but maybe you could just take a few minutes to sort of outline what your main issues are. And then I would like to know kind of how you think it would be most constructive given the discussion we have had about the negotiations with Britain, that this Committee might engage you in talking through some of those issues so that we could actually update the law to reflect not both privacy concerns—both privacy concerns as they are 30 years on, but also security concerns.

Mr. BITKOWER. So thank you, Congressman. I will begin with the ECPA related proposals, and I am concerning to make sure you get a copy of the testimony we submitted in connection with that hearing. But as we have said in that testimony and elsewhere, the Department absolutely recognizes that some of the provisions of

ECPA have not kept pace with the way technology is used today, and the way people think of their emails.

And we are certainly open to a change that would require a warrant when criminal law enforcement authorities seek to compel the content of emails, whether they are older than 180 degrees, newer than 180 degrees, whether they have been opened, whether they have not been opened. We are certainly open to that change. We do have a concern that any change in law create an accommodation for certain very limited civil investigative functions where a warrant is simply not available, because they are not criminal investigators.

Mr. PETERS. That would be something of the SEC for instance.

Mr. BITKOWER. The SEC, I am talking about important civil rights investigations, anti-trust investigations. Things that affect important rights for Americans every day. We have a number of other concerns with the Email Privacy Act, which we are happy to provide further information on, but we do have some concerns.

For example, in the area where it permits us to obtain records from a corporation, where a corporation provides email to its employees, there needs to be a mechanism and a functional mechanism where you can get those emails. Traditionally we do those investigations by subpoena, because traditionally the employees do not have privacy rights in those emails, and we want to make sure that provision works well. And there were a couple of other areas where the bill gives us some concerns. But we are happy to work with this Committee and others in making those understood.

Mr. PETERS. Have you been in conversation with Committee staff about these issues?

Mr. BITKOWER. We certainly have, sir.

Mr. PETERS. Okay. Well I appreciate that. And I thank you again for your time. I am looking forward to the second panel. And I yield back.

Mr. BITKOWER. Thank you.

Mr. GOODLATTE. I thank the gentleman. Mr. Bitkower, we very much appreciate your testimony here this morning, and we can excuse you at this time, and we will go to our second panel.

Mr. BITKOWER. Thank you very much.

Mr. GOODLATTE. We now welcome our second panel of distinguished witnesses today, and if you would all please rise up, I will begin by swearing you in. Please raise your right hand. Do you and each of you swear that the testimony that you are about to give shall be the truth, the whole truth and nothing but the truth, so help you God? Thank you very much.

Let us let the record reflect that all of the witnesses have responded in the affirmative. And we will begin our introductions by recognizing the gentlewoman from Washington for the purpose of introducing Mr. Smith.

Ms. DELBENE. Thank you Mr. Chair. It is my pleasure to welcome Brad Smith as a witness today. Brad serves as the president and chief legal officer at Microsoft, and had joined Microsoft in 1993 and became general counsel in 2002 and then was made president and chief legal officer just last summer. He is responsible for the company's corporate external and legal affairs, and he is a graduate of Princeton University and the Columbia University

School of Law. And it is great to have someone here from Washington State and we just want to welcome you and thank you for being here. I yield back.

Mr. GOODLATTE. Welcome. Our next witness is the Honorable Michael Chertoff. He is the executive chairman and co-founder of the Chertoff Group. From 2005 to 2009, Mr. Chertoff served as Secretary of the Department of Homeland Security. Federal judge of the U.S. Court of Appeals for the Third Circuit and Assistant Attorney General of the Department of Justice, Criminal Division. Mr. Chertoff is a graduate of Harvard College and Harvard Law School.

Our next witness, the Honorable David Kris, began his career with the U.S. Department of Justice serving as an attorney in the criminal division and then as Associate Deputy Attorney General. He went on to be deputy general counsel and chief ethics and compliance officer at Time Warner, Incorporated, as well as an adjunct professor of law at Georgetown University and a non-resident senior fellow at the Brookings Institution. Mr. Kris currently teaches national security law at the University of Washington Law School, and he is a graduate of Haverford College and Harvard Law School. Harvard Law School is well represented here.

Our final witness is Ms. Jennifer Daskal. Ms. Daskal is an associate professor of law at American University, Washington College of Law where she teaches and writes in the fields of criminal law, national security law and constitutional law. From 2009 to 2011, Ms. Daskal was counsel to the Assistant Attorney General for National Security at the Department of Justice and among other things, served as the Secretary of Defense and Attorney Generalled Detention Policy Task Force. Prior to joining the Department of Justice, she was the senior counter-terrorism counsel at Human Rights Watch and worked as a staff attorney for the Public Defender's Service for the District of Columbia. She earned a bachelor's degree from Brown University, a master's degree from Cambridge University and not surprisingly, a J.D. from Harvard Law School.

We welcome all of you. Your written statements will be entered into the record in their entirety and I ask that each of you summarize your testimony in 5 minutes or less. To help you stay within that time, there is a timing light at the table. When the light switches from green to yellow, you have 1 minute to conclude your testimony. When the light turns red, that is it. You are done.

Mr. Smith, welcome. We are pleased to have you here, and you may begin the testimony.

TESTIMONY OF BRAD SMITH, PRESIDENT AND CHIEF LEGAL OFFICER, MICROSOFT CORPORATION

Mr. SMITH. Chairman Goodlatte, Ranking Member Conyers, Members of the Committee, it is my pleasure to represent Microsoft this morning. Today's hearing provides an important opportunity to address a critical issue—the growing conflict between countries and among laws that are affecting not only technology, but people's safety and privacy. I think the ramifications of this issue are really illustrated by two real-world examples.

The first is a case involving Microsoft a year ago in Paris. The day after the horrific terrorist attack on Charlie Hebdo, the French

police using international legal process worked with the FBI and served on Microsoft lawful requests seeking the emails of the two terrorists that were at large in the streets of France. Because the French used international legal process, we at Microsoft were able to examine the orders, determine they were valid, pull the email and provide them to the FBI and the French all in exactly 45 minutes. That was a day when the system worked. But unfortunately, that has become the exception, not the norm. The norm is illustrated by the second example. A case involving Microsoft in Brazil; there, the Brazilian police have in pursuit of a local suspect served a local order requiring Microsoft to turn over content that is not in Brazil, but is in the United States. And because U.S. law prohibits us from turning over some of this content, Microsoft has had to refuse. The Brazilians have not turned to international process. They have not obtained the information they need, but they have fined Microsoft, and they are pursuing a criminal prosecution of one of our executives in Brazil for the sole reason that we are comply with United States law.

And unfortunately, that kind of case is spreading. It is spreading because other governments, including the United States government is using unilateral legal process rather than international legal process to obtain data around the world. Now, we appreciate that law enforcement needs information, sometimes located in other countries to do its job, but this approach to using unilateral process is causing concern around the world. It is causing concern in other countries about people's privacy rights. It is causing concern about whether other countries can even trust and use American products and technology. It is causing concern that is leading other countries to enact new laws to block the very steps that our government typically takes through unilateral search warrants.

Now, the good news is there are solutions at hand. There is a solution in the form of Federal legislation modeled on something like the LEADS Act. There is a solution in the form of modernization of the mutual legal assistance treaties. There is a solution in the form of new international agreements that are designed and built for the 21st century. Like the one that is now being considered between the U.S. and the U.K. All of this will require action across the executive branch, but it requires action by Congress as well because all of these problems have a root cause. Our law is old and has become outdated.

When Congress passed the Electronic Communications Privacy Act, when the House passed that bill by voice vote on June the 23rd, 1986, Ronald Reagan was president, Tip O'Neill was speaker, and Mark Zuckerberg was 2 years old. In the 30 years that have followed, 125 million new Americans have been born. Technology has moved ahead by leaps and bounds, but at least in this field, the law has mostly stood still. I have here on one hand, and IBM computer that was first sold in 1986, and I have here on the other hand, a Microsoft Surface that is for sale today. The computer that is for sale today not only connects to all of the world's information on the internet, it has 355,000 times as much storage capacity as the floppy diskette that one had to use in this computer that was sold when ECPA was passed. These two computers make the story

clear. Technology has moved forward. Now, the law needs to catch up. Thank you very much.

[The prepared statement of Mr. Smith follows:]

Written Testimony of Brad Smith
President and Chief Legal Officer, Microsoft Corporation

House Judiciary Committee
Hearing on International Conflicts of Law Concerning
Cross Border Data Flow and Law Enforcement Requests

February 25, 2016

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, my name is Brad Smith and I am the President and Chief Legal Officer at Microsoft Corporation. Thank you for the opportunity to provide Microsoft's perspective on these important issues.

Like many leading global technology companies, Microsoft was founded in the United States but now serves customers worldwide. In 1989, Microsoft opened its first datacenter in Redmond, Washington. Today, our company has more than 100 datacenters in over 40 countries around the world. Microsoft now serves more than 90 markets around the world from these datacenters, delivering more than 200 online services from our datacenters across the globe and supporting more than one billion customers. Like the rest of our industry, cloud computing has changed our business and our fundamental approach to technology.

Our company is proof positive that information technology in the 21st century is truly global. Today's technology providers are likely to be headquartered in one country, serve customers and store their data in a number of other countries, and face legal demands from potentially any government in the world seeking access to their customers' electronic communications and related data. Just last week I met with government officials and customers in Berlin, London, and New Delhi. It could just as easily have been anywhere else in Asia, Australia, Africa, or Latin America. And my counterparts, not just from the technology sector but from manufacturing and other industries, also travel the globe. This global reach of American businesses isn't just good for our companies; it is good for our country.

Even more important than the global reach of this new technology are the potential benefits it offers. We recognize, of course, that progress may be uneven and we should be sensitive not only to technology's promise, but to its potential pitfalls and perils. But there is no mistaking the fact that cloud computing is the future. If done well, this new technology, coupled with big data and machine learning, offers the potential to help people and organizations everywhere make progress in addressing some of humanity's greatest challenges.

This is good news.

But as the title for this hearing reflects, new challenges are arising as well. On some days, these are increasingly stark. For example, on a January morning last year the French Government sought the contents of emails from two customer accounts held by Microsoft, as it pursued the two terrorist suspects who were at large after the Charlie Hebdo attacks in Paris. It was apparent that information stored in the cloud was vital for the protection of public safety. The French authorities contacted the FBI in the United States – and the FBI served upon us a lawful

emergency request under U.S. law. Despite the fact that the FBI's letter arrived electronically at 5:47 a.m. on the west coast of the United States, we were able to assess its validity under U.S. law, conclude it was proper, pull the email content in question, and deliver it to the FBI in New York – all in exactly 45 minutes. In short, there are times, especially in emergency situations, when international legal processes for cloud technology can work well.

But that type of effective international legal cooperation process is all too often the exception rather than the norm. Most days the trend is different.

The international situation is worsening as competing laws increasingly are putting tech companies in the position of dealing with laws that conflict with each other. Global companies must obey the laws and respect the rights of consumers and companies in the countries where we do business. Yet we're increasingly encountering countries seeking to reach across borders with unilateral and extraterritorial search warrants that ignore the local legal rights of citizens. And we're starting to see other countries respond by passing or considering blocking statutes that will cause companies that seek to comply with one law engage in action that will violate another. We're encountering this in multiple parts of the world, including as a result of unilateral and extraterritorial search warrants issued in the United States, where as a consequence we have litigation currently pending before the Second Circuit Court of Appeals.

As I discuss below, the current legal trends are clear. Unless governments change course and adopt a new and more international approach, we risk confronting a conflict of law on steroids. This conflict should concern more than lawyers and people in the tech sector. What's at stake is our ability to protect people's privacy and keep the public safe. And it's important for American job creation and economic growth, as otherwise these conflicts will continue to undermine around the world people's trust in American technology.

This situation results in part from a very concrete problem: current laws are old and outdated. The principal domestic electronic privacy law on which the Government relies is now 30 years old. Put simply, it no longer reflects the way technology works.

We need new solutions that create new principles and new international legal processes. As I discuss below, we need to establish a modernized approach that enables law enforcement to work with our allies to fight crime jointly by sharing evidence quickly and efficiently through clear rules. It also needs to protect people's privacy in accordance with new principles that recognize the importance of a person's nationality and their right to be protected by their own law. We need new solutions that are international in nature and reflect the way that current technology actually works. I hope that today's hearing will represent an important step in helping this Congress – and the country and the world – develop new solutions that will work not only for technology, but for people.

I. The International Situation is Worsening.

Over the past several years, we have witnessed a rapid global expansion of governments extraterritorially asserting the power to regulate global technology companies. Countries are increasingly claiming new extraterritorial legal authority (and interpreting existing legal

authorities) to access and intercept data. And in response, other countries are enacting a range of laws intended to counterbalance such extraterritorial authorities, including data localization and data retention requirements.

We see this pattern in many parts of the world. As the problem broadens, technology companies increasingly are whipsawed by the push and pull of conflicting laws that govern their legal responsibilities. And both public safety and privacy risk are being sacrificed in the process. Global companies must obey the laws and respect the rights of consumers and companies in each country where they do business. But because laws that are applied extraterritorially increasingly conflict with each other, a company trying to comply with the law in one country may be required to engage in actions that violate the law of another country.

These conflicts are not speculative. In fact, the consequences for global providers and their employees in the countries requesting data are very real. This is illustrated, at least for Microsoft, by recent events in Brazil. The Brazilian courts have long asserted the authority to compel U.S. tech companies to disclose the contents of users' communications to Brazilian law enforcement, even when the data is located in other countries. Recently, the Brazilian Government enacted new legislation that reaffirms this point. Microsoft currently stores this data in the United States, and its disclosure is clearly prohibited by the Electronic Communications Privacy Act of 1986 ("ECPA"), in 18 U.S.C. § 2702(a), even when the data belongs to a Brazilian user. Hence, unless the information is sought by Brazilian authorities through international legal processes via the U.S. Government, Microsoft will violate U.S. law if it complies with a unilateral and extraterritorial Brazilian legal order.

Though we have explained this intractable conflict to authorities in Brazil, to date they have refused to seek the information through a Mutual Legal Assistance Treaty ("MLAT") due to time sensitivities. Instead, when we have refused to violate U.S. law by complying with unilateral and extraterritorial Brazilian orders, government authorities in Brazil have levied fines against our local subsidiary and in one case even arrested and criminally charged a local employee.

Lest one think that the authorities in Brazil are unique in the world by seeking unilateral and extraterritorial warrants over data stored in the cloud, perhaps one point above all is worth emphasizing: U.S. federal authorities are doing the same thing. To date our own Government has insisted that it has the legal authority under ECPA to serve warrants to obtain email and other content located in data centers anywhere in the world, in any case they are investigating, over any company against which they can exercise jurisdiction, and even when the content belongs to individuals who have never been to the United States. Even when technology companies have suggested that conflicts can be avoided by the use of MLATs between friendly allies, our Government has insisted that it prefers instead what it regards as faster and more convenient unilateral and extraterritorial legal action.

These types of actions are leading to increasingly strong reactions that are undermining trust in American technology around the world. They are putting technology companies in the untenable position of choosing which of two conflicting laws they must obey – and which of two laws they must violate. They conflict with long-term opportunities to encourage growth, investment, and innovation in the global technology sector, a sector led by U.S. companies and contributing to

millions of good U.S. jobs. And they create uncertainty for users – consumers and citizens – who are left without clarity about whether their own rights will be protected by their own courts and their own laws.

These issues already have caused substantial international tension, as we have seen in the recent invalidation of the U.S.-EU Safe Harbor Agreement and the subsequent negotiations of the new EU-U.S. Privacy Shield. On October 6 last year, the Court of Justice of the European Union struck down an international legal regime that over 4,000 companies had been relying upon not just to move data across the Atlantic, but to do business and serve consumers on two continents with over 800 million people. The Court made clear that its decision was motivated in large part by a concern about the extent to which the U.S. Government could access the data of EU citizens. As a result, in connection with the new EU-U.S. Privacy Shield, the U.S. Intelligence Community has described to the European Commission the layers of constitutional, statutory, and policy safeguards that apply to its operations, as well as oversight provided by other branches of the U.S. Government.

This most recent government-to-government interaction across the Atlantic is encouraging. But if we do not do more to build on this recent step, these issues are going to grow worse, not better.

One of the clearest illustrations of the worsening situation – and the one that effectively imposes a deadline that we need to heed – is the EU's upcoming implementation of the proposed General Data Protection Regulation ("GDPR"). Once adopted and implemented, the GDPR will replace Europe's existing data protection framework, and it makes major changes to the current legal regime in Europe. The GDPR is likely to take effect in the spring of 2018, giving us just two years to resolve these critical issues.

Current EU data protection law already imposes significant constraints on the ability of technology companies to lawfully transfer personal data from Europe to the United States in response to unilateral U.S. Government orders. But once the GDPR comes into force, the conflict between EU law and U.S. requirements will become even more stark. This is because, under Article 43a of the GDPR, orders mandating cross-border transfers of personal data will *only* be recognizable and enforceable if they are conducted *pursuant to an international agreement*, such as an MLAT.[1]

For technology companies, this means that in the near future, EU laws effectively will prohibit us from transferring electronic communications that we store in the EU in response to unilateral legal process from most third countries – including from the Government of the United States. While there are exceptions, these are extremely narrow.

---

[1] The full text of the new Article 43a of the GDPR states that "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."

The adoption of Article 43a will replicate across the Atlantic the conflict that has already arisen involving Brazil – but in this case it will be the U.S. Government that is compelling the disclosure of information in contravention of the laws of countries across Europe that will bar U.S. technology companies from complying.

Making this emerging conflict even more striking will be the larger fines that technology companies will face if they violate the GDPR. Under its terms, these can amount to fines of up to four percent of a company's worldwide annual turnover. The math is simple. Unless this problem is solved, we're talking about potential economic damages to the U.S. tech sector of billions of dollars per year, beginning in 2018.

As challenging as this will be for the tech sector, it may present even more serious challenges for public safety. This is because the U.S. Government today relies principally on unilateral legal processes served on companies to obtain extraterritorial access to information that is needed for criminal investigations. But it's hard to believe that this approach will remain tenable for our Government as the GDPR and other similar laws take effect. In effect, this will create a situation where the FBI, because of conflicting obligations imposed on global technology companies, is prevented from obtaining information that it needs.

To be clear, the EU is not forbidding other countries from lawfully obtaining data stored within their borders. But it is requiring that in order for these demands to be recognizable, they must be made pursuant to international agreements that reflect international law rather than unilateral action. That requirement is not unreasonable. As mentioned above, ECPA itself operates in certain respects in a similar manner.[2] In effect, the GDPR will bring to Europe what the United States has long had in terms of a statutory provision that effectively bars tech companies from moving personal data stored out of one country in order to comply with a unilateral and extraterritorial legal order issued by another.[3] In short, unless we change course and move from unilateral action to a more international approach, we will confront a conflict of law on steroids.

Ultimately all of this posits important questions. Is our national interest best served by governments acting unilaterally to obtain data in other countries? Or do we need instead new agreements and new legal norms and processes that will enable governments to work across borders effectively and pursuant to the international rule of law? Before answering these questions, it's worth noting the root cause for our current problems.

---

[2] ECPA contains a broad prohibition against the disclosure of the contents of stored communications. It then has exceptions to this prohibition, including responding to lawful orders from U.S. authorities. However, these exceptions do not permit tech companies to comply with lawful orders from a foreign country, even when that country is seeking data about one of its own citizens.

[3] Article 43a of the GDPR in fact was enacted out of a recognition that "[s]ome third countries enact laws . . . which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States." *See* GDPR Recital 90. The GDPR recognizes that the "extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed" under EU law.

II. Our Electronic Privacy Laws Are Outdated.

At bottom, the cause of our current problem is straightforward: too many of the laws that govern access to electronic communications today are old and outdated. The principal U.S. law regulating governmental access to digital information – ECPA – is now 30 years old. Put simply, it no longer reflects the way technology works.

When Congress enacted ECPA in 1986, it never conceived of today's cloud computing environment, where companies operate datacenters around the world. There was no World Wide Web, no cloud computing, and no social media – much of the technology that we take for granted today.

The technology of 1986 is particularly memorable to me, because that was the year I moved here to Washington and began working as an associate at a large law firm here. Computers were not standard at the time, to say the least, and I was the first attorney in the law firm's history to insist on having a personal computer at my desk as a condition of taking the job. But what is most striking is how little I could do with that computer, compared to the power of computing today. For years, any online activity required connecting to what feels today like a primitive modem to access an online service. It was an activity so foreign that it never even occurred to me to ask the law firm for both a computer and a modem. Today, of course, that technology is unrecognizable in an age where computers fit into the palm of our hands and we can connect to all of our most important digital information virtually no matter where in the world we are at a given moment.

The outdated vision of technology embodied in old technology laws is a threat, however, to both individual privacy and public safety because it fails to account for the ways that people actually use technology now. For example, ECPA draws lines between communications held by "electronic communication service" providers and those held by "remote computing service" providers – lines that are fundamentally unrecognizable to today's technology users.

ECPA also draws a line between communications such as emails that are 180 days old or less – which can be obtained only by a warrant – and those older than 180 days, which can be obtained by a subpoena. That line appears to reflect an assumption in 1986 that people didn't save records or communications that were more than six months old. Given the limits of computer storage at the time, that was easy to understand in the mid-1980s. Today, however, this obviously makes no sense. Most of us have more old emails than we can count. In fact, if someone has an email account that only has email less than six months old, it probably means they opened their account less than six months ago. For many of us, our email inbox is a repository of more private, personal information or sensitive business documents than any other medium – more than our homes or our computer's local hard drive. This distinction makes so little sense that in 2010, the Sixth Circuit held it unconstitutional. Ever since, we have seen prosecutors use warrants – not subpoenas – to obtain all communications, regardless of their age. Yet in the six years since, Congress has yet to modernize ECPA in any fundamental way. And the Government's position in our pending litigation in the Second Circuit effectively ignores the Sixth Circuit's ruling.

