DATA STORED ABROAD: ENSURING LAWFUL ACCESS AND PRIVACY PROTECTION IN THE DIGITAL ERA

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JUNE 15, 2017

Serial No. 115–36

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

31–564 WASHINGTON : 2018

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR SMITH, Texas
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
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
KEN BUCK, Colorado
JOHN RATCLIFFE, Texas
MARTHA ROBY, Alabama
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
ANDY BIGGS, Arizona

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
THEODORE E. DEUTCH, Florida
LUIS V. GUTIÉRREZ, Illinois
KAREN BASS, California
CEDRIC L. RICHMOND, Louisiana
HAKEEM S. JEFFRIES, New York
DAVID CICILLINE, Rhode Island
ERIC SWALWELL, California
TED LIEU, California
JAMIE RASKIN, Maryland
PRAMILA JAYAPAL, Washington
BRAD SCHNEIDER, Illinois

SHELLEY HUSBAND, *Chief of Staff and General Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

CONTENTS

JUNE 15, 2017

OPENING STATEMENTS

WITNESSES

OFFICIAL HEARING RECORD

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

DATA STORED ABROAD: ENSURING LAWFUL ACCESS AND PRIVACY PROTECTION IN THE DIGITAL ERA

THURSDAY, JUNE 15, 2017

HOUSE OF REPRESENTATIVES

COMMITTEE ON THE JUDICIARY

Washington, DC

The committee met, pursuant to call, at 10:12 a.m., in Room 2141, Rayburn House Office Building, Hon. Bob Goodlatte [chairman of the committee] presiding.

Present: Representatives Goodlatte, Chabot, Issa, King, Gohmert, Jordan, Chaffetz, Marino, Farenthold, Collins, Buck, Ratcliffe, Roby, Gaetz, Biggs, Rutherford, Conyers, Nadler, Lofgren, Jackson Lee, Johnson of Georgia, Deutch, Cicilline, Lieu, Raskin, Jayapal, and Schneider.

Staff Present: Shelley Husband, Staff Director; Branden Ritchie, Deputy Staff Director; Zach Somers, Parliamentarian and General Counsel; Ryan Breitenbach, Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Aaron Hiller, Minority Chief Oversight Counsel; Joe Graupensperger, Minority Chief Counsel, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations; Veronica Eligan, Minority Professional Staff Member; Sandy Alkoutami, Minority Intern, Judiciary Committee; and Monalisa Dugue, Minority Deputy Chief Council, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.

CHAIRMAN 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 data stored abroad: ensuring lawful access and privacy protection in the digital era. I will recognize myself for an opening statement.

Today's hearing will examine various issues related to digital data, including international conflicts of law; storage and transmission practices; governmental acquisition challenges; and protection of consumer information.

This hearing brings together a diverse array of interests, including law enforcement, technology companies, the economy, and the importance of individual privacy and civil liberties throughout the world. In the digital age, U.S. technology companies have flourished and provide services to customers across the globe. However,

the rapid growth of international communications infrastructure has presented challenges as well as opportunities.

For example, there is a growing tension between U.S. law and foreign law, often with U.S. technology companies at the center. U.S. law restricts access to data by foreign countries making it difficult, if not impossible, in some instances, for foreign governments to obtain evidence of crimes or terror plots carried out by their own citizens. This has resulted in foreign governments enacting their own legislation to address the problem, including laws requiring U.S. companies, as a prerequisite for doing business, to comply with foreign government requests for data.

Others are considering legislation that would require U.S. providers to locate servers in the foreign country to ensure foreign jurisdiction over the U.S. provider. This is sometimes referred to as data localization. Moreover, certain foreign countries prohibit the removal of data from their boundaries.

U.S. law, by contrast, makes no distinction between data stored domestically and data stored abroad, nor with regard to the nationality or location of the customer. The result of these conflicts is that U.S. technology companies find themselves having to comply with either U.S. law or foreign law, as it is often impossible to comply with both.

This is an untenable situation. The last time this committee considered these important issues was prior to the Second Circuit's 2016 decision in Microsoft v. United States, where the court ruled that the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer email content that is stored exclusively on foreign servers.