But laws regulating technology are not the only outdated part of our legal system. The MLAT process has also failed to keep up with the changing pace of technology. MLATs create treaty-

based frameworks that governments can use to obtain evidence located beyond their borders. Officials in the Executive Branch have suggested the MLAT process is too slow to serve today's needs, and they have a point. A 2013 report by the President's Review Group on Intelligence and Communications Technologies found that MLAT requests can take an average of 10 months to fulfill – and that such response times can prompt countries to enact data localization laws so that the country can issue process for that data directly, without going through an MLAT.[4] But the report suggested sensible solutions that address these problems without placing technology providers in the middle of conflicting law, including increasing resources for the branch of the Department of Justice that handles MLAT requests, creating an online submission form for MLATs that today are often filed by paper, and streamlining the process including by considering creating a single point of contact that can expedite a request.[5]

Cloud computing is the future of technology. When individuals and businesses use the cloud, they can access their customized services from any computer anywhere in the world, so long as they can connect to the Internet. Indeed, cloud computing is becoming the norm among American technology users. Anyone who uses Gmail or Facebook or Yahoo! or Outlook.com is using cloud computing – by entrusting technology providers to store their email on the provider's own server and remotely accessing those emails from their own computer. Cloud services also help businesses achieve greater computing power, analyze and share data more effectively, and improve data security – even as they reduce costs.

American individuals and businesses recognize the power of cloud computing. As a report published last July by the International Trade Administration acknowledged, cloud computing has emerged as a "game-changing" information and communications technology phenomenon with a "wide array of benefits for businesses and consumers."[6] One study cited in that report found that 17 of the top 20 enterprise cloud services come from companies based in the United States.[7] The forecasts for this growth are bullish – one projection expects businesses to spend $191 billion on cloud computing services by 2020, compared with $72 billion in 2014.[8]

Even in this new cloud-based and digital era, whether you are a consumer or a company, we believe that you own your email, your text messages, your photos, your documents, and all of the other content you create. Even when you put your content in our datacenters or on devices that we make, you still own it. The American people understand this. In survey after survey, over 80 percent of those polled have said that they believe that something they write in an email and

---

[4] *See* President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World, Dec. 12, 2013, at 226-29, *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[5] *Id.*

[6] *See* International Trade Administration, *2015 Top Markets Report Cloud Computing*, July 2015, at 3, *available at* http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf.

[7] *Id.*

[8] *Id.*

store in the cloud should not be any less private than something they write in a letter and store in a desk drawer.

That means personal information that consumers store with technology companies should not be accessed or seized without proper legal process. This is all the more important given the massive amounts of sensitive information consumers are storing with technology companies. Outdated laws that do not fit today's technology create a policy vacuum in which courts are forced to determine how to apply their obligations under substantial legal uncertainty. The Executive Branch has stepped in to fill this vacuum, generally by urging courts to adopt positions that strengthen the power of law enforcement. But these important policy decisions should not be left to the courts and executive branch alone. They raise issues of core concern to our most fundamental values, including not only our security but our personal privacy.

Congress – the branch of government directly accountable to the people – must weigh these concerns and take the lead in developing an appropriate legal framework that reflects and regulates today's technology and the expectations and values of today's consumers and today's citizens. In short, we need new law for a new century, not continued reliance on a law that is older than many devices that now sit in a museum.

III. We Need New Solutions That Are Both Modern and International in Nature.

Only a new and more international approach can protect privacy, keep the public safe, and promote economic growth. This approach must establish a modernized approach to regulating governmental access to electronic communications stored worldwide – one that enables law enforcement to work with our allies to fight crime jointly by sharing evidence quickly and efficiently through clearly-established legal rules and processes. But these solutions must also protect the privacy of technology users, who store their most sensitive personal information and most confidential business records with technology providers. Any solution must therefore contain three core elements:

- *First*, new solutions must work effectively on an international basis. The problems we have discussed today – created when one country asserts the power to access electronic communications extraterritorially – are international problems. They can only be truly addressed through international solutions that enable the rule of law – and the Internet itself – to function smoothly across national borders.

- *Second*, new solutions must continue to preserve our fundamental values and protect the Internet's unique ability to promote free expression and the sharing of information and ideas. At the same time, it must reflect that public safety is also a paramount public need – and a government responsibility. Governments have a legitimate need to access digital information to bring criminals to justice and to investigate terrorist threats. The only way to keep the public safe, to ensure healthy free expression, and to protect individual privacy, is to create a framework that reflects all of these values.

- *Third*, new solutions cannot simply ignore national sovereignty or trample on it. Governments can and must respect each other's borders. Instead, the key is to strengthen the ability of governments to act pursuant to the rule of law in cooperation with each other.

To implement such solutions, we must take action at both the national and international levels. At the national level, we must ensure that individual nations enact laws that more carefully weigh the circumstances in which a nation should assert the power to obtain evidence. Such assertions should be grounded in due process and must be consistent with international law. Moreover, new laws should recognize the importance of a user's right to be protected by the law of his or her own country.

One such approach would be to focus new legal norms on a person's nationality or location rather than the location of the person's data. For example, if a person is an American citizen or resident, their rights may be appropriately determined by U.S. law, and it seems appropriate for U.S. law to permit the extraterritorial and unilateral reach of a search warrant to that person's data regardless of where it is located. But when someone is not a U.S. citizen and lives outside the United States, we need U.S. law enforcement to work in accordance with new international legal processes to strike the right balance between privacy and safety and avoid legal conflicts and international tensions.

In the United States, one example of this type of solution is the Law Enforcement Access to Data Stored Abroad (or "LEADS") Act, H.R. 1174 and S. 512, introduced by Representatives Tom Marino and Suzan DelBene in the House and Senators Orrin Hatch, Chris Coons, and Dean Heller in the Senate. That legislation is a great starting point for a modern legal framework, which prescribes clear rules and limited circumstances in which the U.S. Government may issue legal process seeking digital information stored outside the United States.

We need more than new national laws, however. We also need new international agreements. Going forward, it is imperative that Congress work with other branches of the government to encourage the development of bilateral and ultimately international agreements to govern access to electronic communications.

To be clear, there is an existing legal foundation for this type of cooperation, although our current framework requires significant updates. For example, the United States has existing Mutual Legal Assistance Treaties ("MLATs") with a number of countries worldwide. These treaties illustrate the potential to agree on the circumstances in which one country may obtain evidence in another country – and to do so through international cooperation, not unilateral intervention. But as noted above, many of these MLATs are even older – and sometimes far older – than ECPA itself.

An international solution must have two components in order to holistically address the issues arising from governmental access to electronic communications worldwide. First, it must update the MLATs that already exist, including the funding that will be needed in order for the Executive Branch to pursue this work successfully. Second, it must create a new international framework that comprehensively addresses data access issues, in recognition of the fact that this is a global problem requiring a global solution.

A. MLATs Should be Modernized.

In the near term, MLATs must be modernized for the digital age. Two improvements, in particular, would be relatively straight-forward to implement:

- *First*, MLATS should move from an era of paper and wax seals into the digital age. We should ensure that the process for obtaining information pursuant to an MLAT is done electronically, and that law enforcement is not hampered by procedures that require paper letters to be mailed across oceans in order to request data.

- *Second*, MLATS should be standardized, both in format and in their terms. This would enable governments and technology companies to undertake faster legal reviews, without sacrificing privacy concerns. When MLATs are not standardized, law enforcement and technology companies must assess different legal terms and different legal obligations arising from requests from different countries. If the terms are standardized, it would create a legal process that could be more quickly navigated, while respecting the privacy rights common to all countries.

B. Creation of a Modern International Framework.

Looking more broadly, we need a new legal model or framework to address governmental access to electronic communications. We cannot stop with modernizing MLATs. Given the importance of public safety and personal privacy, we should work to forge new international legal rules that will better enable law enforcement – with appropriate safeguards – to obtain information needed for lawful investigations across borders. Again, there are existing agreements that we can build from to create this framework. For example, new legal rules can be built on past and current examples of multilateral law enforcement cooperation, such as the Budapest Convention on Cybercrime and the EU-U.S. Mutual Legal Assistance Treaty.

But whatever form it takes, any new framework addressing international digital access rights should reflect five important principles, all of which need to be pursued in new international agreements rather than unilaterally:

1. *Direct Legal Service on Service Providers.* First, new legal rules should enable the authorities in proper circumstances in one country to serve a new and proper order on a service provider in another country, but pursuant to legal rules that ensure respect for the rights of technology users. These rules should require that the government issuing the order simultaneously notify the government in the country of residence of the service provider or the user, so it is aware of the law enforcement activity that in effect is taking place within its borders or impacting one of its citizens. And these rules should enable either the service provider or the receiving government (or both) to object if the order is improper.

2. *Nexus with Country Issuing the Order.* Second, there should be a proper nexus between the country issuing the order and the individual whose content is being sought, and this new legal authority to obtain cloud content should be limited to specific and agreed upon criminal offenses. For physical evidence, the general rule is that the country where the evidence is located is the one with the right to obtain it, as seizing evidence is the exercise of a police

power. But an agreement governing cloud content might extend this rule or focus instead on reaching the content of citizens and residents of a country, even when the content belonging to those citizens or residents is stored in another nation. In other words, if the content of a U.S. resident is stored in Ireland, the U.S. Government could use this new legal instrument to serve a warrant directly on a service provider located there. And if a French resident's content is stored in the U.S., the French Government could similarly make use of this rule to obtain the content held by U.S. providers.

3. *Clear Standard for Issuance of an Order.* Third, in order to ensure that citizens' privacy rights are respected, there should be a required minimum showing that the investigating authority must make to obtain an order requiring disclosure of content. While countries have somewhat differing legal traditions, in the U.S., to obtain users' content, the law focuses on requiring "probable cause" to believe an individual has committed or possesses evidence of a specific crime. It is important to develop a minimum legal standard with which people can feel comfortable in creating this international framework.

4. *Transparency, Oversight, and Accountability.* Fourth, there should be a robust system in place to ensure there is adequate oversight of governments' use of these authorities, including accountability for any misuse. Companies should have the right to publish regular and appropriate transparency reports that document the number of orders they are receiving, the number of customer accounts affected, and the governments that issue such orders. Orders for the most sensitive data such as email content should be issued only by a court or similar independent authority in the requesting country. An order to turn over information constitutes an infringement of privacy. It is therefore appropriate that in almost all circumstances, this fundamental right should be infringed only after an independent judgment, by someone such as a magistrate or neutral authority, in which the need for the information justifies the order based on the facts known at the time.

5. *Respect for Human Rights.* Finally, countries should only be allowed to accede to any international framework agreement if they meet and maintain an adequate human rights record.

One example of this sort of agreement – bilateral in its current form – could result from the recently reported negotiations between the United States and the United Kingdom. As described by The Washington Post, those two countries are working on an agreement that can serve as a model for solving "an untenable situation in which foreign governments such as Britain cannot quickly obtain data for domestic probes because it happens to be held by companies in the United States."[9] That situation is indeed untenable. By adhering to the principles outlined above, these negotiations can put us on a path toward a solution that enhances individual privacy and law enforcement's ability to protect the public.

---

[9] *See* Ellen Nakashima and Andrea Peterson, *The British Want to Come to America with Wiretap Orders and Search Warrants*, Washington Post, Feb. 4, 2016, *available at* https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america--with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html.

* * *

Congress has an opportunity to modernize the outdated laws that regulate governmental access to electronic communications today. In addition, Congress can play a critical role in addressing these issues at an international level, by encouraging the creation of an international framework that will provide a sustainable and modern approach to ensuring governmental access to electronic communications worldwide. I know I speak for many in the tech sector in saying that I hope this Committee and Congress will act on these opportunities. We welcome the opportunity to discuss how technology companies can assist appropriately in these efforts.

Mr. GOODLATTE. Thank you, Mr. Smith. Mr. Chertoff, welcome.

TESTIMONY OF THE HONORABLE MICHAEL CHERTOFF, CO-FOUNDER AND EXECUTIVE CHAIRMAN, THE CHERTOFF GROUP

Mr. CHERTOFF. Mr. Chairman, it is good to be back. I am looking at that IBM computer. It looks like what I have at home still. I obviously would like to indicate that I am speaking here in a personal capacity, although my firm does do work with Microsoft and other tech companies in this area, and as I also previously disclosed, I am of counsel with Covington and Burling, which is actually involved in representing Microsoft in this litigation. But whatever I am saying here really reflects my own views and no one else should be held accountable for them.

I think it is really important that this Committee have this hearing, and that Congress get involved in legislating in this area. The issues that surround the intersection between modern technology and the law are frankly quite complicated. They are quite technical, and even having been a Federal judge, I have to say I am not sure the Federal courts in the first instance are the right place to resolve all of the competing issues in technical dimensions of these kinds of questions. Now, here, we are dealing with one aspect of this, which is as Brad Smith pointed out kind of dramatically—the amount of data now which is—moves around the world and is held in this so called cloud dwarfs what was being confronted when ECPA was passed. And contrary to what maybe some people think, obviously when the data is in the cloud, it is not really in the cloud. It is living somewhere in the world in a server, and the ability to house it anywhere in the world and to move it around rapidly as possible really changes the dimensions of the question about where something is and who ought to have the jurisdiction to compel it to be turned over.

I think we are seeing the issue of conflict of laws in three areas. First substantive areas where different countries in parts of the world have different views about what gets protected as private and what does not. Second, the question of process—different standards of process about what is required when a government seeks data, and finally, the problem of global companies that are often caught between different legal regimes and are damned if they do and damned if they do not.

And so, I think we do need to take the opportunity to look at rationalizing the law and particularly to the extent we can, globalizing the law. Coming up with agreements and processes that allow us to synchronize the law so that companies that are in the business of housing data are not caught between the so-called rock and a hard place. And I would suggest as I do in my statement, just a couple of points about this.

First, I think to the extent we can have agreements or frameworks in a statute that lead to agreements, we ought to be focusing on the citizenship of the accountholder and not where the data happens to be located. Data location should be driven by engineering considerations, and not by desires to create legal safe havens or to find places that are legally more or less hospitable.

The second thing I would say is if we are going to have agreements, we do need to make sure that the companies we are dealing with have process in place that is comparable to what we require with respect to our own citizens when other countries want to have data that is held over here. We do not want to create a situation where we are jeopardizing the constitutional rights of our Americans by simply in the pursuit of an agreement.

And finally, we have to recognize there will be certain types of requests from other countries that will run afoul substantive issues and so, we are going to have to create a regime—a legal regime in place through any agreement and through any statute that respects that. Finally, there has been a lot of discussion about the MLAT process and I think, you know, Brad Smith was very clear in indicating this process can work if we want it to work. Often, frankly, I can speak from my own experience, honoring MLAT requests goes to the bottom of the pile of overworked assistant U.S. attorneys, but with modern technology and if the government views these as high priority cases, we can move to the kind of process that gives you the results that occurred in the Paris case. And which I think would encourage both our country and other countries to use the international treaty process rather than unilateral action as a way to get information that is stored in other parts of the world.

So, thank you, Mr. Chairman, and I look forward to answering questions.

[The prepared statement of Mr. Chertoff follows:]

Statement for the Record
by
The Honorable Michael Chertoff
Co-Founder & Executive Chairman of
The Chertoff Group
and
Former Secretary of the
U.S. Department of Homeland Security

U.S. House Judiciary Committee Hearing:
"International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests"

Thursday, February 25, 2016

STATEMENT FOR THE RECORD
BY THE HONORABLE MICHAEL CHERTOFF
UNITED STATES HOUSE JUDICIARY COMMITTEE
FEBRUARY 25, 2016

I want to thank Chairman Goodlatte, Representative Conyers and members of the Committee for inviting me to testify and for the opportunity to contribute to this important discussion. I am hopeful that discussions like these today will ultimately contribute to a better understanding of how our world has changed when it comes to the way we use data and where possible reforms may be necessary to update laws and policies that reflect today's environment.

I want to state clearly that I am testifying today and submitting my Statement for the Record in my personal capacity, although, for the record, I am co-founder and executive chairman of The Chertoff Group, a security and risk management company that provides strategic advisory services on a wide range of issues, including those we may discuss today. As I communicated previously to the Committee, The Chertoff Group does have technology clients interested in the topic of this hearing, including Microsoft who is also testifying as a witness today. However, I am not representing any specific company at this hearing and I will provide my opinion and testimony based on my own experience and understanding of the issues. Additionally, I also serve as Senior of Counsel to the law firm of Covington and Burling, LLP, which is counsel to Microsoft in a related litigation, although I am not personally engaged in that representation.

Today we live in a world shaped by a global digital economy – an economy made possible by the networking and communications infrastructure of the Internet which has enabled individuals, businesses and institutions, and governments to communicate, collaborate, trade and conduct business in a way never imagined before. The singular characteristic that defines our global cyber network is its universality. It is the Internet's ability to make information available instantly on a global scale which has enabled critical communications and services essential to our way of life.

The Internet was started more than 30 years ago by a small group at Stanford University in response to a government request to create a small, collaborative environment to be used by a

small group of trusted users. Security was never a concern because the group of users was small and known to each other. It was designed to be free, open, flexible and efficient.

Today, the Internet is a globe-spanning domain. More than three billion citizens and six billion devices are connected to the Internet. Its value proposition is that it is an open network of networks. As we work to preserve the openness of the Internet, we must do so through collaboration between the private sector, government, and the broader international community.

Today, I want to address some of the unique challenges we face in this global Internet economy and how, we … speaking collectively across government and industry … can best govern and secure the Internet in a way that protects public safety and enhances privacy without creating barriers that will diminish the important benefits we yield today.

The transition to a global Internet economy has been accompanied by a significant change in the nature of how we communicate, conduct transactions and exchange commerce. Today, we see a world through data. Our smart phones and devices hold vast amounts of data relating to our personal lives as well as daily business interactions. This data is not stored in any one specific place but today, it is often stored in the "cloud." To be clear, data stored in the cloud still resides on a physical server; however, the location of the server and where the data is ultimately stored can be anywhere around the world and is often determined based on several factors such as the location of the customer; facility resources (for example, adequate power and cooling capacity); and cost effective business environment. As a result, servers in one country can be storing communications between two people in another country.

The result is an increasingly common phenomenon – disputes and transactions that cross national boundaries. To be sure, the phenomenon is not new. There have been transnational commercial transactions and transnational criminal activity since the time that borders between nations were first created.

But the growth of a system of near-instantaneous global communication and interaction has democratized the phenomenon of cross-border commerce in a transformative way that challenges and disrupts settled conventions.

These challenges and disruptions have led to uncertainty including:

- Conflicts with regard to whose laws govern data held in cyberspace;
- Unilateralism or assertion by nations that its laws control actions by evidence holders, irrespective of other countervailing interests; and
- Global companies subject to competing and inconsistent legal demands where one country may require disclosure of information that another country prohibits from being disclosed

These issues pose challenging questions from a legal standpoint about who has jurisdiction over data held elsewhere and how one governs data in the cloud? How do we modernize our laws in a way that balances legitimate public safety needs and lawful access requests with the security and privacy of our citizens?

Without resolution or agreement on rule of law, all of this uncertainty contributes to concerns that these conflicts can lead to fragmentation of the Internet as we know it today. It could lead to second and third order effects such as data localization. If we don't figure out a new way of resolving legal conflicts, the universal Web as we know it may soon be Balkanized. We will lose the free and openness of the Internet as we do today and sacrifice the benefits that has brought incredible advances in our society.

The inevitable result will be that consumers suffer diminished access to the network overall. Decisions companies make about the location of their servers and hardware will be driven by legal gamesmanship rather than by technological or infrastructure considerations. We should work together to identify an agreed-upon international system for newly designed choice-of-law rules for data, particularly data in the Internet cloud. Such rules would determine which country's law governs in a dispute, as when we try to decide whose law governs a contract for the sale of goods. We need to harmonize existing rules in a framework of law for the cyber age.

For consideration, here are a few principles that ought to guide us going forward:

- Rules imposing localized requirements for data storage, processing, retention and distribution distort markets and create uncertainty. We should preferentially choose globalized rule-sets that apply across the entire domain, rather than nation-specific rules that add unnecessary costs and may even impose significant conflicting obligations;

- Because we need globally applicable rules, there will be challenges in securing world-wide agreement. Accordingly we need to work together and identify the smallest set of rules that are universally acceptable and necessary to the functioning of the network;

- In those instances where the laws of two countries conflict, we need an overarching choice of law agreement that determines which law controls based, preferably, on the citizenship of the individual account holder.

As previously mentioned, the overall public benefits resulting from new opportunities and innovation relating to the Internet have also brought forward new opportunities for criminal activity as well. Together, the way communication and information is exchanged has created new challenges for law enforcement. Fundamentally, it has changed the nature of evidence – how it is created; how it is stored; and how it is accessed. That change arises from both technical aspects of how electronic data is stored and practical aspects of competing global legal systems.

The Mutual Legal Assistance Treaty or MLAT process - the system by which law enforcement cooperate across borders – is hopelessly outdated. The President's Review Group on Intelligence and Communications Technology reports that the average length of time it takes for the U.S. to secure a response to its requests for evidence from foreign police partners is 10 months. And doubtless the converse is true as well – American responsiveness is also tedious and slow. None of this is adequate.

As our Congress considers reforms, we should highlight the need for reciprocity. American improvements will be insufficient if they are not matched by our partners around the globe. An

improved and functioning MLAT process would also have the collateral benefit of incentivizing nations to forego the exercise of unilateral evidentiary collection methods.

There is no doubt that issues concerning technology, data access, security and privacy within this globe-spanning Internet domain will continue to evolve as forecasts call for tremendous growth in the numbers of users and devices connected to the Internet. We do have an opportunity, however, to bring forward significant security reforms that can protect the greater public good without harming the digital economy which is also an essential element of our national security. Enhancing privacy and security, as well as providing clarity and consistency with regard to how we govern and apply rule of law, would be major achievements in this current environment.

###

Mr. GOODLATTE. Thank you, Mr. Chertoiff. Mr. Kris, welcome.

TESTIMONY OF THE HONORABLE DAVID S. KRIS, FORMER ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY, UNITED STATES DEPARTMENT OF JUSTICE

Mr. KRIS. Thank you, Mr. Chairman, Mr. Ranking Member, and Members of the Committee for inviting me to testify. I, too, am speaking only in my personal capacity. There is obviously a range of opinion represented on the Committee today, but I think there is also an unusual degree of consensus, which I have heard during the course of this morning's proceedings on at least three important points. First, there is a problem.

We have a situation where there are international conflicts of laws in which one government's laws can compel the production of data, while simultaneously, another government's laws will prohibit it. This is very vexing for the holders of data, like Microsoft, who understandably wish to comply with all of the laws and rules to which they are subject. Second, this problem is not unprecedented, but it is getting worse over time. I think that is true for three technical reasons and three political reasons which I will outline quickly.

Technically, the size and scope of international data networks, the degree of international data storage in the cloud and the use of encryption are all on the rise in previous—in recent years. Politically, the Snowden disclosures, I think, have caused the U.S. Government to decrease the scope and increase the transparency of its surveillance. That is particularly true in the foreign intelligence realm, but there is a good deal of overlap with law enforcement.

On the other hand, in Europe, the rise of ISIL and some of the technical factors that I have mentioned, I think have caused European governments to go the other way to expand their surveillance authorities and to put a lot of pressure on providers. And third, the providers for their part are a little bit caught in the middle of that. And they have reacted, understandably, again, I think in two ways. By reducing the degree of cooperation, one, with respect to voluntary production of data rather than compelled production of data, and then, also at the margins in resisting certain compulsions.

I want to be clear this is not in any way some kind of wholesale civil disobedience and it is again perfectly understandable given their fiduciary duties. Even if, in any given instance, one might argue that it either does not go far enough or goes too far. Given that problem and the nature of the problem, I think there has been consensus third that some kind of international solution is in order to address it. You have heard today about the MLAT process, and one of the solutions that has been discussed is some kind of fairly drastic increase in the resources available for processing MLATs. If the current time to process is 10 months and the equation scales linearly and I am not sure it does—if you wanted to reduce the time down to 1 day, you would be scaling up by a factor of 300. Again, I am not sure, it scales in a linear fashion. There are some structural limits in MLAT.

And the other means of addressing the problem we have talked about today involve direct access by foreign governments. In some

carefully delineated class or sub-class of cases, I understand the executive branch is currently working with the U.K. on a bilateral agreement. Perhaps it would be limited to non-U.S. persons located abroad by analogy to the FISA Amendments Act. Perhaps to certain kinds of crimes; perhaps to certain kinds of directives on certain predicate showings made by certain officials in the U.K. You can imagine lots of limits here. And then, of course, Congress will need to evaluate whether those limits are appropriate and only then make the necessary amendments to the Stored Communications Act to allow that agreement to be effectuated.

So, there is definitely a profound role for Congress in this area regardless of these executive agreement. Finally, I want to mention, but I do not know as we can discuss fully in this setting, a couple of foreign intelligence surveillance concerns that I outlined in my testimony. I urge you to have a conversation with the executive branch about the two gaps in FISA that I have set forth. I would love to be wrong about those, but I think it is something that is worth your exploring in an appropriate setting with the executive branch. Thank you very much.

[The prepared statement of Mr. Kris follows:]

Statement of David S. Kris
Before the Committee on the Judiciary, U.S. House of Representatives,
Hearing on International Conflicts of Law Concerning Cross Border Data Flow and
Law Enforcement Requests
February 25, 2016

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, thank you for inviting me to testify. I am a former Department of Justice official and the co-author of a treatise on national security investigations and prosecutions, and I am testifying in my individual capacity, not as a representative of any other party. My testimony is drawn from two papers that I recently wrote: *Preliminary Thoughts on Cross-Border Data Requests*, and *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, both of which are available at www.lawfareblog.com. These papers cover in more detail, with appropriate citations and support, the points set out below.

1. Today, for reasons both technological and political, there are growing conflicts between U.S. and foreign laws regulating production of data in response to governmental surveillance directives. These conflicts arise where one government's laws compel the production of data, and another government's laws forbid that production. From the U.S. perspective, the conflicts typically present in two main forms.

First, major U.S. electronic communication service providers face escalating pressure from foreign governments, asserting foreign law, to require production of data stored by the providers in the United States, where the production would violate U.S. law. For example, the United Kingdom's Data Retention and Investigatory Powers Act 2014 (DRIPA) explicitly authorizes the UK to compel production of data from anyone providing a communications service (such as email) to customers in the UK, even if the data in question are stored abroad. But the U.S. Stored Communications Act (SCA) generally forbids production of certain data (including the contents of email) stored in the U.S., and does not contain an exception for production of data in response to a UK directive.

Second, at the same time, foreign governments also are increasingly likely to enact laws forbidding production of locally-held data in response to U.S. (and other) demands for its production, and also to enact laws requiring certain data to be held locally, creating a form of reciprocal pressure. Currently pending in the Second Circuit is a case in which the U.S. government is relying on the SCA to compel Microsoft to produce email stored in Ireland; Microsoft is resisting on the ground that the SCA cannot compel production of data stored abroad; and the Government of Ireland has filed an amicus brief supporting Microsoft and asserting its sovereignty, but conceding that it is "incumbent upon Ireland to acknowledge" that "there may be circumstances in which an Irish court would order the production of records from an Irish entity on foreign soil," perhaps even if "execution of the order would violate the law of the foreign sovereign."

In this environment, the same action in response to a surveillance directive may be at once both legally required by one government's laws, and legally forbidden by another's. Although this problem is not unprecedented – with antecedents in cases involving U.S. grand jury subpoenas for bank records held in foreign countries with strict bank secrecy laws – the conflicts have been increasing lately in frequency and intensity. That is due to technological and political factors, including the growing size, speed and use of the Internet and other data networks; greater use of remote data storage (e.g., the cloud); the Snowden disclosures and resulting suspicion of U.S. surveillance practices in Europe; the U.S.

government's reaction to those disclosures by decreasing the scope and increasing the transparency of certain of its surveillance practices; the increased use of encryption; the rise of the Islamic State of Syria and the Levant (ISIL); and European governments' reaction to ISIL's rise by increasing the scope of their own surveillance.

International agreements, and appropriate domestic legislation, could help reduce conflicts and rationalize surveillance rules to promote international commerce, law enforcement, protection of civil liberties, and the worldwide rule of law. The simplest approach in concept would be to remove or override domestic legal prohibitions on disclosure, where desired, in response to certain types of favored foreign production directives. This would probably begin in a bi-lateral setting with the UK, and could expand from there. As a matter of U.S. law, it would not be difficult technically, although it might be very challenging politically, to make the necessary amendments. There certainly are other ways to approach the issue, including reforms to our various Mutual Legal Assistance Treaties or the processes for implementing them. Absent some new international approach, however, we face the prospect of an increasingly chaotic and dysfunctional system for cross-border data requests that benefits no one.

2. Although many of the challenges in this area arise in connection with ordinary law enforcement, I should highlight two related gaps in U.S. law regulating foreign intelligence surveillance. First, whatever the merits of Microsoft's argument in the case discussed above, there is no real doubt that it would prevail if the U.S. government sought to compel production of email stored in Ireland under the Foreign Intelligence Surveillance Act (FISA), if the target were either a U.S. person (in any location) or a person (of any nationality) located in the United States. That is because traditional FISA searches may only occur in the United States; traditional FISA electronic surveillance applies to stored data only when the surveillance device is used in the United States; Section 702 of the FISA Amendments Act (FAA) applies only to non-U.S. persons located abroad; Section 703 applies only when the surveillance is conducted in the United States; and Section 704 (which applies to U.S. persons abroad) cannot be used to compel assistance from a provider. In short, unless the provider voluntarily repatriates the stored email, its production cannot be compelled under FISA. This is a potentially significant shortfall in the statute, particularly as data become more and more mobile, subject to being stored in any location, or even fragmented and stored in several locations at once.

A second possible gap concerns the situation in which all parties to a communication are located abroad, but the communication transits a wire in the United States. In that situation, it has long been the case that the U.S. government generally cannot get a FISA Court order to compel the assistance of the provider that owns the wire. Unless it has a valid target under FAA Section 702 (a non-U.S. person located abroad), the most the government can do is assure the provider, in the form of a certification from the Attorney General, that it may lawfully cooperate, but not that it must do so. If a provider refuses, the government has very little recourse. Today, with providers more recalcitrant than they have been, voluntary assistance may not be forthcoming.

These two and several other important issues in the field of foreign intelligence surveillance (addressed in the papers cited above) should, in my opinion, be considered by Congress soon.

Again, thank you very much for inviting me to testify and for considering my views. I am happy to answer any questions.

Mr. GOODLATTE. Thank you, Mr. Kris. Ms. Daskal, welcome.

TESTIMONY OF MS. JENNIFER DASKAL, ASSISTANT PROFESSOR, AMERICAN UNIVERSITY WASHINGTON COLLEGE OF LAW

Ms. DASKAL. Thank you, Mr. Chairman, Mr. Ranking Member, and Members of the Committee. Thank you for inviting me here today. I want to spend my time talking about three things. The problem, why Congress is needed, and specifically, what Congress should do. So, as has already been discussed pretty extensively, the Stored Communications Act operates as a blocking statute. It prohibits U.S. space providers from disclosing certain data, including emails to anyone other than the U.S. Government pursuant to a warrant.

Now, let us consider U.S. investigation of a London murder. Imagine that the U.K. officials seek the emails of the alleged perpetrator to help establish motive. If the alleged perpetrator uses a U.K.-based provider, the officials could likely get access to the date within days, if not sooner. If instead, the data is held by an American-based provider, the Brits will be told that they need to go through the mutual legal assistance process and initiate a diplomatic request. This is, as we have already heard, a notoriously inefficient process taking an average of 10 months, and foreign governments are frustrated, understandably, by the state of affairs, and they are responding in a number of concerning ways, including the mandating of data localization which undercuts the growth potential of the internet, increases the cost to American businesses and facilitates domestic surveillance; unilateral assertions of extra territorial jurisdiction which put American companies in the crosshairs of two competing legal obligations with a foreign government demanding the compulsion of data and U.S. law prohibiting it; and the use of malware and other less accountable forms of accessing the sort after data, which undercut the privacy and security of all.

Now, in response to this, as we have heard, the U.S. and U.K. have been negotiating an agreement that would allow the Brits, in certain circumstances, to make direct requests to U.S. companies for stored communications. Such an agreement is needed. If done right, it is an important step forward, which then brings me to my second point, the need for Congress. As we have already heard, none of this can be implemented without congressional authorization.

So, what should Congress do? Congress should amend the Stored Communications Act. It should authorize the executive to enter into bilateral and multilateral agreements that would allow, in specified cases, foreign governments to directly request stored content from U.S. providers. In doing so, Congress should also set the key parameters of such agreements, ensuring, among other things, that the partner country meets basic human rights standards; that the particular requests satisfy a baseline set of procedural requirements; and, that the system is subject to meaningful transparency and accountability mechanisms. These parameters are essential and they are justified for at least two reasons.

First, even as I think as envisioned by these agreements, the target of the request is a foreign national, it is likely, in fact, almost

certain that at some point, some time, such requests will lead to the incidental collection of U.S. citizen data. And second, whereas, the United States is often in the position of exhorting other countries to improve their human rights standards and protect free expression, this is one of those rare opportunities to couple such exhortations with a carrot, that of expedited access to U.S. data. And in so doing, help set the system of a global system of cross border access to data.

Now, in making these recommendations for Congress to engage, I am not alone. For the past 6 months, I have been working with a cross-section of civil liberties groups, companies and academics all focused on the need to reform the system governing law enforcement access to data across borders. My recommendations draw heavily on the conversations with this group. Although, I speak solely in my personal capacity and not on behalf of anybody else.

To sum up, the system for responding to law enforcement requests for data is broken. The time to fix it is now. Congress has an opportunity, and in my view, a responsibility to help build a system for the future. One that simultaneously safeguards privacy, protects American businesses and promotes the growth of an open and secure internet. Thanks.

[The prepared statement of Ms. Daskal follows:]

AMERICAN UNIVERSITY
WASHINGTON, DC

Statement of
Jennifer Daskal

Assistant Professor
American University Washington College of Law

Committee on the Judiciary
United States House of Representatives

Hearing on International Conflicts of Law
Concerning Cross Border Data Flow and
Law Enforcement Requests

February 25, 2016

WASHINGTON COLLEGE OF LAW
4300 NEBRASKA AVENUE, NW WASHINGTON, DC 20016
http://www.wcl.american.edu

Statement of
Jennifer Daskal
Assistant Professor
American University Washington College of Law

Committee on the Judiciary
United States House of Representatives

Hearing on International Conflicts of Law Concerning
Cross Border Data Flow and Law Enforcement Requests

February 25, 2016

Chairman Goodlatte, Ranking Member Conyers, and Members of the Committee, thank you for inviting me to testify.

For the past six months, I have been working with a cross-section of companies, civil society groups, and other academics who share common concerns about the rules governing law enforcement access to data across borders — and the potentially negative consequences of these rules for privacy, security, American business, and the future of the Internet. While my testimony draws on those conversations, I speak solely in my personal capacity and not on behalf of anyone else.

Earlier this month, the *Washington Post* reported that the United States and United Kingdom are negotiating an agreement that would begin to address some of these concerns.[1] Specifically, the agreement would, according to press reports, permit U.K. law enforcement officials to directly request the content of stored emails and other data from U.S.-based providers. Such an agreement is needed. If done right, it would be an important step forward — one that can minimize dangerous incentives toward data localization and other less accountable means of accessing sought-after data; promote privacy and related human rights; and protect U.S.-based companies from being increasingly caught between conflicting laws.

But an agreement of this kind cannot be implemented without Congress's authorization. Congress thus has an important opportunity — and in my view responsibility — to empower the executive to enter into such agreements and to set the key parameters as to their details. Such parameters are essential to protecting American interests in both the short and long term, and to setting the stage for a system of access to cross-border data that simultaneously protects privacy, security, and the Internet of the 21st century.

[1] Ellen Nakashima & Andrea Peterson, *The British want to come to America — with wiretap orders and search warrants*, THE WASH. POST, Feb. 4, 2016.

The following testimony describes the problem and offers a suggested way forward. I end with a discussion of several important and related issues, including the need to modernize the Mutual Legal Assistance Treaty (MLAT) system, the absence of rules governing foreign government access to transactional records (such as to/from lines on emails), and the ongoing debate over the reach of the United States' warrant authority under the Stored Communications Act (SCA). As I explain in more detail below, the basic jurisdictional questions should be answered in a reciprocal way for both the United States and foreign governments, and should turn primarily on the location and nationality of the target of the investigation, rather than the location of the data.

The Problem

The SCA, enacted in 1986 before communications were truly global, operates as a blocking statute. Except in very limited circumstances, it prohibits U.S.-based Internet Service Providers (ISPs) from disclosing certain data, including the content of users' communications (such as stored emails), to anyone other than the U.S. government pursuant to a U.S.-judge issued warrant based on a U.S.-based standard of probable cause.[2] While such a warrant requirement is a strong privacy-protective standard — and one that I hope Congress ultimately makes applicable, as a matter of statutory law, to *all* United States government requests for stored content[3] — it poses a combination of normative and practical problems when imposed on other countries. Ironically, the end result, as I explain in what follows, may be a reduction of privacy and related rights-protections for all.

As a result of the SCA's blocking provision, law enforcement seeking the content of stored communications, such as emails, that are held by a U.S.-based ISP cannot directly request the data from the ISP. Rather, they must make government-to-government requests for the data — even when they are seeking data of their own citizens in connection with the investigation of a local crime. This is a time-consuming process, and it is frustrating key foreign partners, particularly as criminal investigations increasingly rely on digital evidence in the hands of U.S.-based ISPs. Why, after all, should the United States insist on American standards and American procedures when the only connection to the United States is that the data happens to be held by a U.S.-based provider?

Consider, for example, U.K. law enforcement officials investigating a London murder. Imagine that the agents think the crime arose from an affair gone bad and seek the emails of the alleged perpetrator to help establish motive. If the target of the investigation uses a U.K.-based ISP, the officials would likely get access to the data within days, if not sooner. If, instead, the data is held by Google or another U.S.-based provider, the U.K. officials will be required to go through what is known as the MLAT process and initiate a formal U.K.-U.S. request for the data.

---

[2] *See* 18 U.S.C. 2702(b); 2703(a) (2012).

[3] I am encouraged by the overwhelming, bipartisan support for the Email Privacy Act, H.R. 699, 114th Cong. (2015), which now has 310 co-sponsors, and I urge the Committee to report the bill favorably and the House leadership to bring it to a vote on the floor.

This is a laborious process. First, the Department of Justice reviews the request. If approved, it is forwarded to the relevant U.S. Attorney's Office. Second, a federal prosecutor must obtain a warrant from a U.S.-based magistrate based on a U.S.-based standard of probable cause to compel production of this data. (Needless to say, processing these foreign requests for data is not often at the top of most U.S. Attorneys' priority lists.) Third, the warrant is served on the ISP. Fourth, the data, once produced, is routed back to the Department of Justice, where it is again reviewed before finally being transferred to the requesting government. The process takes an average of ten months.[4]

Foreign governments' frustrations are understandable, and they are responding in a number of concerning ways — all designed to bypass this cumbersome process. The range of responses include:

- *mandatory data localization requirements*, pursuant to which the content of communications (or a copy of such content) of a country's residents and/or citizens are required to be held in-country.[5] This ensures that the requesting country can access the data pursuant to domestic legal process, without having to make a diplomatic request to the United States. Not only do such localization requirements facilitate domestic surveillance in ways that threaten to undercut user privacy, but they increase the costs of doing business and undercut the Internet's innovative potential;

- *unilateral assertions of extraterritorial jurisdiction,* in ways that increasingly put U.S. companies in the cross-hairs between conflicting laws, with foreign governments compelling production of data and U.S. law prohibiting it. In fact, current (albeit soon to expire) U.K. law asserts the authority to compel the production of stored content from any company that does business in its jurisdiction, without any limit based on the target's nationality or place of residence;[6]

---

[4] *See, e.g.*, RICHARD A. CLARKE ET AL., PRESIDENT'S REV. GRP. ON INTELLIGENCE & COMMC'N TECH., LIBERTY AND SECURITY IN A CHANGING WORLD 226-29 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [http://perma.cc/36EE-6J9F] (noting that the United States takes an average of ten months to respond to official requests made through the MLAT process for email records).

[5] *See, e.g.*, Sergei Blagov, *Russia's 2016 Data Localization Audit Released,* BLOOMBERG LAW, Jan. 13, 2016, http://www.bna.com/russias-2016-data-n57982066291/; Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677 (2015) (surveying localization laws); Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders*, THE HAGUE INST. FOR GLOBAL JUST. (May 1, 2014), http://ssrn.com/abstract=2430275 [http://perma.cc/D2FC-F29Y] (describing the rise of data localization movements and analyzing the key motivating factors).

[6] *See, e.g.*, Data Retention and Investigatory Powers Act 2014, c.27, § 4, (Eng.) (expires December 31, 2016). While the legislation specifies that "regard is to be had" to a possible conflict of laws, the legislation does not say whether and in what situations the laws of the nation in which the data is located would trump. *Id.* § 4(4); *see also* INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, REP. ON THE INTELLIGENCE RELATING TO THE MURDER OF FUSILIER LEE RIGBY, 2014, HC 795, at 151 (UK) (describing

- *threats against employees or officers of local subsidiaries* for failing to turn over the sought-after data, even in situations where U.S. law prohibits them from doing so;[7]

- *mandatory anti-encryption regimes* (e.g., mandatory backdoors) that facilitate live interception of the data as it transits through the requesting government's jurisdiction and thereby provide an alternative way to access sought-after communications;[8] and

- *increased use of malware* and other opaque and less accountable means of accessing the data that weaken the security for all users.[9]

These responses threaten the privacy rights of all users of the Internet, including American citizens and residents. They undermine security, harm U.S. business interests, and diminish the productive potential of the Internet over time.

The Solution

The U.S.-U.K. discussions provide a possible response to some of these concerns. If done right, such an agreement could provide a front door alternative to back channel methods of gaining access to the same evidence. It would help to minimize the dangerous incentives in favor of mandatory localization, unilateral assertions of extraterritorial jurisdiction, and mandatory decryption requirements. And it is an opportunity to establish a set of transparent, accountable, and privacy-protective rules — rules that can then become a model for further bilateral and multilateral agreements.[10]

Specifically, the draft agreement, at least as reported by the *Washington Post*, would permit U.K. law enforcement officials to make direct requests to U.S.-based ISPs for stored content, so long as the target of the request resides outside the United States, and is not a U.S. citizen or legal permanent resident. If, however, the U.K. sought emails of U.S. citizens, legal permanent residents, or persons residing in the United States, regardless of their nationality, it would need to employ the MLAT system, and could only

---

a key goal of the legislation as permitting access to otherwise difficult-to-obtain data held by U.S.-based providers).

[7] *See, e.g.*, Elias Groll, *Microsoft vs. the Feds, Cloud Computing Edition*, FOREIGN POLICY, Jan. 21, 2016, http://foreignpolicy.com/2016/01/21/microsoft-vs-the-feds-cloud-computing-edition/ (discussing the arrest of a Microsoft executive in 2014 in Brazil for his company's refusal to produce Skype data belonging to the target of a criminal investigation).

[8] *Cf.*, Regulation of Investigatory Powers Act 2000, c.23, §§ 49-51, (Eng.) (laying out situations in which the UK government can mandate providers to assist with de-encryption).