Microsoft had refused to comply with a search warrant for email content on the basis that Microsoft stored the email data on a server in Ireland, rather than in the United States. In the wake of the Microsoft decision, other providers have refused to comply with warrants on the basis that some or all of the data pertaining to the subject of an investigation is stored on servers located outside of the United States.

In the courts, however, five recently-issued opinions diverged from the Second Circuit's ruling concluding that data must be disclosed pursuant to lawful process, regardless of the location of the data being sought.

It is clear that Congress must find a contemporary solution that embraces the modern manner in which data is stored and acquired internationally. A legislative fix to the Stored Communications Act is necessary to remedy the problem made clear by the Microsoft decision.

Furthermore, Congress should take additional steps to resolve the conflict of laws issues. Various options exist on this score. A formal, multilateral treaty could result in broadly raising international privacy standards to more closely match the United States' rigorous probable cause standard and would comport, to the Founder's insistence, that broad, international agreements affecting many parties require Senate consent and ratification.

Another option is bilateral agreements. The United States and the United Kingdom are currently engaged in negotiations on a bi-

lateral agreement that would authorize the U.K. Government to request data directly from U.S. companies in criminal and national security investigations not involving U.S. persons.

To ensure clarity on this point, any international agreement that provides access by a foreign government to communications stored or flowing through the United States will not authorize that foreign government to wiretap or target U.S. persons or those located in the United States. This restriction applies even to our closest ally in the United Kingdom. Such an agreement could only be used to obtain evidence on non-U.S. persons located abroad.

The potential U.S.-U.K. bilateral agreement may serve as a model for future agreements, relieve some of the international pressure on U.S. tech companies, and help to alleviate any conflicts of law related to requests by the U.S. for data stored abroad by U.S. companies. In order for an international agreement of this kind to take effect, Congress must first change U.S. law to grant specific authority for U.S. companies to respond to direct requests by foreign authorities and prescribe the criteria that must be met by the foreign government.

These are not the only options available to Congress. In addition, there are legislative proposals that would attempt to resolve conflicts by basing the authority to obtain information on the nationality of the targeted individual. The committee will continue to explore all of these aforementioned options.

Once again, House Judiciary Committee finds itself at the forefront of a pressing issue that impacts personal privacy, national security, and public safety, economic viability, and the rule of law. Members of this committee will continue to examine all options for a thoughtful and balanced resolution to this problem.

I appreciate our distinguished witnesses testifying today. I want to particularly thank one of our first witnesses, Mr. Paddy McGuinness, for agreeing to travel to our country during such a difficult period in the United Kingdom, which has suffered multiple terrorist attacks in recent weeks. We greatly appreciate your presence and your vital perspective on the challenges with new forms of digital data storage and transmission.

I want to thank all of our witnesses and I look forward to their testimony. And I now turn to the ranking member of the committee, the gentleman from Michigan, Mr. Conyers, for his opening statement.

Mr. CONYERS. I thank you, Chairman Goodlatte. To our colleagues and to our distinguished witnesses in the first panel, it seems we keep returning to the same theme; the statutes that protect our privacy and regulate government access to our communications were written decades ago before the invention of the internet and are in urgent need of an overhaul. Under your leadership, Chairman Goodlatte, we have already worked together to address one aspect of this problem.

The Email Privacy Act has passed unanimously in the House twice. That measure allows us to move to a clear, uniform domestic standard for law enforcement agencies to access the content of communications namely, a warrant based on probable cause. There is no reason that the Senate should not pass the same bill that the

House has approved in the past, so that we can turn to the important work before us on additional related issues without delay.

In this hearing, we will examine a framework that seems inadequate to the 21st century: our existing system of mutual legal assistance treaties, and the overseas application of the Electronic Communications Privacy Act. The mutual legal assistance treaty system was written for a different era, quite frankly. I agree with the long-held view of the British Government that it is absurd for a police officer investigating routine crime in London to have to wait months, sometimes years, to access digital evidence stored in the United States, evidence that relates entirely to their citizens and not to ours.