[9] *See, e.g.*, Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JUST SECURITY, Feb. 16 , 2014 https://www.justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/ (explaining how malware could be used to subvert otherwise applicable territorial limits on direct access to sought-after data)

[10] *See* Jennifer Daskal, *A New US-UK Data Sharing Agreement: A Tremendous Opportunity, If Done Right*, JUST SECURITY, Feb. 8, 2016, https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/.

obtain the data based on the issuance of a U.S. warrant. Such a demarcation reflects the idea that U.S. standards should continue to govern access to data of U.S. citizens, legal permanent residents, and persons located within the United States — whereas the United States has little justification in imposing these specific standards on foreign government access to data of non-citizens who are located outside the United States. This approach presents a much preferable alternative to the U.K. claim that U.K. law enforcement can unilaterally compel the production of certain communications content from any provider that does business in its jurisdiction, including emails sent and received by U.S. citizens.

These privileges and limits also are reportedly designed to be reciprocal (as they should be), meaning that the U.S. would be permitted to directly compel the production of non-U.K. resident and non-U.K. national data from U.K. providers, but would need to initiate diplomatic processes if it wanted a U.K.-based provider to turn over data on one of its own citizens.

None of this, however, can happen without Congress. For any such bilateral or multilateral agreement to be implemented, Congress first needs to amend the SCA to permit foreign governments to directly request emails and other stored content from U.S.-based providers in certain, specified circumstances.

Specifically, Congress should amend the SCA to authorize the executive branch to enter, on a case-by-case basis, bilateral and multilateral agreements that permit foreign law enforcement to make direct requests to U.S.-based ISPs for U.S.-held stored content. In doing so, Congress should also *set the key parameters of such agreements* — ensuring among other things that the requesting country meets basic human rights standards, that the particular requests satisfy a baseline set of procedural protections, and that the system is subject to meaningful transparency and accountability mechanisms.

In addition to requiring foreign governments to rely on the MLAT system (including the requirement of a warrant based on probable cause) to get the data of U.S. residents, as well as U.S. citizens and legal permanent residents wherever located, Congress should specify that any agreement include the following elements:

(i) *General Human Rights Protections*: The executive branch should be required to certify that the partner government meets basic human rights norms prior to entering into such an agreement. This is critical to guard against sought-after data being used to torture, abuse, or otherwise violate the target's (or others') human rights;

(ii) *Request-Level Protections:* The legislation should specify a set of baseline requirements that the requests made under this system should meet. These should include, at a minimum, a requirement that the requests be made by an independent and impartial adjudicator; be targeted to a particular person, account, or device; be narrowly tailored as to duration; and be subject to robust minimization requirements to protect against the retention and dissemination of non-relevant information;

(iii) *Transparency and Accountability Measures*: The legislation should mandate that the partner government publish reports regarding the number, type, and temporal scope of the data requests they issue under this framework. (The United States would similarly need to agree to do the same with respect to requests made of foreign-based providers.) The partner government should also be required to comply with regular assessments designed to evaluate compliance with these requirements; and

(iv) *Sunset Provision*: The legislation should specify that any such agreement sunset after a set period of years, absent an assessment that the requisite procedural and substantive requirements have been met.[11]

These requirements are both essential and justified for at least two key reasons. *First*, while the targets of foreign government requests under this system will be foreign nationals that are located outside the United States, communications are inherently intermingled. It is likely — in fact almost certain — that such requests will at times lead to the incidental collection of U.S. citizen data and data of other persons physically residing in the United States. This reality provides both an opportunity, and arguably an obligation, for Congress to demand a minimal set of baseline standards to protect those persons that fall squarely within its responsibility and authority to protect.

Second, these types of agreements provide the United States with a unique opportunity to begin to set the contours of global privacy rights and at the same time promote Internet security. The United States is often in the position, via its annual State Department Human Rights reporting and a myriad other diplomatic channels, of exhorting other countries to improve human rights standards and protect free expression. The United States now has a rare opportunity to couple such exhortations with an attractive carrot. Countries need only meet the specified standards in order to get access to data in legitimate cases. It thus provides an opportunity for the leveling up, rather than the leveling down, of protections for all.

Additional Issues

Mutual Legal Assistance Reform. At least initially, only a handful of countries may be in a position to meet the specified requirements. And even those that do still will need to employ the mutual legal assistance system if they seek data of U.S.-located persons, as well as U.S. citizens and legal permanent residents, wherever located.

There is thus an ongoing need to update and streamline the mutual legal assistance system, and I applaud the efforts of many members of this Committee who have advocated for reforms such as the creation of an online system for tracking foreign government requests. Additional resources are needed to facilitate more efficient and

[11] For a further elaboration of these principles, *see* Jennifer Daskal & Andrew K. Woods, *Cross-Border Data Requests: A Proposed Framework*, JUST SECURITY, Nov. 24, 2015, https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/.

expeditious handling of such foreign government requests — requests that will only increase over time as more and more evidence becomes digitalized.[12]

Wiretap Authority. The U.K. also wants the authority to compel U.S. provider assistance with live intercepts of data transiting through the United States and/or controlled by U.S.-based providers. And in fact, the draft U.S.-U.K. agreement, as reported, covers both stored communications and live intercepts. If enacted, U.K. law enforcement would be permitted to directly compel U.S.-based providers to assist with live intercepts. But this, too, would require Congressional action, in the form of an amendment to the Wiretap Act.

In considering this possibility, it is worth clarifying a few points. The *Washington Post* characterizes this possibility as the Brits "com[ing] to America,"[13] but this is not an accurate description of what the U.K. seeks. The agreement would, at least according to the publicly available information (and according to anything that Congress would reasonably authorize), be limited to U.K. wiretap orders for foreign national targets located outside the United States. It would allow, for example, the U.K. to compel a U.S.-based provider to assist with the real-time monitoring of a live chat between two U.K. nationals who are located in London and are suspected of plotting a terrorist attack on Big Ben. It would *not* permit the U.K. to wiretap persons located in the United States, or U.S. citizens or U.S. legal permanent residents wherever located. Nor should it.

It would, however, operate as a *new* authority. Currently, foreign governments can get access to U.S.-held stored content; they just have to use the laborious and inefficient MLAT system. No such mechanism exists for foreign law enforcement to directly compel the production of live intercepts from U.S.-based providers. And while U.S. agents may assist the U.K. — or other foreign governments — in certain circumstances (such as in the course of a joint venture), wiretap applications under U.S. law are subject to much more rigorous court review and minimization requirements than the requests for stored communications.

These historical facts are important, and suggest the need for caution — or at least further inquiry and the possible implementation of additional protections — prior to amending the Wiretap Act. That said, the history should not be decisive. The line between live and stored communications is increasingly blurred. And depending on the details, prospective time-limited intercepts can be much less intrusive than the acquisition of stored content over a much longer time frame. More information about the full range of communications and types of orders that might be subject to such an agreement is needed.

---

[12] *See, e.g.*, Andrew K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, GLOBAL NETWORK INITIATIVE (2015), http://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf [http://perma.cc/PA6M-XVLZ] (suggesting a range of useful improvements to the mutual legal assistance system); *supra* note 3, THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES at 226-29 (Dec. 12, 2013) (suggesting ways to improve the mutual legal assistance treaty process).

[13] *See, supra*, note 1.

Transactional Records. Notably, the SCA's blocking provision applies only to content. Transactional records (or what the international community calls "traffic data"),[14] including to/from lines in emails and location data, and other non-content data can be provided directly to foreign governments. Transparency reporting suggests that non-content data is in fact turned over to foreign governments in large numbers.[15]

But whereas there is a range of non-content data that U.S. officials can only obtain through a court order, based on a finding of "specific and articulable facts showing that there are reasonable grounds to believe that the [data] sought, are relevant and material to an ongoing criminal investigation,"[16] no such analogous standard applies to foreign government requests — even when seeking data of U.S. citizens and persons located in the United States. This suggests a need to limit foreign government access to such data, particularly in instances when foreign governments are seeking information about U.S. citizens, legal permanent residents, and others located within in the United States.

The Microsoft Case and the LEADS Act. The precise converse of the issues I have described above (with respect to foreign governments seeking access to U.S. held data) are playing out in the pending *Microsoft* case now before the Second Circuit. In that case, the U.S. government is seeking data held outside the United States. Specifically, the government is seeking to compel the production of emails controlled by Microsoft, but stored in Dublin, Ireland. Microsoft objects on the grounds that the U.S. government's warrant authority does not have extraterritorial reach, and that the United States should make a direct request to Ireland for the data, via the MLAT in place between the United States and Ireland.

As I have argued elsewhere, both positions are flawed.[17] The United States is asserting a very broad theory of its jurisdictional reach over data; so long as it has jurisdiction over the provider it can compel production of data, wherever located, and without regard to the nationality or location of the target. This is the exact converse of the authority claimed by the U.K. — an authority that the United States rightly rejects.

Microsoft, in contrast, is unduly focused on data location as the key criterion for establishing warrant jurisdiction. According to Microsoft, the government can only

---

[14] *See, e.g.*, Council of Europe Convention on Cybercrime art. 1(d), opened for signature Nov. 23, 2001, S. TREATY DOC. NO. 108-11 (2006), E.T.S. No. 185 (entered into force July 1, 2004).

[15] *See, e.g.*, *Microsoft Transparency Hub, Law Enforcement Requests Report Jan-June 2015*, https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/lerr/ (indicating that Microsoft received approximately 30,000 foreign government requests for data between January and June 2015 and disclosed non-content data in response to about 10,000 such requests); Yahoo! *Transparency Report: Government Data Requests*, https://transparency.yahoo.com/government-data-requests/index.htm, (indicating that Yahoo! received approximately 10,000 foreign government requests for data between January and June 2015 and disclosed non-content data in response to about 4,500 such requests).

[16] 18 U.S.C. § 2703(d) (2012).

[17] *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015); Jennifer Daskal, *The Microsoft Warrant Case: The Policy Issues*, JUST SECURITY, Sep. 8, 2015, https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues/.

compel production if the *data* is located within the United States. But this position both fails to account for the unique attributes of data and further incentivizes concerning data localization requirements. Data is, after all, highly mobile, potentially divisible, and, thanks to the cloud, often held in locations disconnected from — and perhaps not even known to – the data user, the person with the primary privacy interest in the data.[18] It thus makes little normative and practical sense for law enforcement jurisdiction to turn on where data happens to be located at any given time.

As a result, Congressional action is needed regardless of who wins the case — as the Second Circuit urged and many members of the committee have already recognized. The pending Law Enforcement Access to Data Stored Abroad Act (the LEADS Act),[19] which was introduced by Representative Tom Marino and is co-sponsored by several members of this Committee, offers one possible attempt to do so and is definitely a step in the right direction. It is very encouraging to see so many members engaging on this important issue.

That said, I worry that the LEADS Act as currently drafted, retains too heavy an emphasis on the location of data, as opposed to other — and in my view preferable — criteria for establishing the scope of warrant jurisdiction. An emphasis on data location runs the risk of entrenching data localization movements and also creates a set of odd anomalies (whereby the ability of the United States to access the data of a foreign national residing in and engaging in criminal activity within the United States would turn on the place where the data is stored).

Consistent with the above-stated approach to the U.S.-U.K. agreement (or any other equivalent agreements that are subsequently negotiated), it would be preferable for warrant jurisdiction to turn on the location and nationality of the target — rather than the location of data. Among many other benefits, such a standard sets the stage for exactly the kind of international agreements that Congress should be encouraging.

***

To sum up, the system for responding to law enforcement's interest in data across borders is broken. The United States has both an opportunity — and in my view a responsibility — to build a future system that simultaneously tracks American values, protects American businesses, safeguards Americans' privacy, and promotes the growth of an open and secure Internet. The fact that the United States and U.K. are talking is a positive step forward. It is now up to Congress to authorize the executive branch to enter into such agreements, but also to ensure that they are done right.

Thank you for the opportunity to testify. I look forward to your questions.

---

[18] *See, supra*, note 13, *The-Unterritoriality of Data*, 125 YALE L.J. at 365-378.

[19] The Law Enforcement Access to Data Stored Abroad (LEADS) Act, H.R. 1174, 114th (2015).

Mr. GOODLATTE. Thank you very much, Ms. Daskal. We will now begin a round of questioning and I will recognize myself. Mr. Smith, let me follow-up on what Ms. Daskal just said, because that seems to get right to the crux of what has held up here in this process. So Microsoft supports international agreements that will address and overcome conflicts of law, but these agreements are likely going to allow foreign countries to acquire data held by U.S. companies on a standard less than probable cause. Do you support this, and if so, why?

Mr. SMITH. Well, first of all, I would like to agree with the testimony that you just heard. I think we do need legislation. We do need international agreements, but I also believe that any international agreements that are negotiated should absolutely ensure that the rights of Americans are protected by U.S. law and the Constitution, including the probable cause requirement.

Mr. GOODLATTE. How does allowing foreign countries to obtain data from U.S. companies on a less than probable cause standard square with the call for a uniform probable cause standard for requests by the U.S. Government?

Mr. SMITH. Well, if the question is to me, I think the answer is two-fold. First, there will be benefit over time if the world can move toward a more uniform standard. But I think between now and then, the most important thing is that people have the protection of their own rights by their own law. I think that is fundamentally what most people in most countries want, and I think that is what Americans want for their own rights as well.

Mr. GOODLATTE. Ms. Daskal, do you want to respond to that?

Ms. DASKAL. I fully agree.

Mr. GOODLATTE. Okay, well, so I am not quite sure I understand. If they are protected under their own laws, but their own laws do not have the same high standard of protection, and they are coming to the U.S., how are we going to have the carrot that you just referred to in your testimony to incentivize countries to provide greater protections?

Ms. DASKAL. Sure, so that the suggestion that I was making is that when Congress authorizes these agreements, that it specify certain requirements that the country must meet, both at the country level and at making specific requests for that——

Mr. GOODLATTE. Would those be the standards contained in U.S. law?

Ms. DASKAL. So, my suggestion would be for Congress to write in the amendment to the Stored Communications Act an exception to the blocking provision that basically says, "The executive has permission to enter into bilateral and multilateral agreements with foreign countries when the following conditions are met." And some of those conditions should specify minimal standards that the requests have to meet.

Mr. GOODLATTE. But not necessarily U.S. standards?

Ms. DASKAL. Not necessarily U.S. standards——

Mr. GOODLATTE. Okay, I got it. All right, good. Then you are in agreement. Should a bilateral agreement—I will direct this back to you, Mr. Smith—should a bilateral agreement, such as the one under consideration with the U.K. also ameliorate any conflicts of law with regards to U.S. requests for data held by U.S. companies

in that country? Would this not resolve the issue currently being litigated in the Second Circuit?

Mr. SMITH. It would resolve the issue that is being litigated in the Second Circuit if the bilateral agreement were between the United States and Ireland. And I think what your question points to in part, is that if a model that works can be created between two countries, then there is an opportunity to replicate it elsewhere, but it will need to be replicated.

Mr. GOODLATTE. And do you see any conflict between your position as it relates to foreign government access to data stored in the U.S., and your position as it relates to U.S. Government access to data stored abroad?

Mr. SMITH. I believe that if you put an international agreement in place, that resolves any potential conflict. It creates the means by which two governments together, and respect the rule of law.

Mr. GOODLATTE. Well, I get that, but it seems to me that if we agree to their standard, they agree to our standard, you still have two different standards that are in place.

Mr. SMITH. But I think it really speaks to an important point. I think the American people want to have their rights protected by U.S. law. I was in London last week. I think the British people want to have their rights protected by British law. We need governments that have—I will just say a like-minded approach. It does not mean that they have to agree on every particularity though.

Mr. GOODLATTE. Ms. Daskal, the rules established under ECPA govern what a U.S. provider can and cannot do with both communications content and non-content records. The result is that the ECPA procedures, including the warrant requirement apply to any customer of a U.S. provider regardless of that customer's nationality or location and regardless of where the data is stored. Why is this insufficient to protect the privacy interests of all U.S. provider customers including foreign customers?

Ms. DASKAL. So, I absolutely think that the answer to the question of the warrant's requirement for content is necessary and it is an important privacy protection for when the United States is accessing data, but that is not really the issue here.* The concern is not about insufficient privacy protections; the real concern is about this really significant conflict of laws which over time is going to lead to an increasing number of things, like increased data localization, increased unilateral assertions of extraterritorial jurisdiction, other means of getting around these restrictions. And so that is where the privacy concerns come in, not because of the warrant requirement, which is a great requirement, but about what other countries are doing in response and what happens as a result of these conflicting obligations.

Mr. GOODLATTE. Thank you. The Chair recognizes the gentleman from Michigan, Mr. Conyers, for his questions.

Mr. CONYERS. Thank you, Chairman. Mr. Smith, it is important for technology to protect both privacy and security. Can policy pro-

*__Note:__ The witness amends her response as follows:

So, I absolutely think that a warrant requirement for content is necessary and is an important privacy protection when the United States is accessing data, but that is not the issue here.

posals being considered today do both, or do they pit one against the other?

Mr. SMITH. I think there are times when these two fundamental values, privacy and security, might be intentioned, but I think there are many times when creative and new laws that are designed for 21st century technology can move privacy and security forward together, and that is what we need to strive to do.

Mr. CONYERS. Secretary Chertoff, do you have any additional comments on that same question?

Mr. CHERTOFF. No, I agree. I think that actually, although occasionally, there is tension between the two, in many instances, you cannot really have privacy without security, and the value of security without privacy is much diminished.

Mr. CONYERS. Thank you. One last comment from Mr. Smith from me—with respect to the Microsoft case pending in the Second Circuit, why has there been challenged the government's demand for data stored in Ireland? What is your goal, or what is the corporation's point in that case?

Mr. SMITH. I think fundamentally, we believe that people need to be able to trust the technology they use. And part of their ability to trust the technology they use turns on confidence that their rights, people's rights are going to be protected by their law. We store emails in data centers that are close to our customers. So, for example, when we have customers in the European Union, we store their data, their emails in our data center in Dublin or in Amsterdam. Our concern is that the U.S. Government first is using power that Congress never gave it. Namely, the power to go around the world to vacuum up emails pursuant to a U.S. search warrant.

And second, our concern is because the U.S. is exercising this type of extraterritorial power on a unilateral basis, it is in effect saying, in this case, to the people of Ireland that their law does not matter; the DOJ does not even need to read it; it does not need to consult with the Irish Government; it does not need to pay any attention to the mutual legal assistance treaty in place between the U.S. and Ireland. All it has to do is turn to an American technology company and apply a power under U.S. law. That is not a recipe for the success of the U.S. technology sector, and it is not a recipe for ensuring people have trust in technology.

Mr. CONYERS. Thank you. For Mr. David Kris—and I might ask Ms. Daskal to both consider this: I think a bilateral agreement framework could be a useful tool in resolving some of the conflict of laws issues that have been discussed here today. But there remain concerns, for example, about how we will reconcile British law with our own legal customs. How will we make sure that privacy, due process and human rights are respected by our partners in these agreements?

Mr. KRIS. That is an excellent question and issue to raise. I am confident that Congress will have a role because even if the United States and Ireland or any other country reach an executive level agreement, for that agreement really to take effect, Congress will need to amend the blocking provisions, as Professor Daskal has referred to them, in the Stored Communications Act.

And it will be, I think, up to you and incumbent on you as a Congress to decide which categories of cases involving what kind of,

say, defendant, non-U.S. persons located abroad have been discussed, such that U.S. persons, or persons in the United States would not be subject to the exemption. Different kinds of crimes exempting political crimes from this provision, for example, various other limits are all possible. And Congress will have an opportunity to consider those, if and when it decides to amend the Stored Communications Act to permit this kind of direct access by way of executive agreement in some specified subset of cases that meet with your policy approval.

Mr. CONYERS. Ms. Daskal, would you add anything?

Mr. ISSA [PRESIDING]. Go ahead, Mr. Ranking Member.

Mr. CONYERS. Thank you.

Ms. DASKAL. So, yes, I agree with all that and I would just—I think it is worth emphasizing that the agreement, as it was explained to us this morning, and I think as Congress should sort of adopt as parameters as well, would solely permit a foreign government to get access to non-U.S. person data and data of people who are not in the United States.** So, we are talking about the Brits being able to get data on their own citizens in connection with the investigation of a local crime.

And Congress, I think, because we are talking about U.S. providers, has a role to play in setting some minimal standards, some minimal important procedural and substantive standards as to what the Brits must do in order to get access to that data from U.S.-based providers. But we are not talking about the British requesting data about American citizens, American permanent residents, or Americans in the United States.

Mr. CONYERS. Thank you all for your responses, and I thank you, Mr. Chairman.

Mr. ISSA. Well, thank you, Mr. Conyers. We now go to the distinguished gentleman from Texas, Mr. Poe.

Mr. POE. I want to thank the Chairman. Thank you all for being here. I, being a lawyer, I did not go to Harvard, but I went to the University of Houston, which we call Harvard on the bayou fondly in Texas. But, Mr. Chertoff, it is great to see you again. Thanks for your service to the country that you have done in the past.

Mr. Smith, I am impressed by your statement. Passionate and you did not read it, so it is obvious that this is important to you. It is important to the country. This, by way of kind of review, ECPA, 30 years old. It would seem to me that we have known for a long time that ECPA law needed to be reformed. And 30 years is long enough for Congress to finally pick a horse and ride it and make some choices and changes in the law to solve the problems that all of you have discussed; whether it is nationally; whether it deals with business; whether it deals with foreign countries; the information; do you think it is about time that we make a decision on reforming ECPA?

Note: The witness amends her response as follows:

So, yes, I agree with all that and I would just—I think it is worth emphasizing that the agreement, as it was explained to us this morning, and I think as Congress should require as part of the adopted parameters, would solely permit a foreign government to get access to non-U.S. person data and data of people who are not in the United States. So, we are talking about the Brits being able to get data on their own citizens in connection with the investigation of a local crime.

Mr. SMITH. I think that the time has come and it is perhaps even overdue. I think what you are really hearing from all of us today and you hear it from the tech sector every day, is that we really do need a new law, and we need Congress to write it.