I also agree with the Department of Justice that we are now facing a reciprocal problem. The recent decision of the Second Circuit appears to limit the application of the Electronic Communications Privacy Act to the United States, which means that, while investigating crimes in the United States, even with a warrant, our government may not be able to access communications that are now stored around the globe.

These are both real problems, and I believe that Congress should act quickly to update our statutes accordingly. But I also believe that we must carefully evaluate the administration's legislative proposal. For example, I am not convinced that simply reversing the Second Circuit solves the problem presented to us by the Microsoft decision. We should address law enforcement's need to access the content of communications with proper legal process. But a straight reversal does little to address the challenges that face companies operating internationally or to accommodate the interests that foreign governments may have in protecting the privacy of their own citizens. We can achieve a better balance here.

Similarly, the proposed bilateral agreement framework is full of promise, but only if we get the details right. Implemented correctly, these agreements could counter the trend towards data localization, incentivize our partners to set better standards for data protection, and help our closest allies investigate serious crimes.

I am not yet convinced, however, that we have landed on the right criteria for determining which countries we should partner with under such a framework and under what criteria. I understand the need to be flexible in order to accommodate different legal regimes. But too much flexibility renders the criteria meaningless.

I am also not yet convinced that it is necessary to give foreign government access to live wiretap information as part of a package that focuses largely on stored communications. It is imperative that both the Congress and the public have a meaningful opportunity to comment on these agreements before they take effect.

Under the administration's proposal, the Attorney General is to give Congress notice 60 days before he or she intends to give a foreign government access to communications stored in the United States.

The proposal includes no mechanism for Congress to respond or for the public to weigh in before the new agreement takes effect. I am certain that we can do better to ensure confidence in the decisions of the Department of Justice. I appreciate that time is of the

essence and that this committee, the Judiciary Committee, must begin grappling with these issues without delay. I am confident that, working together, we are prepared to do so. And I thank the chairman for convening this important hearing, and we are ready to go. Thank you.

Chairman GOODLATTE. Thank you, Mr. Conyers. Without objection, all other members opening statements will be made a part of the record.

Chairman GOODLATTE. Now, we welcome our distinguished witnesses, and if you would both please rise, I will begin by swearing you in.

Do you and each of you solemnly 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. Let the record show that the witnesses answered in the affirmative.

Mr. Richard Downing is the Acting Deputy Assistant Attorney General in the Criminal Division of the Department of Justice. Previously, Mr. Downing served as Deputy Chief of the Computer Crime and Intellectual Property Section of the DOJ. During his tenure there, he supervised the prosecution of hacking, identity theft, and intellectual property crimes; oversaw policy and litigation governing the constitutional and statutory rules for the collection of electronic evidence; and supervised the development of international law enforcement cooperation related to cybercrime and intellectual property crime.

Before joining the Department of Justice in 1999, Mr. Downing served as an assistant district attorney in Philadelphia. He is a graduate of Stanford Law School and received his bachelor of arts from Yale University.

Mr. Paddy McGuinness is the United Kingdom's Deputy National Security Adviser for Intelligence, Security, and Resilience at the Cabinet Office. In this role, he supports the Prime Minister and National Security Adviser on all aspects of counterterrorism, cybersecurity, national resilience, and crisis management and security policy; as well as the governance, resourcing, and policies surrounding the U.K.'s intelligence agencies.

Mr. McGuinness has had an expansive career in Foreign Service since joining the Foreign & Commonwealth Office in 1985. He has served in Yemen, United Arab Emirates, Egypt, and Italy, holding leadership positions covering the Middle East, counterterrorism, and all aspects of cybercrime. Mr. McGuinness attended Ampleforth College and the University of Oxford.

I want to, again, thank the witnesses. Your written statements will be made a part of the record in their entirety. We ask that you summarize your testimony in 5 minutes. 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 your testimony. When the light turns red, it signals your 5 minutes have expired. And Mr. Downing, you may begin. Welcome.

STATEMENTS OF RICHARD DOWNING, ACTING DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE; AND PADDY MCGUINNESS, U.K. DEPUTY NATIONAL SECURITY ADVISER, OXFORD, U.K.

STATEMENT OF RICHARD DOWNING

Mr. DOWNING. Good morning, Chairman Goodlatte, Ranking Member Conyers, and members of the committee. Thank you very much for the opportunity to testify on behalf of the Department of Justice concerning a significant impact on public safety and national security.

We are, unfortunately, living in a world where criminals, both in the U.S. and abroad, prey on Americans. Cybercriminals steal our intellectual property and empty our bank accounts; terrorists threaten us with brutal attacks; and pedophiles seek to sexually exploit our young children. Never before have we had as a great a need for access to electronic evidence in order to solve crimes, bring criminals to justice, and to project public safety.

Today, U.S. communication service providers often store customers' data, including the data of American customers in data centers in foreign countries. Some providers constantly move that data in and out of the United States and around the world, sometimes minute by minute, for business efficiency and other purposes.

It is against this backdrop that I want to deliver two important messages. The first is this: the rule announced in last year's Second Circuit decision in Microsoft v. United States is undermining the public safety of the American people. We believe the case was wrongly decided. That decision and the choice by major U.S. providers to provide its ruling across the country is preventing effective and efficient access to critical evidence where the provider has chosen to store that data overseas.

And the remarkable thing is that it sometimes prevents us from using a warrant, even when the crime, the victim, the offender, the account holder are all inside the United States. These developments are affecting law enforcement efforts in just about every kind of case that we investigate.

Let me give you a couple of examples. In one case, a U.S. defendant was arrested for sexually assaulting children, and a search warrant was issued and served on Google for the content of that offender's account. Google did not produce photo attachments in that account, and investigators need those photos in order to identify and locate other child victims.

In a drug trafficking investigation involving targets in the United States, Canada, and China, a search warrant was issued to Microsoft. Microsoft did not produce any email content. Investigators need that content to identify the members of the drug trafficking organization.

We need swift action by Congress to correct this problem. The Department recommends a clarifying amendment that would explicitly require providers subject to the jurisdiction of the United States to disclose data, pursuant to legal process, no matter where the provider has chosen to store the data.

This brings me to the second message. The amendment should be passed as part of a package that would also improve cross-bor-

der access by foreign law enforcement to data stored within the United States, a so-called U.S.-U.K. framework. We are, of course, not alone in facing challenges in protecting our citizens due to the globalization of the U.S. service providers.

Our foreign law enforcement partners also face obstacles in obtaining electronic evidence stored outside their territory. Increasingly, those countries have issued their own legal process for evidence from U.S. providers. And, at times, the providers have to decide whether to follow the foreign laws and obligations or the restrictions on the disclosure found in the Electronic Communications Privacy Act.

That is why a group of large U.S. providers came to the Department of Justice and asked us to help develop a new bilateral framework for cross-border data access. These U.S. providers want to be able to comply with foreign court orders, without violating U.S. law, in situations where the U.S. interest in protecting the information from such disclosure is at a minimum.

Consider the investigation of a homicide in the U.K.: Scotland Yard opens an investigation, questions witnesses, searches houses, seizes phones. Everything to do with the case, the victim, the crime, the suspects, is in the U.K. except, that is, for the victim's email and social media accounts, which are stored in the United States. It is pure happenstance that the data is stored here, and there is no meaningful U.S. nexus to the case.

This is a prime example of where it makes sense for U.K. law to control. Congress should enact legislation to lift the restrictions in U.S. law where a bilateral agreement exists between the two countries. We have explored how such an agreement would work with the U.K., and if the approach proves successful, we would consider it for other like-minded governments who respect the rule of law and have robust privacy safeguards.

Thank you again for the opportunity to testify on this important issue, and I look forward to answering your questions.

Chairman GOODLATTE. Thank you, Mr. Downing.

Mr. McGuinness, welcome. We are especially pleased that you have made a long trip to be with us today to testify about the importance of this issue. So, welcome.

STATEMENT OF PADDY McGUINNESS

Mr. MCGUINNESS. Chairman Goodlatte, Ranking Member Conyers, members of the committee, it is an honor to appear before you on behalf of Her Majesty's government. Before I turn to the substance of my remarks, I would like to express my sympathy for yesterday's shocking attack against this Congress, its staff, friends, and your police service.