Mr. POE. And it should be Congress' responsibility to set the standard of law rather than letting the courts make the determination as to what the expectation of privacy is for citizens, or corporations, or letting the Justice Department take the law as they see it and interpret it the way they see it. Congress needs to weigh in and make these decisions and make it the law of the land. I mean, that is our responsibility.

Mr. SMITH. Absolutely, and I think, frankly, one of the points that we have heard this morning that should give all of us the most concern is the acknowledge by the Justice Department that the Stored Communications Act passed in 1986 is silent on whether the DOJ has the authority to apply these search warrants worldwide. And the DOJ says, that because Congress was silent, the executive branch has power. Well, that basically amounts to an argument that Congress needs to write really long laws, because every time Congress neglects to address something, it is giving Congress—it is giving the executive branch some power. That is not the way the Constitution was written. That is not the way common sense works.

Mr. POE. There you go. I agree with that. And the Justice Department, they are doing what they think they can do under the law, and I think they are wrong, but ECPA was written to protect privacy of individuals. That is the purpose of the law, why it was written. So, Congress needs to weigh in on it, pass legislation that has been pending for a long time. I think we set the standard for the expectation of privacy. It should be up to us, not some judge or group of judges, and we need to move on with that. Set aside those comments, and tell me the economic impact of not making a decision, and how that is affecting industry.

Mr. SMITH. I think there are two ways to think about this. One is narrow, one is broad. They are both important. First, because we are seeing this emerging conflict of laws, we are seeing the risk of increasing fines on U.S. companies when we get into these conflicts. Already to date, Microsoft has been fined $28 million by the Brazilian authorities because of this——

Mr. POE. And that is a criminal fine. That is not a civil fine. That is a criminal crime.

Mr. SMITH. Right, yes. This is all connected to a criminal proceeding, and we are being fined simply for obeying U.S. law, and think about a start-up and what $28 million means. But the implications are really broader because I find, in countries like Germany and the United Kingdom, where I was last week, I increasingly meet people in government and elsewhere who say that unless this issue is resolved—they basically say, "Unless you win your case in New York, we are not going to be able to trust American technology and we are not going to be able to move our content to the cloud when the cloud is operated by a U.S. company with a data center." So, a lot is at stake for the American economy and American jobs.

Mr. POE. Well, I appreciate all of you being here. I do not have time to ask the rest of you questions. But I think you are exactly correct. For the problems that you have all mentioned, it is time for Congress, like I said, to pick a horse and ride it and let us pass some legislation to fix this problem. And I yield back.

Mr. ISSA. I thank the gentleman. We now go to the gentlelady from San Jose, Ms. Lofgren.

Ms. LOFGREN. Thank you. Before my questions, I would ask unanimous consent that we put into the record the Yale Law Journal article by our witness, Ms. Daskal.

Mr. ISSA. Without objection, the document will be placed in the record.

Ms. LOFGREN. Thank you. This has been a very interesting hearing and, comes at interesting time for our country, because the issues we face are of law, but also of technology. And I do not think we can talk about the legal issues without getting into the technology issues. And I was looking at the Trans-Pacific Partnership Agreement. Now, some of us have issues about human rights in Vietnam, you know, health issues and the like, but in terms of encryption, it is pretty clear.

It basically says that you cannot require a backdoor, an encryption, if you are a party to this agreement. It prohibits governments from requiring companies to either disclose their keys or to use specific cryptographic algorithms. And the Department of Justice's application and courts' subsequent decision to compel Apple to provide special software circumventing security protections would actually violate this international norm, that is specified in the TPP, against government mandates for backdoors. But also, we had several votes here in the House of Representatives where we had over two-thirds of the House vote in opposition to backdoors.

So, I am wondering, Mr. Smith, if I could ask you, what is Microsoft's view of this? Do you support the position that Apple has taken, that the court is setting a dangerous precedent by forcing Apple to break its own security protections? Does Microsoft plan to be involved in the litigation that apparently is going to go on for a while? I know Mr. Gates said something, but he has been gone from the company since—for a long time. I am just wondering what the—Microsoft's position is, if that is fair to ask?

Mr. SMITH. Yeah, we at Microsoft support Apple, and we will be filing an amicus brief to support Apple's position in the court case next week. And I believe that Apple is making an important point that, in fact, connects directly with the kinds of issues that are being considered by this hearing today.

In the Apple case, the Justice Department has asked the magistrate to apply language in the All Writs Act that was passed by Congress, and written in 1911. The leading computing device of that era is right here in front of me. It is an adding machine that went on sale in 1912. Quite simply, we do not believe that courts should seek to resolve issues of 21st century technology with law that was written in the era of the adding machine. We need 21st century laws that address 21st century technology issues, and we need these laws to be written by Congress. We, therefore, agree wholeheartedly with Apple that the right place to bring this discus-

sion is here, to the House of Representatives and the Senate, so the people who are elected by the people can make these decisions.

Ms. LOFGREN. Well, thank you very much, and do you have any other props?

Mr. SMITH. No, not props.

Ms. LOFGREN. I was surprised to see that, but——

Mr. SMITH. But believe me, it is amazing what you can buy on the internet.

Ms. LOFGREN. Well, I have heard that——

Mr. ISSA. Would the gentlelady yield?

Ms. LOFGREN. If I can get——

Mr. ISSA. What is the operating system on that?

Ms. LOFGREN. What is the operating system?

Mr. POE. It is called a hand crank.

Ms. LOFGREN. I would like to follow up because I actually very much believe that the encryption issue should be before Congress. The Judiciary Committee has started that process, but the Justice Department alleges that this is just one phone, and I was surprised to hear that when we heard the district attorney in New York saying he had 175 phones and then we found out there were a number of others where we are seeking to utilize the new operating system that the court has ordered Apple to devise. Do you think that this issue goes beyond that one phone?

Mr. SMITH. Well, every case is obviously about one case, but every case obviously has implications for lots of other cases. The real concern here is actually the law and the implications for the future. And the only way to get the law right for the future is for Congress to act.

Ms. LOFGREN. If I can just close, Mr. Chairman, I started with the TPP, the international standard, and that is important because encryption keeps us safe. It keeps people from breaking into our data systems and causing problems for us. The either hackers or terrorists or enemies of our country and I—the idea that my data would have to be opened to hackers in China because of specific cases is really what I think this is about, and I thank you very much, Mr. Smith, for answering.

Mr. ISSA. I thank the gentlelady. We now go to the gentleman from Pennsylvania, Mr. Marino.

Mr. MARINO. Thank you, Chairman. Secretary Chertoff, you mentioned a term, legal regime, in your opening. Would you expand on that? And do you mean legal regime, meaning legislation, or an expansion of MLAT, or something else, or a combination?

Mr. CHERTOFF. I really principally meant legislation, because as I think we also started a discussion about encryption, in order to make decisions about how to structure a legal architecture, when you are dealing with global data, different forms of citizenship and evolving technology, I can tell you having been a judge, the courts are not equipped to weigh all of those things, and the unintended consequences of a decision are often not clear in an individual case. So, to me, this cries out—I know Chairman McCaul suggested a commission to look at the issue of encryption, but to me, this cries out for taking a comprehensive look at the way the technology actually exists in the real world, and how one can then reconcile the

need to preserve privacy and the need to promote security with that technological background.

To give you one example, you know, 100 years ago, when they first invented telephones and photography, initially the courts tried to deal with the issue of the Fourth Amendment by forcing the facts into those old rules about not searching someone's houses. So, we had the trespass cases. And finally, in some of the more recent cases, the court said, "Wait a second. This is about expectation of privacy." It is not just about whether I physically invaded a room or wire. And I think we need to have that kind of technologically-informed discussion now.

Mr. MARINO. Thank you. Mr. Smith, what do you do in a situation when you have conflicts like you have explained, as far as advising your employees on how to approach these matters?

Mr. SMITH. Well, it is really a terrible situation that we are being put into. I thought Chairman Goodlatte put it well at the outset when he referred to it as a Hobbesian choice. Imagine the kind of meeting that I have had to have with a Brazilian employee who is being prosecuted. And imagine trying to talk about the fact that we cannot, in fact, take the steps that would bring the prosecution to an end in Brazil, because it would require that we commit a felony in the United States. This is a classic example, I think, of the fact that we need governments to act, and we need our own government and we need this Congress to act, perhaps most of all.

Mr. MARINO. Thank you. Ms. Daskal, referring back to the secretary's atement on legislation, do you agree with that, or do you see a combination of varieties of treaties and legislation, or just the legislation?

Ms. DASKAL. So, again, it depends on the specific issue, but with respect to the problem of conflicting laws, there absolutely needs to be legislation.

Mr. MARINO. Good.

Ms. DASKAL. Because the executive does not have the authority to enter into the kinds of agreements that are needed without Congress authorizing it and ideally setting parameters as what those agreements look like.

Mr. MARINO. Thank you, and Mr. Kris, would you expand a little bit on the two points you raised in the FISA gap?

Mr. KRIS. Sure. Again, I would love to be wrong on this. I mean, I do think you should have a conversation with the executive branch, but the jurisdiction and the reach of the FISA statute depend fundamentally on the definitions of electronic surveillance and physical search in the statute itself, and those are very, very complex. But I am concerned that given the way those definitions are written, the statute cannot currently be used to compel the production of data stored abroad; for example, the kind of situation we have in the Second Circuit case involving Microsoft.

If the target of the surveillance is either a U.S. person located anywhere, or a person of any nationality located here, in either of those situations, I am concerned that the statute cannot be used to issue a compulsion order to a provider to turn over the data, and the government has to rely on a voluntary repatriation of the data back into this country to bring it within the jurisdiction of the statute.

Mr. MARION. Thank you. I yield back.

Mr. ISSA. Gentleman yields back. With that, we go to the gentlelady from Texas, Ms. Sheila Jackson Lee.

Ms. JACKSON LEE. Thank you very much. I noticed in the course of materials that I have here that—oh, first of all, let me thank all the witnesses for their testimony. And I take note of the fact—and I want to ask Mr. Smith and Mr. Chertoff on this; that the issue at the European Union had been an outstanding issue for a period of time in terms of data and data protection, privacy. And just recently the U.S. data transfer pack was agreed to.

Can both of you comment on what impact as we are discussing legislation, the LEAD Act, and where are in the having not acted, what that agreement does for you, even if it is sort of around the ring of what we are discussing? Mr. Smith first.

Mr. SMITH. Yeah, well thank you for asking that question, congresswoman, because it actually raises a very important point that we have not talked about yet today. You know, the recent Safe Harbor negotiation I think, you know, put a Band-Aid on a legal system that has been in existence since the year 2000 and, therefore, it appears the data will continue to be able to move across the Atlantic. But time and time again, to this morning you heard Mr. Bitkower talk about whether there is or is not a conflict of laws across the Atlantic. The key thing we need to think about here is that the new European Union General Data Protection Regulation will take effect in 2 years. And that regulation has an article, Article 43A, that will make it unlawful for a company to move data out of Europe to comply with a search warrant unless it is done pursuant to an international legal agreement or process.

So in 2 years, a legal curtain is going to descend across the Atlantic. There is going to be a conflict in every one of these cases the Justice Department wants to pursue on a continent that has 508 million people living on it, unless action is taken to put new international agreements in place.

Ms. JACKSON LEE. And so that would be aside from a statute here in the United States. It would be additional international agreements.

Mr. SMITH. Basically what it means, I believe, is that we have 2 years to try to figure out how to craft an agreement, as we are trying to do with the United Kingdom, get legislation in Congress, and then determine how and whether to replicate that with the other countries in the European Union; so we do not have a day to waste.

Ms. JACKSON LEE. Sense of urgency; Mr. Chertoff, thank you for your service as Homeland Security secretary. So, I am going to add a subset to the question is to reflect on the international agreements, but also reflect upon the crucial question of privacy and security in the backdrop of what we are facing now. And Microsoft case represents—even the case was a criminal case we have, as an ongoing looming issue, is at least a dialogue or the issue of Apple. But can you, from your perspective, speak to how we have a number of factors that are impacting on our decision for the legislation and our exchange on data?

Mr. CHERTOFF. Yeah, well thank you. And again, it is a pleasure to appear before you again. I agree with what Mr. Smith said about

the need to particularly work out an agreement with the Europeans, because they have typically been, at least some of the countries there, the most reluctant to cooperate in these areas. And yet the urgency of doing that cooperation now is more evident than ever when you look at what happened in Paris.

So we ought to move forward with that. I think in general also, though, there are a series of issues which require us to think in a little bit more of a technologically savvy way about how we deal with data. And to go back to Congresswoman Lofgren's point on encryption—I am a real believer that it would be a mistake to legislate a requirement to create backdoors or duplicate keys or other limitations on the ability to have ubiquitous encryption. Because I know that encryption is one of the key tools that we use to protect innocent people against criminals or, for example, the North Koreans getting into your data. And to sacrifice the security of the many in this instance seems to me to be not worth it, particularly because I am quite confident that the bad guys can find tools overseas that are going to wind up allowing them to encrypt anyway.

But, again, this is an area where I think—I know there is a litigation going on now. For a court to be asked to make or resolve this decision strikes me as the wrong way to go about it. This is something that requires looking end to end at what the problem is in trying to reconcile what—I do not think they are inevitably contradictory impulses. But what I think are impulses that need to be coordinated and synchronized so we do not go too far in the direction of handicapping security, and too far in the direction of handicapping privacy.

Ms. JACKSON LEE. Mr. Chairman, thank you very much. Mr. Chairman, can I sneak in one question for Mr.——

Mr. GOODLATTE. Quickly, because we have just enough time for each Member to have 5 minutes before our hard stop at 1:30.

Ms. JACKSON LEE. In answer to Mr. Chertoff, the LEADS legislation does lay out a process. What is your comment on the statutory fix for this issue? Did you hear me?

Ms. DASKAL. Yeah, yes.

Ms. JACKSON LEE. Yeah, thank you.

Ms. DASKAL. So I think the fact that the Congress is engaging with LEADS is a terrific step forward. I do have some concerns about LEADS as currently written in the way that it makes jurisdiction turn on the location of data, which I think has all kinds of practical and normative problems, because of the way data moves around so quickly, because of its divisibility, because of the fact that oftentimes when we store things in the cloud we do not even know where it is located at any given time. So making jurisdiction turn over where our data is does not seem to make a lot sense. That said——

Mr. ISSA. Thank you. I am afraid we are going to have to cut you off but——

Ms. JACKSON LEE. I think you and I thank the Chairman.

Mr. ISSA. Thank you.

Ms. JACKSON LEE. I thank the witnesses.

Mr. ISSA. Young lady from California, Ms. Walters.

Ms. WALTERS. Thank you, Mr. Chairman. Mr. Smith, your testimony describes Microsoft's dilemma with the Brazilian Govern-

ment seeking disclosures that would blatantly violate U.S. law. And I am sure that legal predicaments like this will only increase as governments enact laws that create additional conflicts. These legal quandaries undoubtedly have negative impact on Microsoft as well as other tech companies, and ultimately impair a vital sector of the American economy. And I know Mr. Poe had asked this question, and you had discussed the fines levied against Microsoft. But I wanted to give you additional time to discuss how this situation has impacted your global customer's willingness to trust Microsoft products, and what it has done to your business.

Mr. SMITH. Well I think more than anything else, congresswoman, your question, which is very important, just underscores, first of all, the importance that people would be able to trust technology. We are all putting so much of our most sensitive information on devices and in the cloud that people, by definition, only want to use technology they can trust.

So the fundamental question that people around the world are asking is whether they can trust American technology. You know, we face this as one American company but I think this is a question that every American company is having to face. And there are a variety of steps we are trying to take to address it, we are being more transparent ourselves; I think that is a good thing. We are taking steps to advance privacy, to address and advance encryption; I think that is a good thing. But at the end of the day, the concern that I hear around the world is that regardless of what we do, the U.S. Government may use its long arm to reach unilaterally across borders and without regard for other countries' laws.

So we need to fix that part as well. We obviously need to do it in a way that ensures that law enforcement can do its job; that is why these kinds of new agreements are needed.

Ms. WALTERS. Yeah, thank you. And then I have a question for the entire panel. What does the internet look like if we do not act and data localization becomes the norm?

Mr. CHERTOFF. I do not want to be overdramatic but you do not have an internet. You have a series of internets or intranets in individual countries. And so much of the value of the internet, which is the ability to operate on a global basis, is hampered. It also means that from an engineering standpoint some of the considerations that you have when you put a server in a particular place gets subordinated to issues about how to manage the legality or kind of legal arbitrage from one jurisdiction to another.

Ms. DASKAL. I would just add as well I completely agree. But I think the other piece of this that is important is when that happens, the United States no longer has a role to say in terms of what protections do or do not apply when a country is getting access to data. And so that is why this opportunity to enter into agreements and to set at least some parameters is a really important opportunity for the United States to engage, to set the parameters, and to do so in a way where the world is still talking to each other.***

***Note:** The witness amends her response as follows:

And so that is why this opportunity to enter into agreements and to set at least some parameters is a really important opportunity for the United States to engage, to set the

Mr. SMITH. And the last thing I would mention is the consequence of that kind of data localization trend and set of requirements is that computing gets more expensive, because it forces companies to build more data centers than, frankly, the world needs just so you can have a data center in every country. That costs money; that is going to lead to higher prices.

Ms. WALTERS. Okay, thank you, I yield back. Do you have anything to add, Mr. Kris? No. I yield back, thank you.

Mr. ISSA. I thank the gentlelady. We now go to the gentleman from Georgia, Mr. Johnson.

Mr. JOHNSON. Thank you. Since we have veered down the road of encryption, and it being a fact that encryption keeps us safe from hackers and garden-variety criminals, we also have this issue of a ungoverned space that is created by encryption; a ungoverned space wherein terrorists can conspire with impunity.

So, you know, on one hand, we have encryption that helps keep us safe from hackers, but then we also have encryption that helps keep terrorist conspirators safe from discovery. And then we have the issue of international competition companies, multi-national corporations, multi-national companies competing in an international market for customers with privacy, or encryption, being a selling point. And this is quite interesting.

It can cause a lot of fear in the minds of people concerned about law enforcement, concerned about intelligence, international intelligence. And so we see where we have gotten to the point where technology has exceeded the capacity of law enforcement, both internationally and domestically, to be on top of the situation which leads us into an area of anarchy, lawlessness. Encryption, Mr. Chertoff—you have talked about the fact that it protects us from hackers. What is your view about terrorists who are able to conspire with impunity in that environment?

Mr. CHERTOFF. Well, Congressman, this is a—look, this is a serious issue, and I take the concerns of the FBI and the law enforcement community very seriously; I understand why this worries them. I guess my response is this: First of all, I know that even if Congress says that companies or items—companies that manufacture items here have to create backdoors or duplicate keys, people who want to do bad things will find devices that do not have backdoors or duplicate keys.

I point out to people that the so-called dark web, where a lot of criminal activity goes on undetected because it is all anonymized, is powered by the Onion Router Tor, which was actually funded by the United States Government as a way of providing anonymity for people who were dissidents. The second thing I would say is that it has always been the case, and I go back in my years of doing law enforcement, that bad people were able to communicate with each other without being detected.

In the old days when we were doing mob cases, they would either turn the radio way up so the listening device could not record it, or they would take a walk around the block. And we nevertheless succeeded in putting a lot of those folks in jail.

---

parameters, and do so in a way that protects our privacy, security, and economic interests.

And the third thing I would say is that actually, if you look at the technology that exists nowadays, and the amount of metadata that is generated that is not encrypted, I would venture to say that from the intelligence and law enforcement standpoint, the ability to detect terrorism now is fantastically better than it was even 15 years ago when, in the wake of 9/11, we were trying to hunt down terrorists in this country.

So, as with all technologies, there are elements of it that are problematic for law enforcement, but there are elements that help law enforcement, and I still think the balance favors our security.

Mr. JOHNSON. Thank you. I do not have anyone on the panel to ask if they would disagree with that, I assume. So with that I will yield back.

Mr. ISSA. And with that I would recognize the gentlelady from Texas for unanimous consent.

Ms. JACKSON LEE. Mr. Chairman, thank you and the Ranking Member. I would like to submit two articles into the record, "New European U.S. Data Transfer Pack Agreed," dated February 2, 2016.

Mr. ISSA. Without objection so ordered.

Ms. JACKSON LEE. Reuters, and Washington Post, "The British want to come to America with Wiretap Orders and Search Warrants," dated February 4th.

Mr. ISSA. Without objection so ordered.

[The information referred to follows:]

Technology | Tue Feb 2, 2016 1:15pm EST

Related: TECH

New European, U.S. data transfer pact agreed

BRUSSELS | BY JULIA FIORETTI AND FOO YUN CHEE

The word 'password' on a computer screen is magnified with a magnifying glass in this picture illustration taken in Berlin May 21, 2013.
REUTERS/PAWEL KOPCZYNSKI

European and U.S. negotiators agreed a data pact on Tuesday that should prevent European Union regulators from restricting data transfers by companies such as Google and Amazon across the Atlantic.

The European Union and the United States have been racing to replace the Safe Harbour framework that was outlawed by a top EU court last year over concerns about U.S. mass surveillance, leaving thousands of companies in legal limbo.

The announcement of the pact, which still requires political approval, coincides with two days of talks in Brussels, where European data protection authorities were poised to restrict data transfers unless a deal was clinched.

The European Commission said that the new Privacy Shield would place stronger obligations on U.S. companies to protect Europeans' personal data and ensure stronger monitoring and enforcement by U.S. agencies.

"We have for the first time received detailed written assurances from the United States on the safeguards and limitations applicable to U.S. surveillance program," Commission Vice-President Andrus Ansip told a news conference.

"On the commercial side, we have obtained strong oversight by the U.S. Department of Commerce and the Federal Trade Commission of companies' compliance with their

obligations to protect EU personal data."

The United States will create an ombudsman within the State Department to deal with complaints and enquiries forwarded by EU data protection agencies. There will also be an alternative dispute resolution mechanism to resolve grievances and a joint annual review of the accord.