We wish Congressman Scalise and all those injured a speedy recovery; they and their families are in our thoughts and prayers. It is a symbol of the resilience of this House that you are pressing ahead with business and tonight's baseball game as well.

I had the honor of appearing before the Senate Judiciary Committee on the 24th of May, 2 days after the cowardly attack in Manchester, which killed 22 people and injured many more. I now return to Congress in the wake of the attack on London Bridge on 3rd of June, during which eight innocents were killed and 48 were

wounded. Five other attack plots have been filed since our parliament at Westminster was attached on the 22nd of March.

Put simply, the scale of the threat against the United Kingdom, its citizens, and the foreign citizens who live there is unprecedented. It is a matter of pride to us that we are resilient. We reacted fast to the attacks and have quickly returned to normality. Manchester and London are safe and open for business.

But our returned Prime Minister has also caught our mood when she said, "Enough is enough." That is why she sent me to appear before you today to explain why Congress should, in our view, amend U.S. law to permit a bilateral agreement on data access.

As Deputy National Security Adviser, my responsibilities are made more complex by a world connected by the internet. Serious crimes like human trafficking, child sexual exploitation, drug traffic, and money laundering do not respect borders. A British citizen who has joined Islamic state can cause untold havoc through a cellular phone, a laptop, and a Wi-Fi connection.

I am not a lawyer, but I know that we share an extraordinary legal heritage derived from the common law with respect for freedom of speech, privacy, and the rule of law. Law is the bedrock of our mutual prosperity. It has enabled America's ingenuity and entrepreneurial spirit to flourish, and, thus, all to benefit. Nowhere is this more evident than in the success of American technology companies. And the people of the United Kingdom are amongst the most enthusiastic users of the services of those companies. Unfortunately, through no fault of the companies, that includes criminals and terrorists.

Today, a British police officer investigating serious crimes taking place in London can get a warrant for the communications between criminals. If those criminals communicate using the services of the U.K. company that warrant can be executed, the crime investigated, and citizens kept safe. When those same criminals communicate, as 90 percent do, through an American tech company, the current law of the United States can prevent that company from providing the content of those communications to the U.K. police officer.

Crimes go on with the criminals unpunished as a result. This cannot be right. It is arbitrary. It places U.S. companies in an impossible position, stuck between the laws of two close partner countries. It constrains law enforcement, and it makes us all less safe. The need to resolve this is urgent. That is why I have come before you today to ask that you make a technical adjustment to U.S. law to remove the restriction on U.S. companies providing date in tightly defined circumstances. This will enable a U.K.-U.S. bilateral agreement to be signed.

You will rightly be concerned, as our lawmakers have been, that privacy, freedom of speech, and other freedoms be protected. Let me, therefore, make clear what this proposal is not an expansion of U.K. investigatory powers. It does not impact the privacy rights of U.S. citizens and residents, any agreement would not permit the U.K. to target U.S. persons or anyone in the U.S.

It is not about encryption; it is entirely encryption neutral. It is not about obtaining communications in bulk. The orders under our agreement would be for individual targets. It is not compulsory; it

simply removes the current legal bar to U.S. companies responding to U.K. orders. It is not one-sided; it is reciprocal. The U.K. law permits the U.S. use of the agreement's provisions in the U.K.

This present conflict of laws is unsustainable. Some countries are requiring data to be stored in their territories. Others are arresting or threatening company employees. This is not good for our mutual prosperity or security. Now, Congress has the opportunity to create a solution to set the standard for transparency, privacy, and legality for the rest of the world to follow. Thank you for the opportunity to appear here before you today. I look forward to answering your questions.

Chairman GOODLATTE. Thank you, Mr. McGuinness. And I will begin the questioning under the 5-minute rule. Mr. Downing, the Department of Justice is engaged in talks with the U.K. Government about a bilateral agreement that would allow the U.K. Government to go directly to U.S. technology providers to obtain stored data, such as emails or to serve wiretap orders for real-time intercepts of communications in criminal and national security investigations not involving U.S. persons. Why is this necessary?

Mr. DOWNING. This sort of agreement has a number of benefits. We have already touched on several of them in a variety of different ways. It is very important for us to help our colleagues and allies to solve the domestic security problems that they have, and it also helps the U.S. companies to make sure that they are avoiding any conflicts of law. It reduces incentives for data localization and creates incentives for countries to raise their own standards of protecting privacy and civil liberties. And as it has been mentioned, it is very important that we have the ability to get access to data in foreign countries for our needs when that data happens to be stored there in appropriate cases.

Chairman GOODLATTE. Is a formal treaty instead a better mechanism that would raise international standards more broadly while accomplishing the stated goal with multiple signatories at once?

Mr. DOWNING. It is an interesting question about what the correct or the best mechanism would be for accomplishing this kind of a goal. Let me begin by saying though, that we very much expect that we would have close collaboration with Congress as we begin to think through these questions, to work with the U.K. and potentially with further countries down the road.

We also have to think about how it would be most efficient in order to be able to build out this idea to further countries as well. We think that the proposal that we put forward really does accomplish a good balance there. It has a very strong role for Congress at the beginning, of course, by setting up the rules, the baseline, the requirements.

And then, of course, as was mentioned, there is a traditional role in the back end where Congress would be notified before anything was entered into. And, of course, that would give an opportunity for Congress to weigh in at that point if it chose to do so. So, we think that a bilateral executive agreement rather than a treaty is probably a more efficient and effective way to get the job done and to help all the benefits that I have just mentioned.

Chairman GOODLATTE. Thank you. Mr. McGuinness, under the bilateral proposal there would be absolutely no bulk collection of data and no investigations of Americans. Is that correct?

Mr. MCGUINNESS. Absolutely.

Chairman GOODLATTE. And what mechanisms would be in place to ensure that American's privacy is protected while also allowing for lawful access by British authorities to British citizens' email content that resides in the United States?

Mr. MCGUINNESS. So, in order to protect U.S. citizens and U.S. persons, we should be clear at the outset that this agreement specifically excludes U.S. citizens and anybody in the United States. That is not the purpose of the access to data. So, that is excluded. We have equivalent high standards to the United States in the way in which we oversee and manage inception of communications.

We monitor closely what is being done, train, study, and have oversight regimes, which means that we have a degree of confidence in what we are able to do. Having said, we will not, even inadvertently, intercept the communications of Americans. We are confident that we can put in place systems and processes that will protect their rights.

Chairman GOODLATTE. What is the standard that British authorities must meet in order to obtain the email content of British citizens in the United Kingdom when the content resides in the U.K.?

Mr. MCGUINNESS. So, we have a concept that we use, which is established and proven and tested in judicial process in the United Kingdom, which is necessity and proportionality. This is a high bar for gaining access. Necessity relates to statutes. So, there are only certain statutory reasons where you might be able to gain access. That would be national security, serious and organized crime, threats to economic well-being.

So, those would be covered. Certain restricted set of organizations can apply for warrants to intercept communications. Necessity means, also, that the individual or entity being targeted; there must be a basis for targeting to them. So, they must have been in dialog with Islamic state. They must have come up in searches relating to child sexual exploitation or whatever it might be.

And then we have proportionality and proportionality tells us that we must use the least intrusive means to enable the investigation. And if a less intrusive means is available we should use that. So, it is possible that you will have a necessity justification, but proportionality will mean that a warrant is not agreed. Proportionality is a critical concept when we have judicial review of these warrants.

Chairman GOODLATTE. And how often do British authorities face obstacles to obtaining lawful access to information held by U.S. companies when conducting investigations?

Mr. MCGUINNESS. So, as I said in my opening statement. Happily, there is an enormous penetration of the British market by U.S. tech companies. Everybody, myself included, makes extensive use of multiple apps when they wish to go about their daily life. What that means is in almost every case that we look at there is extensive use by the target of investigation of U.S. applications provided by U.S. companies. And that means that in almost every case

there is a basis to potentially to ask for data if that particular communication use is relevant.

Chairman GOODLATTE. And, finally, could you explain the new judicial system in the U.K. under the investigatory powers regime? In which ways did passage of the Investigatory Powers Act strengthen and bring more accountability to the U.K.'s judicial system?