European data protection authorities will also work with the U.S. Federal Trade Commission to police the system.

THUMBS UP

The accord received a thumbs up from lobbying groups The Information Technology Industry Council, BSA The Software Alliance and DigitalEurope, as well Paris-based International Chamber of Commerce and BusinessEurope.

"The free flow of data between the EU and the U.S. is the most important in the world. This agreement is essential because it provides a reliable framework for international data transfers," BusinessEurope Director General Markus Beyrer said.

However, Max Schrems, the Austrian law student whose court case against Facebook in Ireland sank Safe Harbour, expressed doubts about the validity of the pact, saying on his website that he is not sure whether the system would stand up to legal challenge.

European Digital Rights, an umbrella group of digital civil rights bodies, described the agreement as flawed.

"The emperor is trying on a new set of clothes. Today's announcement means that European citizens and businesses on both sides of the Atlantic face an extended period of uncertainty while waiting for this new stop-gap solution to fail," Executive Director Joe McNamee said.

Safe Harbour had for 15 years allowed more than 4,000 companies to avoid cumbersome EU data transfer rules by stating that they complied with EU data protection law.

Cross-border data transfers are used in many industries for sharing employee information, when consumer data is shared to complete credit card, travel or e-commerce transactions, or to target advertising based on customer preferences.

(Additional reporting by Shadia Nasralla in Vienna; Editing by David Clarke and David Goodman)

The Washington Post

National Security

The British want to come to America — with wiretap orders and search warrants

By Ellen Nakashima and Andrea Peterson February 4

If U.S. and British negotiators have their way, MI5, the British domestic security service, could one day go directly to American companies such as Facebook or Google with a wiretap order for the online chats of British suspects in a counterterrorism investigation.

The transatlantic allies have quietly begun negotiations this month on an agreement that would enable the British government to serve wiretap orders directly on U.S. communication firms for live intercepts in criminal and national security investigations involving its own citizens. Britain would also be able to serve orders to obtain stored data, such as emails.

The previously undisclosed talks are driven by what the two sides and tech firms say is an untenable situation in which foreign governments such as Britain cannot quickly obtain data for domestic probes because it happens to be held by companies in the United States. The issue highlights how digital data increasingly ignores national borders, creating vexing challenges for national security and public safety, and new concerns about privacy.

The two countries recently concluded a draft negotiating document, which will serve as the basis for the talks. The text has not been made public, but a copy was reviewed by The Washington Post.

The British government would not be able to directly obtain the records of Americans if a U.S. citizen or resident surfaced in an investigation. And it would still have to follow the country's legal rules to obtain warrants.

Any final agreement will need congressional action, through amendments to surveillance laws such as the Wiretap Act and the Stored Communications Act.

Senior administration officials say that they have concluded that British rules for data requests have "robust

protections" for privacy and that they will not seek to amend them. But British and U.S. privacy advocates argue that civil liberties safeguards in Britain are inadequate.

The negotiating text was silent on the legal standard the British government must meet to obtain a wiretap order or a search warrant for stored data. Its system does not require a judge to approve search and wiretap warrants for surveillance based on probable cause, as is done in the United States. Instead, the home secretary, who oversees police and internal affairs, approves the warrant if that cabinet member finds that it is "necessary" for national security or to prevent serious crime and that it is "proportionate" to the intrusion.

If U.S. officials or Congress do not seek changes in the British standards, "what it means is they're going to allow a country that doesn't require independent judicial authorization before getting a wiretap to continue that practice, which seems to be a pretty fundamental constitutional protection in the United States," said Eric King, a privacy advocate and visiting lecturer in surveillance law at Queen Mary University of London. "That's being traded away."

Senior administration officials said that they are seeking to relieve the pressure on U.S. companies caught in a "conflict of laws." The United States bars American firms from providing intercepts to anyone but the U.S. government after law enforcement has obtained a court order. Britain wants to directly compel the production of the data and has already passed legislation to make that happen.

To obtain stored emails, a foreign government must rely on a mutual legal assistance treaty (MLAT) by which the country makes a formal diplomatic request for the data and the Justice Department then seeks a court order on its behalf — a process that is said to take an average of 10 months.

"This has been an issue with the U.K. and other countries for a number of years," said one senior administration official, who like several others spoke on the condition of anonymity to discuss the negotiations. "Because of technological changes, the U.K. can no longer access data in the U.K. like they used to be able to, and more and more, U.K. nationals — including criminals in their country — are using providers like Google, Facebook, Hotmail. The more they are having challenges getting access to the data, the more our U.S. providers are facing a conflict of laws."

Administration officials and officials from several tech firms said the stakes are high if no agreement is reached.

They fear that if the trend continues, more foreign governments will force U.S. firms to host their data in those countries — a practice known as "data localization." They also fear passage of laws, like the one in Britain that has not yet been enforced, requiring foreign firms doing business in their country to comply with their surveillance orders, even if the orders conflict with U.S. law.

"We're reaching a moment where the status quo is no longer workable," said an official at a major tech firm. "We're concerned about the mounting frustration and the inability of foreign governments, including the U.K., to receive

responsive data in law enforcement investigations in a timely manner."

Up to now, he said, U.S. firms have "held their ground" when pressured to turn over data or conduct wiretaps in conflict with U.S. law. "Increasingly, that's not something we'll be able to do," he said.

Just over a week ago, the White House gave the State and Justice departments the green light to begin the formal negotiations. Officials stressed that they were in the very early stages of the talks, which probably will go on for months. They said they will seek to ensure that any agreement protects civil liberties.

But Gregory Nojeim, senior counsel at the Center for Democracy & Technology, a Washington-based privacy group, said allowing Britain to go to U.S. firms directly with wiretap orders "would be a sea change in current law. I don't see Congress going down that road."

Senior administration officials said that the goal is to help a close ally investigate serious crimes — something that the United States has a shared interest in.

One potential example: London police are investigating a murder-for-hire plot, and the suspects are using Hotmail to communicate, and there's no connection to the United States other than the fact that the suspects' emails are on a Microsoft server in Redmond, Wash. Today, the police would have to use the MLAT process and wait months.

"Why should they have to do that?" said the administration official. "Why can't they investigate crimes in the U.K., involving U.K. nationals under their own laws, regardless of the fact that the data happens to be on a server overseas?"

Jennifer Daskal, a national security law professor at American University and a former Justice Department official, said before U.S. firms are asked to turn over data, they should be assured that the legal standard for the request is sufficiently high. It need not mimic precise U.S. standards, she said, but should at least require that requests be targeted, and subject to independent review and privacy protections that weed out irrelevant information. If not in the agreement, Congress should mandate requirements, said Daskal, who is part of a coalition of privacy groups, companies and academics working on the issue.

A second administration official said that U.S. officials have concluded that Britain "already [has] strong substantive and procedural protections for privacy." He added: "They may not be word for word exactly what ours are, but they are equivalent in the sense of being robust protections."

As a result, he said, Britain's legal standards are not at issue in the talks. "We are not weighing into legal process standards in the U.K., no more than we would want the U.K. to weigh in on what our orders look like," he said.

The agreement is intended to be reciprocal, so that the U.S. government could directly request wiretaps or stored data of a British provider as long as the target is American and not a British citizen.

Karla Adam in London contributed to this report.

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. Follow @nakashimae

Andrea Peterson covers technology policy for The Washington Post, with an emphasis on cybersecurity, consumer privacy, transparency, surveillance and open government. Follow @kansasalps

Ms. JACKSON LEE. Thank you.

Mr. ISSA. We now go to Mr. Ratcliffe.

Mr. RATCLIFFE. Thank you, Mr. Chairman. Mr. Chertoff, or Secretary Chertoff, I thank you as well for your service while you were over at the Department of Homeland Security, I was a U.S. attorney and a former terrorism prosecutor. So I wanted to ask you about your testimony; you seem to suggest that we revert to a global standard of data control based on where the target of the investigation is a resident, is that right?

Mr. CHERTOFF. Actually, I would be probably inclined to say it should be based on where the citizenship of the accountholder as opposed to the target. But I could see an argument that might look at the target as well. But I think probably the accountholder makes the most sense.

Mr. RATCLIFFE. Okay, well let's walk through a scenario that we have probably both been through before. What if the information on say a suspected terrorist is located, and to use an example others have used here, is actually stored in Ireland but we know—let's say we know that that individual is a Saudi national. How would you reconcile that?

Mr. CHERTOFF. Well, so first of all, I mean I think the default position would be to go based on a treaty request, like an MLAT, but hopefully in a world in which these requests are not 10 months, but are more like 10 hours. And we have seen from what Mr. Smith said that it is possible, in fact, to do that.

Mr. RATCLIFFE. Okay. So under the standard that you—tell me the impact that you would think that would have with respect to national security investigations generally.

Mr. CHERTOFF. Well, and again, I am predicating this on a more efficient regime of answering these requests. But I think in many ways we have dealt with these cases in the past. I think that provided people put an adequate priority on this—and my experience is generally they do in a terrorism case—I think it would not impede investigations unduly, and I think what it would do is avoid the kind of conflict that actually winds up slowing up investigations, because that person who is holding the data, or the entity that is holding the data, is caught on maybe unnecessarily between two conflicting legal systems when an agreement to go by way of a treaty would eliminate that sense of conflict.

Mr. RATCLIFFE. Do we get into a situation there where we would be increasing our reliance on intelligence authorities rather than law enforcement authorities?

Mr. CHERTOFF. Well, I will acknowledge to you that when you are dealing with terrorism, particularly prevention, a lot of what we do is intelligence based. And that is a different set of issues than access by legal process. And so I am not suggesting we do not do that, but I am saying if we are using legal process, I think a system that eliminates conflict is something that both enables us to actually speed up cooperation, and avoids putting companies in a difficult position.

Mr. RATCLIFFE. Okay. And speaking of processes, you mentioned before the MLAT process. And you may have already given your thoughts with respect to reforms, but that was something that I tried to utilize during my time at the Department of Justice and

admittedly not very effectively utilized it. And so I want to give you an opportunity to expound on the MLAT process and the best way to reform that from a congressional perspective.

Mr. CHERTOFF. Well, your experience and mine are very similar. And I think there are two elements to this. One is I think the technology, at least when I was a prosecutor, you know, it was a paper-based system. And it tended to be, from a technological as well as, frankly, a priority standpoint, you know, pretty slow. I think we could build a technology platform that would make this much, much quicker. We see this in a lot of areas in the commercial domain.

I think the second issue would be the policy standpoint. And there, I think, whether it is additional resources, or a decision at a high level of the law enforcement community to treat at least a certain category of these very high priority would be—enable us to move these more quickly. And I think, again, the lesson of what happened after the Paris attacks, where it took 45 minutes to respond to a request is illustrative.

Mr. RATCLIFFE. Right. Well, out of respect for the other Members that have questions, I will yield back the balance of my time. I do want to thank everyone for being here. We all understand what an important issue we are discussing today. I yield back.

Mr. ISSA. I thank the gentleman. We now go to the gentlelady from Washington, Ms. DelBene.

Ms. DELBENE. Thank you, Mr. Chair. And thanks to all of you for being with us today. Mr. Smith, when ECPA was written many years ago, as you were highlighting, in 1986, it was also the very early days of email. When I first started working on email in 1989, even then it was still really only used in companies that had it for internal communications. And if you did get an email, folks always downloaded it from a server because capacity in servers was very low. And they would regularly delete those servers to have room for new information.

So it seems clear that some of the fundamental technical assumptions that were made when ECPA was written have definitely changed vastly since then. And I wonder if you could comment on the mechanics of cloud computing today and what legal questions that creates, especially with respect to ECPA. And why cannot the courts just shoehorn kind of all of these—today's legal issues and to, like, the international storage issue, into that old law.

Mr. SMITH. Well I think your question raises an excellent point. A company like Microsoft built its first data center outside the United States only in 2010. So cloud computing and the explosion of cloud computing is really a phenomenon of this decade. That is what has created all of these issues that we are talking about today. And it has created the need at times for law enforcement, quite rightly, to want to get access to information, to content, to email in other countries.

I think the fundamental question in a sense from a U.S. legal perspective is that when technology moves forward and the law needs to catch up, as it does here, what is the best way for that to happen? And we would say the best way is for the executive branch, if it wants new power, to come back to Congress and ask Congress to enact it.

Ms. DELBENE. And when you say when the law was written it was written actually with respect to the way technology was working then, as opposed to providing intent going forward.

Mr. SMITH. Well absolutely, and the most interesting and telling aspect of ECPA in this regard is the fact that it applied a lower standard to protect email that was over 6 months old. And that was all based on some thinking in the 1980's that, I think, barely anybody can remember, that most businesses moved their paper records offsite after 6 months. Maybe that was true. But who the heck has an email account that has only email that is less than 6 months old? The answer is only email accounts that have been opened less than 6 months ago. All the rest of us have email that is older than that, and that just shows how much the world has changed.

Ms. DELBENE. And with the shift to cloud computing now, more and more of that information is stored on servers.

Mr. SMITH. Well, the amazing thing about the cloud, as you point out quite rightly, is now we are not only talking about email, we are talking about all the photographs of our lives. We are talking about all of the other digital records that we have. We are talking about the PDFs that—in our lives. It is everything that sort of documents what we do every day.

Ms. DELBENE. And do you think that people should have a different expectation of how digital information is treated versus physical information? Is there a legal significance to the fact that you might information that is in digital form versus paper form?

Mr. SMITH. I think that technology needs to advance, but certain timeless values need to endure. And among these timeless values are the rights to privacy. And every time the American public has been asked, they have said the same thing. They want the data they store in the cloud to get the same privacy protection as the information they store on paper. And I think that is exactly the right point of view.

Ms. DELBENE. Does anyone else think there is a difference between digital or paper in terms of the legal significance and that differentiation?

Mr. Chertoff. I agree with Mr. Smith. I think one of the challenges here, frankly, is people—sometimes because of the fact that the data moves electronically and seamlessly, conflate what is a business record and a provider with what is something that a provider holds as a custodian so to speak. And to use an example from the banking world, it is one thing to subpoena a bank for bank records which are the bank's own documents or the bank's own information.

It is another thing if you want to get into a safety deposit box. The bank does not have a limitless right to enter the box and, therefore, you need a warrant for the box that is separate and distinct from a subpoena for the business records. And because electronic data does not neatly fall into that obvious category, categorization, there is a tendency to conflate the two. But I think as Brad says, that the principles ought to be the same.

Ms. DELBENE. Mr. Kris?

Mr. KRIS. I would just say the two factors that strike me as the most significant here are first, the incredible amount of digital data

that is now created and available. Digital dust or digital footprints of your daily life are everywhere created. And they are also, second point, stored with third parties in a way that they did not use to be. And so I find myself in strong agreement with Mr. Smith when he had his 1912 adding machine in front of him.

It is, I think, important and appropriate for Congress to look at the All Writs Act again. I would go further, and suggest you also consider the technical assistance provisions in both the Wiretap Act and FISA to clarify exactly what kind of assistance is going to be required from third parties in making digital data in the clear available to the government. You know, at one extreme is legislation now pending in the U.K. which, if I read it correctly, would essentially allow them to compel providers to push down widgets, malware in bulk, across a network and all the users on that network.

And at the other extreme would be, you know, essentially no compelled assistance. There is going to be a middle ground there, and I think Congress is the appropriate institution of our government to come to grips with that.

Mr. ISSA. I thank the gentlelady. And with that we go to the gentleman——

Ms. DELBENE. Sorry, my time expired.

Mr. ISSA. Yes, I am afraid so. And we now go to the gentleman from South Carolina, Mr. Gowdy.

Mr. GOWDY. Thank you, Mr. Chairman. And I apologize for having to leave. I had a meeting on the Senate side. But I am happy to report that they are up at this early hour working on the Senate side. And I see that almost all the good lawyers have gone, so it is my turn. Mr. Smith, from a law enforcement perspective, you receive a warrant for information that you maintain in a foreign country. And I know some of this has already come up, but just humor me because I find this stuff interesting and I would rather you say it twice than not say it once. You get a search warrant for material that is in a foreign country from a U.S. law enforcement official, and it violates the law of that foreign country for you to access that information. How do you resolve that?

Mr. SMITH. Well I think the real problem is we are just being put in an impossible position. You know, certainly what we have done to date is looked at U.S. law and if the information is in the United States and it would violate the Stored Communications Act for us to turn it over, we simply do not turn it over. That is why, as I was saying earlier, we have now been fined $28 million by the Brazilian Government, and we have an executive there who is being prosecuted. I think the big quandary we are all going to face in 2 years is what happens once the new European Union regulation takes effect, and their blocking statute that would prohibit us from turning information over to the DOJ outside of an international agreement kicks in. I do not see how we can turn information over to the Justice Department if it is in Europe, and European law prohibits us from doing so, which is why I think the fundamental argument that the Justice Department, that it needs this, both has some merit but, ultimately, frankly, sort of misses the point. The day of unilateral search warrants is fast coming to an end; it needs

to be replaced by something new and something better and we had better act quickly.

Mr. GOWDY. Are there any facts from the Brazilian fact pattern where you have an executive that is facing—did you say criminal prosecution?

Mr. SMITH. Yes, criminal prosecution.

Mr. GOWDY. For being out of compliance with a discovery order, or what is the procedure for where he finds himself, or herself?

Mr. SMITH. You can think of it as akin to what in the United States would be a contempt order from a court. You know, a local court has issued a local order requiring us to turn over certain information but in this case the information is not in Brazil, it is in the United States, and U.S. law prohibits us from turning it over. As we talk about pressure for data localization, this is the ultimate pressure for data localization. Because obviously, what it is intended to do is encourage U.S. companies to build data centers in Brazil so we no longer have to follow U.S. law.

So, again, the specter of concerns that people have in some ways are coming true before our very eyes if we cannot find a better way to solve them.

Mr. GOWDY. For those of us in the past who have experienced the joy of facing potential contempt from a judge, what is your executive supposed to do? How is he or she supposed to get out of this quandary?

Mr. SMITH. Let me just say I do not want to get into the privileged conversations that I have had with our employee. It is a darn complicated situation. Yeah, these are situations where people's life and liberty ultimately is at stake. And, you know, we at Microsoft are not alone in having faced these kinds of issues around the world. And there are a number of companies facing similar issues in Brazil itself. And, you know, it, among other things, calls into question how one continues to do business in certain countries, whether people can continue to live there. You know, these are not easy decisions to make.

Mr. GOWDY. Have you proposed either a legislative or regulatory remedy to the Department on how to resolve fact patterns like the Brazilian one?

Mr. SMITH. Yes, and I have talked with the Brazilian Government as well as you might imagine. Ultimately, I believe that if the U.S. and the U.K. can fashion an agreement that works, the people in the United States can feel comfortable with, that law enforcement can feel meets its needs, it creates a model that we can consider then advancing in other countries.

And I, frankly, hope there will a day when there is an agreement between the United States and Brazil as well. I think that that kind of solution is needed for the people of Brazil, and the Brazilian Government, who have legitimate needs I appreciate, but we just need a new solution, not an old one.

Mr. GOWDY. I am almost out of time, so this will be my last question. Going back to when we were in law school and this expectation of privacy, and the fact that it has to be an expectation that the public considers to be reasonable, but the public can change its mind. So the bank records case from 30 years ago, or however old that was, if that is really the most recent precedent or the prece-

dent that people cite for this, where do you see the public's reasonable expectation in terms of what they think they have a privacy interest in?

Mr. SMITH. I think technology has moved forward, public expectations of privacy have caught up, people actually do expect the data they store in the cloud and put on their devices to be private. And the Supreme Court, I think, recognized this unanimously 2 years ago in the Riley case. And I thought the fact that it was a unanimous Supreme Court decision acknowledging this public expectation to privacy was of fundamental importance for the country.

Mr. GOWDY. Thank you, Mr. Chairman.

Mr. ISSA. Thank you, Mr. Chairman. We now go to the gentleman from New York, Mr. Jeffries.

Mr. JEFFRIES. Thank you, Mr. Chairman. I thank all the witnesses for their presence here today. Let me start with Mr. Smith. Microsoft is a U.S.-based company in Washington that employs around tens of thousands of individuals in the country, is that fair to say?

Mr. SMITH. That is correct. We employ more than 50,000 people in the United States.

Mr. JEFFRIES. And other companies like Google and Apple and Facebook also employ tens of thousands of people here in the country?

Mr. SMITH. Collectively our industry employs hundreds of thousands, indeed probably millions, of people in the United States.

Mr. JEFFRIES. And it is projected, I think, over the next 5 years that at least a million, if not more, jobs will be created here in America as a result of the activity of technology innovation companies.

Mr. SMITH. Assuming our country can give people the skills and education they need, absolutely we will create the jobs and fill them here.

Mr. JEFFRIES. Now, collectively, companies like Microsoft and Apple and some of the others that I mentioned are sort of world leaders in the technology and innovation economy. Is that also a fair assessment?

Mr. SMITH. That is what we aspire to be every day, yes.

Mr. JEFFRIES. And I would be interested in your thoughts as to this notion that the trust factor, which has been eroding all across the world as it relates to the view that many other countries have toward our leading technology companies, could adversely impact our position as a world leader in technology and innovation.

Mr. SMITH. It is, I just think, an imperative for the U.S. technology sector to restore trust in American technology. We really, over the last 3 years, since the Snowden disclosures, there has been a global conversation taking place about whether people can trust technology. And as a tech sector, we have been out taking new steps, including investments in end-to-end encryption to advance that kind of trust. And I just think it is fundamental to our ability to succeed globally in the future.

Mr. JEFFRIES. Secretary Chertoff, could you comment in this trust dynamic and the notion of eroding American competitiveness?

Mr. CHERTOFF. Yeah, I would be delighted to, Congressman. I will give you an example of what happens when you do not have trust. It is not a surprise that some of the major Chinese companies that are involved in producing telecommunications and IT equipment have a bit of a trust problem around the world. And I think in the last couple of years they wanted to be—one of them wanted to be the backbone of the IT system in Australia, and the Australian government said no, they would not allow it because, again, there was a trust issue.

I think we underestimate sometime the strategic value of the United States of the ability to have an IT system, and to produce products and services that people do trust, and are willing to rely upon and implement. And I think, you know, since the Snowden disclosures, the effort to rebuild trust by making sure that first of all we have clear processes about, you know, what the law is, what is private, under what circumstances it has to be turned over—I think that is critical to maintaining our competitive position and that has an effect not only on our, frankly, our jobs, but on our national security as well.

Mr. JEFFRIES. Thank you. Mr. Smith, the Department of Justice seems to have taken a position that there are no existing conflicts of law. Is that your understanding of their position, or your understanding of what the actual landscape is at this moment in time?

Mr. SMITH. It is clearly what Mr. Bitkower said this morning. I do not believe it is an accurate characterization of the issues in our lawsuit at the Second Circuit. We pointed out that there are serious issues and concerns involving the potential conflict between U.S. and Irish law. There is no Irish court decision that is yet on point, but I think that the issues are serious.

As I have mentioned, in Europe the law will be clear. There will be a concrete conflict across Europe in 2 years. And fundamentally, the case is not about whether there is a conflict of laws. It is about whether the executive branch is exercising power that the Congress gave it in ECPA.

Mr. JEFFRIES. Now are countries in other continents likely to follow the lead of the European Union and move in the direction that becomes more restrictive, countries on the Continent of South America, Africa, Asia?

Mr. SMITH. We are following these regulatory and legal trends around the world. And what we are basically seeing is a number of governments considering or enacting new laws or regulations that, in some cases, are requiring data localization, and in other cases are considering or moving toward these kinds of so-called blocking statutes like the one I have referred to in the European Union; yes.

Mr. JEFFRIES. Thank you. And lastly, Secretary Chertoff, the 19th century was the century of the telegraph, the 20th century the century of the typewriter, and then the personal computer, 21st century, century of the smart phone, internet of things, who knows what other innovation will take place. There seems to be an emerging consensus from many colleagues on both sides of the aisle that Congress needs to step in, in this vacuum.

My question is with the explosive growth of innovation and technology, which is a great thing, you know, how—it is difficult for

Congress to keep up with the changes in technology. But what framework should we take in looking to enact legislation that recognizes the fact that we want to create some certainty, but also flexibility in interpretation in order to capture the dramatic and rapid change of technology?

Mr. CHERTOFF. I think that is a very important question, it is one that I am not going to be able to fully answer in the remaining time allotted. I would say this—I do think it is time for Congress, whether they do it by way of a commission or some other body, to really take a comprehensive look at the question of how the change in technology has affected a lot of our expectations. I would not legislate on a micromanagement level but I do think some general principles could be fleshed out. And just to give you one example, Mr. Smith talked about the Riley case. Much of our rule about privacy is based on the idea that we are thinking about when you search an object or a case, you are searching what is in the case. But in many ways when you now pick up a smart phone and you start to search the phone, what you are doing is you are taking a key to your house. And it is as if you are taking the key and walking over to someone's house and searching the whole house.

So as we think about the issue of, how do we deal with data that is remotely held I think there is a general set of principles that we could come up with that would not micromanage every situation, but would help give a framework for applying?

Mr. JEFFRIES. Thank you, and I yield back.

Mr. ISSA. I thank the gentleman. Now all you have left are the non-attorney, four attorneys behind me, that will undoubtedly question a lot of my questions, but rightfully so. You know, Secretary Chertoff, I am going to use you as part of it; I am going to use probably Mr. Smith as part of it. First question was, since you brought all of your props and they are all tangible old props do you view—as I asked the first panel—do you view that, in fact, what we need to do is write specifics, but write them based on the same principles that we had in the tangible world? That is a fair analysis, is it? Secretary, same thing. Because I mean I think that is the first thing. We are going to have to write legislation. Do we write it based on principles of the past that our Founders saw in the tangible world, and then find a way to make them versatile in a instantaneous transfer world?

Mr. CHERTOFF. I would say the answer to that is yes, in the sense that the enduring principles are what we want to make sure are preserved. But without minimizing the fact that it is not simply a matter of translating, you know, what is physical to what is virtual. There are going to be some differences, but the values remain the same.

Mr. ISSA. Well let me go over some of these values. And if I see a headshake no, I will call on you. Otherwise, we will assume that I have got some yeses on these, which I like to get to yes. You might have noticed that in the past. Principles that we need to do if we pass updated legislation; first of all, we need to deal with the predictability, not just in the United States, but around the world.

We need to have a reciprocity concept at the time that we produce this legislation, because the rest of the world is looking to us for whether we will live by our rules when the shoe is on the

other foot. The American people need to have a notice of what their rights are, and likely, in most cases, a notice of the taking of their information. We know there are certain times that it will not happen. We need to deal with what nexus is in a virtual world; not just is it a U.S. person, but did it originate in the United States? Did it transfer through the United States? And so on.

We are likely, I believe, as a principle to have to break into two parts; one is the criminal part, including national security, the other is civil. Because, again, I suspect that we are going to have a custody battle between two people, and yet records are going to be demanded from around the world.

It seems like, back to the same point, there has to be an informed consent. In other words, today most of us have no idea whether or not the storage of some item might give us additional rights or might not. And I presume we are going to have to look at that from a standpoint of both law and treaty. One that I, because I am also on foreign affairs, I am become very familiar with is the principle that does not seem to exist here but clearly exists in Europe, the right to be forgotten is going to have to be addressed if we are going to have reciprocal agreements with other countries who truly believe that if you host something in another country, it will not eliminate the likelihood that you have to honor, let's just say a European Union citizen, the right to disappear, which they are clearly working on. I have not got a no yet.

Lastly, the expectation of privacy. It appears as though one of the most important things we are going to have to do is define what the American people can expect from data which is stored anywhere outside of their pocket in an inanimate object with no battery and a cloister of multiple different shrouds, so that it cannot possibly be energized remotely, and thus activated and taken.

And, Mr. Chertoff, you were laughing because we all know exactly how that happens. So did I go through points you all agreed to? And it looks like I did. What did I leave out? What additional considerations should this Committee have in the record today as we look to what is obviously our primary jurisdiction and a long overdue look at the world as it exists electronically? And I will just go right down the list.

Mr. SMITH. Well first I would say that you have shown once again what Abraham Lincoln first proved, you do not have to go to law school to have a great legal mind. I think you have captured the legal issues that the world needs to address and certainly this Congress needs to address. I do not think there is anything that you have left out or—let me put it another way—if Congress could answer the questions that you have posed, the whole world of technology and the world for people would be much better off.

Mr. CHERTOFF. I really agree with that. I would say one thing, just not to be naive. You know, I think in our minds when we talk about the ability to reach a global accommodation, we are thinking of the Europeans, we are thinking of countries that are more or less kind of western style democracies.

Mr. ISSA. But I serve on Foreign Affairs so I know that we are—we may all be created equally but we do not all think the same.

Mr. CHERTOFF. Exactly. And I think when we deal, for example, with Russia, we are going to need to be realistic about that. But,

you know, if we can reach a reasonable set of agreements with a good deal of the globe, that would be a major, major step forward.

Mr. ISSA. And so that is where the reciprocity may not be universal but at least the standards among those who have reciprocity would be universal. Mr. Kris.

Mr. KRIS. Yeah, I agree. I thought that was an excellent summary of all of the issues that need to be addressed.

Mr. ISSA. That is why I went last.

Mr. KRIS. Instantiating them, you know, in all of the various digital and other settings is going to be, as you know, enormously challenging. The only additional point I would make is you have, I will call it an opportunity, before the end of 2017 to consider renewal of the FISA Amendments Act. And so that is, as an adjunct to this, another area in which you are going to want to, I think, harmonize your efforts. Thank you.

Ms. DASKAL. So I echo the agreement with the incredible list. I would just add that when one is thinking about the relevant nexus, which you raised just now and you also raised in your earlier questions to Mr. Bitkower, and the analogies to tangible property, I think the analogies are right in the sense that it does not make sense for the United States to assert unilateral jurisdiction over everything everywhere in the world; that there is a concern about that. At the same time, I think it is worth thinking about other jurisdictional hooks other than location of data, given the differences between data and other forms of tangible property.

Mr. ISSA. I think your point is good. And just as one Member of this Committee, I believe that is one of the challenges we face from a business standpoint. And I will put my recovering, hopefully, never fully recovered businessman's hat on for a moment.

And that is that we want the world to have an expectation that rule of law will exist for them, no matter where the data is. The data transfer or, let's just take J.P. Morgan Chase; if they only have one server farm, or two server farms, and they are both in the United States that will not happen. But if it did, we do not want the world to believe they are disenfranchised and begin ordering balkanization. And I certainly think although that is not part of the principles of our Constitution here, it is good common sense that we have to find a solution that does not adversely affect business models, cause countries essentially to order, even if it is Russia, to order that you localize for some reason.

Let me beg your indulgence; I have 4 minutes left on the Chairman's mandate that we finish at 1:30. There is an elephant not in the room, which is the Apple case, but since I am bringing it into the room, I want to ask just a basic question, and I will start with Mr. Smith. Microsoft, you mentioned in your testimony, and in some of your answers, you are looking at end-to-end encryption for a multitude of products. Your products, if they do not now, will shortly un-encrypt, use data, re-encrypt as a matter of course because we now have the processing power that allows you to do that. Is that a fair statement?

Mr. SMITH. Well we are certainly focused on implementing encryption. It was two and a half years ago we said we would implement encryption at rest, encryption in transit, encryption in

more scenarios. So I think fundamentally encryption is an important part of safeguarding people's information for the future.

Mr. ISSA. So is it fair to say that what Apple is dealing with—you mentioned you are going to submit an amicus brief—what Apple is dealing with, every software company, and probably every communication company, and perhaps most, if you will, social networking and even ecommerce companies, all are going to face similar questions to the one that Apple is facing today.

Mr. SMITH. I think in one form or another, many, many technology companies in many, many countries are going to need to address these encryption issues. And certainly Apple's case is an important example of one form of that.

Mr. ISSA. And Secretary Chertoff, I am going to take advantage of the fact you have worn so many hats, and your knowing what FISA judges go through, knowing how the NSA provides information, knowing what the Central Intelligence—what their sources and methods historically have been. Let me just ask you a question in the open. Is not one of the most important tools that we have in going after terrorists and criminal networks, the lack of their predictability and knowledge of what we can or cannot break, what we do or do not know, and what we can or cannot find out?

Mr. CHERTOFF. I think that is absolutely correct. And that is one of the things that was very damaging about Snowden is to some extent he at least put them on alert about certain things.

Mr. ISSA. So when Apple and others say that ordering a predictable key encryption, a backdoor, guarantees that at least as to those who have complied with it, that the bad guys will know not to use that product. And if I think of sort of the entrepreneurial nature of criminals and terrorists, by definition will we not be begging them to take their millions or billions of dollars and use it to develop items that do not have a backdoor and, thus, reduce the chances that we are going to have commercial off the shelf software that we might be able to produce our own independent backdoors from time to time without their knowing it?

Mr. CHERTOFF. I think you are absolutely right. One of the unfortunate things about this being a public dispute is that it pretty much guarantees that terrorists will now be looking to other tools. And, in fact, there was something in the paper recently about a manual they found or some kind of a document of ISIS folks going through what are the best encrypted technologies. Now sometimes they are wrong, and that works for us, but only if we keep it quiet.

Mr. ISSA. Thank you. I want to thank all of our guests. You were great witnesses. It is exactly 1:30, and we stand adjourned.

Ms. DASKAL. Thank you.

[Whereupon, at 1:30 p.m., the Committee adjourned subject to the call of the Chair.]

APPENDIX

Material Submitted for the Hearing Record

Questions for the Record submitted to David Bitkower, Principal Deputy Assistant Attorney General United States Department of Justice*

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–3951
http://www.house.gov/judiciary

March 16, 2016

Mr. David Bitkower
Principal Deputy Assistant Attorney General
United States Department of Justice
Washington, D.C. 20530

Dear Mr. Bitkower,

The Committee on the Judiciary held a hearing on "International Conflicts of Law and their Implications for Cross Border Data Requests by Law Enforcement" on February 25, 2016 in room 2141 of the Rayburn House Office Building. Thank you for your testimony.

Questions for the record have been submitted to the Committee within five legislative days of the hearing. The questions addressed to you are attached. We will appreciate a full and complete response as they will be included in the official hearing record.

Please submit your written answers by **Wednesday, May 11, 2016** to Kelsey Williams at kelsey.williams@mail.house.gov or 2138 Rayburn House Office Building, Washington, DC, 20515. If you have any further questions or concerns, please contact or at 202-225-3951.

Thank you again for your participation in the hearing.

Sincerely,

Bob Goodlatte
Chairman

Enclosure

*Note: The Committee did not receive a response from this witness before this hearing transcript was finalized in October 2016.

Questions for the record from Chairman Bob Goodlatte (VA-06):

1. From the Department of Justice's perspective, please describe the predicament that U.S. technology companies find themselves in with respect to foreign law that requires U.S. technology companies to produce content of communications pursuant foreign legal process, and the U.S. law (ECPA) that prohibits U.S. technology companies from making such disclosures? What are some possible solutions?

2. Why is the Mutual Legal Assistance Treaty process ill-suited for requests by U.S. agencies to U.S. companies for data stored abroad? Do any existing MLATS contemplate these types of requests?

3. A great deal of attention has been given to the impact of foreign laws on U.S. companies. But what is the effect of foreign laws prohibiting data transfers or laws requiring data localization on the U.S. government and U.S. investigations?

4. What will happen if Congress fails to implement legislation to facilitate international agreements such as the one currently being negotiated with the U.K.?

5. Shouldn't we be concerned that certain requests for data from U.S. agencies to U.S. companies may create a conflict of law for the companies to comply with if the data is stored abroad?

6. Should a bilateral agreement such as the one under consideration with the U.K. also ameliorate any conflicts of law with regards to U.S. requests for data held by U.S. companies in that country? Wouldn't this resolve the issue currently being litigated in the Second Circuit?

7. Why should the U.K. be allowed to make requests for data in motion, i.e. wiretaps, in addition to data at rest? Why is this necessary? Under U.S. law, the government has a higher burden to meet for a wiretap than for a search warrant. Will the U.K. be required to also meet a higher burden for real-time data collection than for stored collection?

8. Will the agreement between the U.S. and the U.K. allow direct requests to U.S. companies for intelligence purposes in addition to criminal investigations?

9. The U.S.-U.K. bilateral agreement has been described as allowing "wiretaps" by the U.K. government. Wiretaps are traditionally thought of as listening to telephone calls in real time. But a request from the U.K. to a U.S. company would not be to listen to a U.K. citizen's telephone calls, correct? Would it not pertain more likely to instant messaging, chat, or texting features offered by U.S. providers?

10. In your written testimony, you say a successful bilateral framework must establish adequate baselines for protecting privacy and civil liberties, both through the agreement

Response to Questions for the Record from Brad Smith, President and Chief Legal Officer, Microsoft Corporation

Hearing on International Conflicts of Law and Their Implications for Cross Border Data Requests by Law Enforcement
House Judiciary Committee
February 25, 2016

Chairman Bob Goodlatte
Questions for the Record
Brad Smith, President and Chief Legal Officer, Microsoft Corporation

1. Can you describe the conflict of law between U.S. and Irish law that is the underpinning of litigation currently pending before the Second Circuit? Is it your position that production of data stored in Ireland pursuant to a U.S. warrant violates Irish law? Aren't the U.S. warrant procedures more protective than what is required under Irish law to obtain data - and it is Irish law that would control were the government to request production through the MLA T process?

Microsoft has not taken a position on whether Irish law would forbid Microsoft from complying with the warrant at issue in that litigation. In our view, the relevant question is whether there is a possibility of conflict and tension, not the presence of an actual conflict. At oral argument before the Second Circuit, Microsoft's counsel acknowledged that the company is "certainly very concerned" that European Union (EU) law may prohibit the disclosure of data stored in the EU.

Others have raised concerns that the warrant at issue would violate Irish or EU law:

- The EU is in the process of approving the new General Data Protection Regulation ("GDPR") which recognizes that not only this warrant, but all similar non-EU orders, violate EU law. Article 48 of the GDPR provides that any "judgment of a court or tribunal . . . requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty," subject only to narrow exceptions.[1]
- The European Commission has taken the formal position that "personal data held by private companies in the EU should not, in principle, be directly accessed by or transferred to foreign enforcement authorities outside of formal channels of cooperation, such as … Mutual Legal Assistance Treaties."[2]
- Europe's Data Protection Authorities also issued a joint statement that, "[a]s a rule, a public authority in a non-EU country should not have unrestricted direct access to the data of individuals processed under EU jurisdiction," so "[f]oreign requests must not be served directly to companies under EU jurisdiction."[3]

---

[1] General Data Protection Regulation, Council of the European Union (April 6, 2016), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT.

[2] European Parliament, Parliamentary Questions, No. E-010602-14 (Mar. 4, 2015), *available at* http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-010602&language=EN.

[3] Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, at 3 (Nov. 26, 2014) (emphasis omitted), *available*

(continued…)

- Michael McDowell, the former Minister of Justice and Attorney General of Ireland, testified that "Ireland's Data Protection Acts . . . highlight its sovereign interest in guarding against the exercise of foreign law enforcement activities within its borders by any means other than applicable MLA treaties" and that "[a]bsent certain particular exceptions, disclosure to a third party of such data . . . is only lawful pursuant to orders made by the Irish courts."[4]

If the U.S. government were to request the data sought by this warrant through an MLAT, it would do so using the procedures in the Irish-U.S. MLAT. Under that MLAT, U.S. authorities would ask Irish authorities to assist in executing a request, by applying for a search warrant from an Irish judge. Respectfully, we believe Congress should not focus on whether U.S. or Irish law is more or less protective of privacy but, rather, which law properly applies to the situation.

2. Prior to the warrants at issue in the Second Circuit litigation, did Microsoft comply with warrants requesting data from a foreign server? If so, what changed that caused Microsoft to decline to comply with the warrants at issue in the litigation?

Microsoft opened its Dublin datacenter in 2010—the first datacenter storing Microsoft consumer data located outside the United States. In connection with opening this datacenter, Microsoft initiated a review process to determine whether its compliance obligations would change as a result of storing customer data outside the United States. Based on this review, Microsoft determined that warrants issued under ECPA could not lawfully compel Microsoft to produce data stored outside the United States and thus brought the legal challenge at issue.

3. What type[s] of laws are foreign countries starting to enact that create a conflict with U.S. law? Can you give us a sense of the types of requirements or restrictions these laws are imposing upon U.S. companies?

Foreign countries are enacting several types of laws, including: (1) data localization laws that require providers to store data within that country and thereby increase the costs associated with serving users in that country; (2) data retention requirements that require providers to store data for specific periods of time, which can affect a provider's practices for storing data worldwide; (3) new extraterritorial law enforcement powers that give these countries the power to access and intercept data stored in other countries, which can result in conflicts between the laws of the country issuing a legal order and the laws of the country in which the data sought by that order is stored; and (4) laws forbidding transfer of data outside the host country except pursuant to international agreements, which can also result in conflicts between the laws of the country requesting the data and the laws of the country in which the data is sought.

---

at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf.

[4] *See* Declaration of Michael McDowell, *available at* http://digitalconstitution.com/wp-content/uploads/2014/11/mcdowell-declaration-district-court-stage-filed-6-6-14.pdf

4. How urgent is this problem? Are we talking just about a handful of foreign countries that are enacting data production or data localization requirements? What is the impact of these laws?

The problem is urgent. As I noted in my testimony, the EU's new General Data Protection Regulation ("GDPR") will take effect in the Spring of 2018. The GDPR will replace the EU's existing data privacy framework—and it will create a stark conflict between EU and the government's interpretation of U.S. laws. Article 48 of the GDPR provides that cross-border transfers of personal data will generally only be recognizable and enforceable if they are conducted pursuant to an international agreement, such as an MLAT. The problem is not just limited to the EU or to a handful of countries worldwide. A number of nations are debating and enacting data localization and data retention laws, and each time one country passes such a law it encourages others to do the same.

5. Microsoft supports international agreements that will address and overcome conflicts of law. But these agreements are likely going to allow foreign countries to acquire data held by U.S. companies on a standard less than probable cause. Do you support this and, if so, why?

Microsoft supports international agreements that would address and resolve conflicts of law, and Microsoft is encouraged by the recently-reported negotiations between the United States and the United Kingdom. We believe U.S. negotiators should pursue balanced solutions that enhance both individual privacy and the ability of law enforcement to protect the public.

a. How does allowing foreign countries to obtain data from U.S. companies on a less-than-probable-cause standard square with the call for a uniform probable cause standard for requests by the U.S. government?

International agreements can help determine which country's law should apply when a law enforcement agency in one country seeks data stored in another country. For example, when a foreign country is investigating a foreign national for crimes that violate foreign law, and requests data that is stored in a foreign country, it may be that the mere fact that the provider is a U.S. company does not justify applying U.S. legal standards, and so an international agreement governing data access may call for application of foreign law rather than U.S. law. In those cases, so long as the foreign law meets a set of internationally-recognized standards, there may be no need to import U.S. legal concepts such as probable cause. In fact, when the data sought belongs to a foreign citizen, the citizen is likely to expect that the laws of her own country apply. But when the U.S. government seeks to obtain data—or when U.S. persons' data is sought—then U.S. law should govern, in line with the expectations of U.S. citizens, including requirements such as probable cause.

b. Should a bilateral agreement such as the one under consideration with the U.K. also ameliorate any conflicts of law with regards to U.S. requests for data held by U.S. companies in that country? Wouldn't this resolve the issue currently being litigated in the Second Circuit?

International agreements would be a productive step toward ameliorating the conflicts of law created by international data access requests. The degree to which such agreements resolve particular conflicts would depend on the scope and implications of the particular international

agreement, as well as which countries are a party to such an agreement or agreements. It is also worth noting resolving these issues through international agreements has other virtues. Among other things, the agreement provides an opportunity to establish a minimum set of standards for privacy and human rights that will govern countries seeking access to the contents of electronic communications.

c. Do you see any conflict between your position as it relates to foreign government access to data stored in the U.S. and your position as it relates to U.S. government access to data stored abroad?

Microsoft supports changes to the laws governing foreign government access to data stored in the U.S., and changes to the laws governing U.S. government access to data stored abroad. In both situations, Microsoft believes that, ultimately, international agreements should set forth a framework governing these international data access issues.

6. As you note in your written statement, following the Charlie Hebdo terrorist attack in France last year, the French government was looking for two at large suspects. The FBI came to you with an emergency request under Section 2702 of ECPA and your company responded with content information "in exactly 45 minutes." Where was that data located? On server located somewhere in the European Union?

ECPA permits a provider of electronic communication services to voluntarily disclose information to a governmental entity if the provider in good faith believes that an emergency involving the danger of death or serious physical injury to any person requires disclosure. Our understanding is that Irish law contains a similar exception. Therefore, when we receive an emergency disclosure request, as in the Charlie Hebdo attack to which I referred in my testimony, we do not check the location of the information sought by that request.

7. Microsoft has, at times, articulated that the location of the data should be a determining factor for which law governs law enforcement access to stored data. In today's world, though, the location of data can be fleeting. Data can be located on a server in one part of the world at noon, and moved to another server located in another part of the world only minutes later. In addition, the location of the data may be different from the location of the customer, which may also be different from the location of the government making the request for content information. Why should the location where data is stored be determinative of which law controls law enforcement access to stored data?

Where data is stored is but one approach to determining which law should govern an international law enforcement access request. In many cases, technology companies, including Microsoft, store a user's data geographically close to that user—such as by storing U.S. users' information in the United States, and EU users' information in the EU. In practice, email accounts are not moved around the world and doing so would not be efficient or practical, as a group of computer and data experts noted in an amicus brief to the Second Circuit. There are other methods of reconciling which law should govern international requests, and Microsoft is open to any solutions that harmonize international laws, enhance users' privacy, foster

technological innovation, and ensure that law enforcement has the tools it needs to protect the public.

8. Some have argued that it should be the nationality or location of the customer that determines which country's law controls law enforcement access to stored data. How does Microsoft definitively determine the location of a customer? How does Microsoft definitively determine the nationality of a customer? If these determinations can't be made in a definitive way, then how can nationality or location of the customer be used to determine which country's law controls law enforcement access to stored data?

The government is more likely to know the nationality of the customers whose data it seeks than is a provider. That is because the government has often conducted an investigation into those customers before serving legal process on the provider, and the background information obtained in such investigations may indicate the nationality and location of the persons whose data is sought. For example, the government may determine a subscriber's location through interviews with other witnesses during the investigation. For cases where neither the government nor the service provider can reasonably determine the nationality or location, the legal framework could clearly articulate the rules that would govern.

Representative Blake Farenthold
Questions for the Record
Brad Smith, President and Chief Legal Officer, Microsoft Corporation

1. Why is this issue - international conflicts of law concerning cross border data flow and law enforcement requests- important for your company? We're hearing a lot these days about technology companies resisting law enforcement requests for data. Can you talk about how Microsoft responds to law enforcement requests?

International conflicts of law can place technology providers in an untenable position, forcing them to determine which of two conflicting laws they must obey and which they must violate. That discourages long-term opportunities for growth, investment and innovation by technology companies at a time when those companies should be growing in response to tremendous consumer demand.

Microsoft takes seriously its obligation to comply with valid legal process. In the second half of 2015, Microsoft received 5,297 requests from law enforcement agencies in the United States, as stated in our most recent transparency report. Non-content data or subscriber information was produced in response to nearly 55% of those requests, and content data was produced in response to less than 10% of the requests. For many of the remaining requests (approximately 15%) no data was found, and other requests (approximately 21%) were rejected, generally because those requests did not meet the legal requirements for disclosure. Microsoft also recognizes the privacy of its customers' information and has adopted policies to protect their privacy. For example, when Microsoft receives a law enforcement request for an enterprise customers' information, it attempts to redirect law enforcement to obtain that information from the enterprise directly. Microsoft is also committed to notifying users of requests for their information, unless it is legally prohibited from doing so.

2. Some seem to want to keep the status quo and would probably argue that we should not update the laws - that the existing legal process is sufficient and that any change means that law enforcement efforts will be stymied. Is that true?

No. Today's laws are inadequate—both for law enforcement and for technology companies. It is clear that a law written 30 years ago was not designed for the technology of today. Leaving the Electronic Communications Privacy Act ("ECPA") intact without amending it undermines technology and public safety. Technology has moved forward in the past 30 years and the law must catch up.

3. Is the current situation sustainable? What is at stake if we do not modernize our legal framework?

This situation is not sustainable. We need a modern approach to ensuring governmental access to electronic communications worldwide. If we cannot modernize this legal framework, countries will continue enacting the types of data localization and data retention laws that we

have already seen. That will further fragment the online community, and it will increase the conflicts of laws that providers face when responding to international data access requests. That will harm not just providers, but also consumers, by discouraging innovation in the type of cloud technologies that have fueled economic productivity and growth in recent years and by introducing unnecessary uncertainty for consumers, who should know what law protects their information.

Representative Mike Bishop
Questions for the Record
Brad Smith, President and Chief Legal Officer, Microsoft Corporation

1. As you note in your written statement, following the Charlie Hebdo terrorist attack in France last year, the French government was looking for two at large suspects. The FBI came to you with an emergency request under Section 2702 of ECPA and your company responded with content information "in exactly 45 minutes." Where was that data located?

ECPA permits a provider of electronic communication services to voluntarily disclose information to a governmental entity if the provider in good faith believes that an emergency involving the danger of death or serious physical injury to any person requires disclosure. Our understanding is that Irish law contains a similar exception. Therefore, when we receive an emergency disclosure request, as in the Charlie Hebdo attack to which I referred in my testimony, we do not check the location of the information sought by that request.

Questions for the Record submitted to the Honorable Michael Chertoff, Co-Founder and Executive Chairman, The Chertoff Group*

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–3951
http://www.house.gov/judiciary

March 16, 2016

The Honorable Michael Chertoff
Executive Chairman and Co-Founder
The Chertoff Group
1399 New York Avenue NW, Suite 900
Washington, D.C. 20005

Dear Mr. Chertoff,

The Committee on the Judiciary held a hearing on "International Conflicts of Law and their Implications for Cross Border Data Requests by Law Enforcement" on February 25, 2016 in room 2141 of the Rayburn House Office Building. Thank you for your testimony.

Questions for the record have been submitted to the Committee within five legislative days of the hearing. The questions addressed to you are attached. We will appreciate a full and complete response as they will be included in the official hearing record.

Please submit your written answers by **Wednesday, May 11, 2016** to Kelsey Williams at kelsey.williams@mail.house.gov or 2138 Rayburn House Office Building, Washington, DC, 20515. If you have any further questions or concerns, please contact or at 202-225-3951.

Thank you again for your participation in the hearing.

Sincerely,

Bob Goodlatte
Chairman

Enclosure

*Note: The Committee did not receive a response from this witness before this hearing transcript was finalized in October 2016.

Questions for the record from Chairman Bob Goodlatte (VA-06):

1. There's been quite a bit of discussion today about "conflicts of law" but I'm curious to know more about exactly what is in conflict. Is it the standard or procedures by which an investigating agency obtains data? Is it the outright prohibition on access to data? What exactly puts our laws in conflict with foreign laws?

2. You suggest that we revert to a global standard of data control based on where the target of the investigation is a resident. What effect would that have on national security investigations? Could that increase the reliance on intelligence authorities rather than law enforcement authorities for gathering data held by subjects outside of the US?

    a. Under such a regime, how would we deal with a foreign citizen, in the United States, whose data is being held overseas?

Response to Questions for the Record from the Honorable David S. Kris, former Assistant Attorney General for National Security, United States Department of Justice

Answers to Questions for the Record
David S. Kris
Committee on the Judiciary, U.S. House of Representatives
Hearing on International Conflicts of Law and their Implications
for Cross Border Data Requests by Law Enforcement (February 25, 2016)

Questions for the record from Chairman Bob Goodlatte (VA-06):

1. **You state that there is no doubt that a challenge to a FISA physical search order for data stored abroad would prevail. Can you explain this in further detail? Is the same conclusion readily apparent in the Second Circuit case? What's the distinction between FISA and the Stored Communications Act that could result in different interpretations by a court?**

The definition of "physical search" in FISA expressly applies only to certain activities that occur "within the United States." 50 U.S.C. § 1821(5). The relevant provisions of the Stored Communications Act (SCA) do not include any such express language. As I understand it, the Second Circuit case discussed at the hearing, *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation,* No. 14-2985-cv, turns primarily on whether the relevant provisions of the SCA are best seen as a "warrant" which does not apply to data stored abroad, or as a hybrid instrument that should be enforced like a subpoena according to whether the court has personal jurisdiction over the custodian of the data (no matter where the data are located). Regardless of how that issue is resolved, it is unlikely to affect the interpretation of "physical search" in FISA.

2. **From your perspective as the former Assistant Attorney General for National Security at the Department of Justice, what kind of MLAT reforms should be made? What impact do you think an improvised MLAT process could have on the international conflict of laws issue being discussed here today?**

With the important caveat that I have been out of government for five years, my impression is that the MLAT process has not been able to keep up with demand, particularly with respect to digital data. The President's Review Group on Intelligence and Communications Technologies reported (page 227) that MLAT requests take an average of 10 months to fulfill. At the hearing (transcript pages 35-36), Mr. Bitkower from the Department of Justice did not dispute that report, and indeed indicated that it may understate the problem. A Department of Justice budget document concerning FY 2015 explains that "[d]elays and difficulties in obtaining evidence, especially internet records, through the MLAT process is [sic] increasingly becoming a source of frustration for many of our foreign partners."

Among the ways to improve the MLAT process may be to increase resources, streamline processes, invest in new technology, and train foreign partners in requirements to improve the quality of requests. The administration's proposed FY 2015 budget for DOJ included "an

additional $24 million to implement a strategy to reduce the current backlog of Mutual Legal Assistance Treaty requests, cut overall response times in half by the end of 2015, and process requests in a matter of weeks." It would be worth tracking budget requests, actual appropriations, and results over time to see if there are lessons to be learned.

As I testified at the hearing, however, I am not confident that increased resources and streamlined MLAT processes will suffice. For that reason, I believe it is appropriate to explore the possibility of direct access by foreign governments to data held by U.S. providers (and by the U.S. government to data held by foreign providers) under carefully-controlled circumstances and with oversight and other protections determined to be appropriate, through international agreements and legislative amendments to the Stored Communications Act.

3. Based on your experience, if bilateral agreements such as the one under negotiation between the U.S. and U.K. come to fruition, what might the oversight and compliance regime look like?

Among the key questions in this area, I believe, will be identifying with precision the following:

• the types of foreign production directives that must be honored by U.S. providers, whether classified by the type of data sought, the location of the data sought, the status, nationality or other characteristic of the provider served with the directive, the nationality of the target or subject of the underlying foreign investigation, the nature of the crime or other matter being investigated, the nature or identity of the foreign authority issuing the directive, and the requirements under foreign law for issuance of the directive;

• the review and approval (and amendment) mechanisms for what will likely need to be detailed guidelines or procedures that implement the international agreement and statutory authority at the operational level;

• the role of the Department of Justice (DOJ) or other elements of the U.S. government, if any, in reviewing the foreign directives, either in advance or after the fact, on an individual or aggregate basis, and the procedures to be followed where the U.S. government believes a directive is improper or outside the scope of the agreement or statute;

• the role of providers in reviewing directives, and the procedures they must follow if they have concerns about the propriety of a directive (e.g., objecting to the foreign government's request directly, or contacting DOJ to allow DOJ to express the objection or otherwise intervene);

• the role of the courts in reviewing directives, perhaps when petitioned to do so by a provider or by DOJ; and

• the information on the use of directives to be provided to Congress, whether that information comes from foreign governments (perhaps through DOJ), from DOJ or another U.S. government agency, from the providers, and/or from the Administrative Office of the U.S. courts.

4. What affect might data localization laws have on U.S. national security and the ability of the U.S. intelligence community to collect necessary intelligence to protect the homeland.

Like most observers, I have concerns about data localization, which might fragment the Internet and make it more difficult for the U.S. government (including law enforcement and the Intelligence Community) to obtain data that is physically unavailable because it is located in a foreign jurisdiction.

Questions for the Record from Representative Mike Bishop (MI-08):

1. Based on your experience, if bilateral agreements such as the one under negotiation between the U.S. and U.K. come to fruition, what might the oversight and compliance regime look like?

Please see the response above to Question 3 from Chairman Goodlatte.

Response to Questions for the Record from Jennifer Daskal, Assistant Professor, American University Washington College of Law

Response of:

Jennifer Daskal
Assistant Professor
American University Washington College of Law

Questions for the record from Chairman Bob Goodlatte (VA-06):

1. **The rules established under ECPA govern what a U.S. provider can and cannot do with both communication content and non-content records. The result is that the ECPA procedures, including the warrant requirement, apply to any customer of a U.S. provider, regardless of that customer's nationality or location and regardless of where the data is stored. Why is this insufficient to protect the privacy interests of all U.S. provider customers, including foreign customers?**

Chairman Goodlatte, thank you for the opportunity to respond to your questions.

As you point out, ECPA specifies when, and according to what procedures, the U.S. government can compel a U.S.-based Internet Service Provider (ISP) to turn over customers' data — including both the content of communications (such as emails) and non-content information (such as credit card information and Internet Protocol (IP) address). In April, thanks in large part to your leadership, the House voted unanimously to pass the Email Privacy Act, which would reform and modernize ECPA. Importantly, the Act eliminates outmoded distinctions between new and old communications, and specifies that, absent a well-delineated exception, the government needs a warrant to obtain emails from an ISP, regardless of how long the email has been in storage or the type of service provider. I urge your colleagues in the Senate to move swiftly to bring this legislation to the floor and pass it as is, without the addition of counterproductive amendments that would undercut the carefully negotiated protections adopted by the House.

Cross-border access to data, however, raises a different set of problems than those resolved by the procedural protections put in place under the Email Privacy Act. The key issue with respect to the cross-border access to data is not about the adequacy of the privacy protections under ECPA, but about whether those specific substantive and procedure requirements of ECPA should be imposed on foreign governments in all circumstances. Current law says yes, at least with respect to the content of communications. This, in turn, has negative privacy and security implications for both Americans and foreigners. It also puts American businesses in the crosshairs between conflicting legal obligations, with

negative consequences for both the economy and future growth of the Internet.

Consider an example. Imagine law enforcement in London is investigated a local murder and seeks the emails of the alleged perpetrator, a U.K. citizen. If the emails were held by a U.K.-based provider, law enforcement agents could, assuming compliance with local substantive and procedural requirements, obtain the data within days, if not sooner. If, however, the sought-after communications are held by Google or Facebook, U.K. law enforcement is essentially told, "Sorry, we'd love to comply, but are prohibited from doing so under U.S. law." U.K. law enforcement officials are instead told to initiate a government-to-government request for the data, employing the procedures spelled out under the Mutual Legal Assistance Treaty (MLAT) between the United States and United Kingdom. Pursuant to this process, requests are first reviewed by the Department of Justice; a U.S. prosecutor must ultimately obtain a U.S. warrant from a U.S. judge before the information can be shared with the U.K. government. The process takes an average of ten months. Meanwhile, the crime goes unsolved.

Foreign governments are understandably frustrated, and are responding in a number of concerning ways. These include the passage of mandatory data localization requirements as a means of ensuring access to sought-after data; unilateral assertions of extraterritorial jurisdiction, which puts U.S.-based companies in the middle of two competing legal obligations; and increased reliance on malware and other opaque means of accessing data. These responses have negative consequences for American's privacy, security, and economy, as well as the future of the Internet.

There is good news, however. A draft U.S.-U.K. agreement, as discussed by David Bitkower, the Principal Deputy Attorney General for the Department of Justice at the February 25 hearing, would permit U.K. law enforcement officials to access the content of communications directly from U.S.-based providers when certain conditions are met. Specifically, it would permit U.K. law enforcement officials to access data of their own citizens, pursuant to their own procedures, in the investigation of local crime; it would *not* permit U.K. officials to directly access the data of U.S. citizens, legal permanent residents, or others located in the United States. The agreement is described as reciprocal – meaning that the United States could directly compel certain data from U.K.-based providers.

Such an agreement provides a much-needed safety valve. If successful, it could provide the framework for agreements with other like-minded nations. But it cannot be implemented without Congress. Specifically, Congress should amend ECPA to allow companies to respond to foreign law enforcement requests for the content of communications pursuant to the

kind of executive agreement being negotiated between the United States and United Kingdom. Congress should also specify the parameters of those agreements — including a requirement that such requests be signed off by an impartial and independent adjudicator, are targeted and narrowly tailored, and are subject to minimization procedures that protect against the retention and dissemination of non-relevant information.

2. **It's also been proposed that a foreign country must meet certain human rights requirements. What are these? How do we define what constitutes a human rights violation? Is failure to criminalize prostitution a human rights violation? What if a foreign country restricts or prohibits certain religious practices such as a ban on Islamic headscarves? Is that a human rights violation? In this country, it's certainly a freedom of religion violation under the First Amendment.**

As described above, it is counterproductive — and in fact ultimately damaging to American's privacy and security — to demand that all countries around the world obtain a U.S.-based warrant to access data on their own citizens in the investigation of a local crime simply because that data is held by a U.S.-based company. That said, the United States also has a responsibility to ensure that baseline human rights protections are in place when foreign governments demand such data. This is the case for two key reasons.

First, while the targets of foreign government requests under the proposed system will be foreign nationals that are located outside the United States, communications are inherently intermingled. It is likely — in fact almost certain — that such requests will at times lead to the incidental collection of U.S. citizen data and data of other persons physically residing in the United States. This reality provides both an opportunity, and arguably an obligation, for Congress to demand a minimal set of baseline standards — including a requirement that requests be approved by an independent and impartial adjudicator, be tailored to a person, account or device, be limited in duration, and be subject to minimization requirements that protect against the retention and dissemination of non-relevant information. These requirements are essential to protecting the interests of those persons that fall squarely within Congress's responsibility and authority to protect.

Second, it would be contrary to American values for companies to be handing over data that is used to unlawfully detain or abuse human rights activists, dissidents, or political opposition leaders, or to otherwise perpetrate human rights abuses. Foreign governments need not adopt the exact same standards as the United States — that is both an unrealistic and counterproductive expectation — but they ought to comply with baseline human rights norms before they can compel data directly from U.S.-based providers.

3. **And how do we balance this requirement with the political, diplomatic, or economic pressures to enter into an agreement with a country that may condone behaviors that we prohibit but who also may have a large number of citizens who use U.S. provider services and therefore could enact data production or data localization laws?**

Such agreements will never be a total bulwark against data localization laws. Absent some fairly significant reforms, there will continue to be nations that fail to meet the criteria that would enable expedited access to U.S.-held data. But even one agreement is better than no agreement. It can reduce incentives for data localization and other concerning responses by the foreign partner involved. And it can become a model for others. No such agreement can take place, however, without Congress first amending the Stored Communications Act to permit companies to share the content of communications with foreign law enforcement in specified circumstances.

Questions for the record from Representative Mike Bishop (MI-08):

1. **As we discuss a remedy for government to pursue information requests, how do you suggest we protect the rights and remedies for companies to challenge a search warrant?**

   It is important to note that the proposed framework — and draft U.S.-U.K. agreement — would *permit*, but not require U.S.-based providers to respond to direct requests for the content of communications from foreign governments when certain conditions are met. Companies always have the option to reject the request. It also will be important to ensure that partner governments provide a meaningful mechanism for companies to challenge the legality of the orders and protect companies from being forced to comply with unlawful or unreasonable orders.

2. **In today's world, data can be located on a server in one part of the world at noon and moved to another server in a different part of the world only minutes later. In addition, the location of the data may be different from the location of the customer, which may also be different form the location of the government making the request for content information. Why should the location where the data is stored be determinative of which law controls the law enforcement access to stored data?**

   I fully agree that location of data is a particularly poor determinative of law enforcement jurisdiction. (In fact, I wrote a law review article raising several of the concerns you mention above: *The Un-Territoriality of Data*, 125 Yale L. J. 326 (2015)). That said, nations around the world have long asserted the authority to compel the production of property, including data, located within their territory. The assumption that they can continue to do so prevails and is driving data localization mandates.

   The adoption of harmonized jurisdictional standards that better account for the unique features of data and minimize jurisdictional conflicts is needed in response. The draft U.S.-U.K. agreement provides one possible approach. Under the draft agreement, as it is has been described, jurisdiction to compel turns on the location and nationality of the target, rather than the location of the data. Specifically, U.K. law enforcement would be permitted to directly compel the production of data from U.S.-based ISPs about foreigners located outside the United States, but would be prohibited from doing so if it wanted data on U.S. citizens, legal permanent residents, or persons within the United States. When seeking data on U.S. persons, U.K. law enforcement would continue to be required to employ the Mutual Legal Assistance Treaty Process and ultimately obtain, via U.S. law

enforcement officials, a U.S. warrant based on a U.S. standard of probable case.

This approach reflects an understanding that the United States has a legitimate interest in setting the rules for, and governing access to, the data of its own residents and nationals. But the United States need not insist that the United Kingdom follow American procedures when it is seeking data on foreigners outside the United States, simply because the data happens to be held by a U.S.-based provider or located within the United States' territory. This kind of approach — pursuant to which law enforcement jurisdiction over data turns on the location and nationality of the target — is something that should be pursued and encouraged.

○