Mr. MCGUINNESS. Certainly. So, in everything I say today I am going to be talking about the system that will operate under the Investigatory Powers Act, which you mentioned, which was passed in November 2016. They are being introduced through this year progressively and that is what I will be talking about.

We are having a double lock. So, an intercepting agency, the police service or security service, will write a warrant. They will submit it to a certain defined set of senior Ministers who will either agree or disagree with the warrant. If it is agreed, it then goes to a Judicial Commissioner.

And that Judicial Commissioner will review the warrant in particular on these issues of necessity and proportionality, but also the public interest and privacy and the need to maintain the security of telecommunication systems. And, if satisfied, will also sign the warrant. So, what you get is a double lock. The Minister signs it, and then the judge signs it. If the Minister refuses, it does not go to the judge; and if the judge refuses, it does not go through.

Chairman GOODLATTE. Thank you. The gentleman from Michigan is recognized.

Mr. CONYERS. Thank you, Mr. Chairman. If you do not mind, Mr. Downing, I am going to ask one question of our visitor and guest here. Welcome to the Congress, to the House Judiciary Committee. We are honored that you would travel as long as you did to join us. And I wanted to just ask you one: criticism of the administration's proposal is that it does not reflect one of our legal traditions that warrants should issue only with probable cause. I understand that the British system works differently, but would there be a problem with tightening the reasonable justification standard reflected in the current proposal, in your judgment?

Mr. MCGUINNESS. So, thank you for the question, and, indeed, thank you for hearing me today. The British Parliament passed the Investigatory Powers Act in November 2016 with a very large majority. It is more than bipartisan, and it is very much the will of the British Parliament that this is the way in which we should manage intrusive powers of this kind. It is founded on established British legal mechanisms, whether that be judicial review or necessity and proportionality.

It was considered on the floor of the House of Commons whether or not we should introduce a new and different standard, a new and different standard. And it was concluded that a new and different standard would contain risk because we could not be sure how it would be implemented, and it would not have been tested as necessity and proportionality have been tested.

So, I think my answer to you is we have very high standards in the United Kingdom. We come from the same legal rootstock that you do. And we have established protections for freedoms, for privacy, for freedom of speech. And that is at the very heart of British

life. And we have legal mechanisms that are proven to deal with that and those are the ones that should apply to any application for data.

Mr. CONYERS. Thank you. Turning now to the Department of Justice representative, Mr. Downing, and thank you for your cooperation. Let's compare two different proposals to solve the problem presented by the Microsoft decision.

The International Communications Privacy Act, as introduced by Mr. Marino, which allows the government access to communications stored overseas, but also requires the court to consider the nationality of the targeted user, as well as any concerns our allies might register about the privacy of their own citizens. It recommends a simple reversal of the Second Circuit. Why should we simply reverse Microsoft? Does it matter that litigation is ongoing? And should we not make some accommodation for our foreign partners?

Mr. DOWNING. Thank you very much for the question. We believe that a clean reversal of the Microsoft decision makes the most sense because of the very real and significant harms that are being caused by that decision along the lines that I have outlined already. Litigation is ongoing. That is actually a symptom of the fact that we feel very strongly about this and the significance of the problem. We are seeking every means that we have available to try to get that situation solved, including in the courts where we have that right to bring those cases. And, of course, that is why we proposed to Congress a way of fixing it.

To your last question: what is the issue with respect to notifying foreign governments? There is a number of aspects to that situation that I would highlight for you. First of all, it is extremely unusual that we would notify a foreign government when we take investigative steps against one of their citizens. We might search the home of a Russian organized crime figure or a Mexican drug dealer inside the U.S., and we would not give those governments notice. And we would not do it even when we did use a mutual legal assistance treaty request.

So, if we sought information from France about a Spanish citizen, we would not turn around and tell Spain that we had done that.

But more practically speaking, there are a number of concerns that we have about a system of notice to foreign governments. We are concerned about notifying a foreign government, which might tip off the target of the investigation. It does not make much sense to notify the Chinese about a Chinese hacking investigation that we are doing or a Syrian terrorist about a terrorist investigation. We are concerned about the reciprocity. Are they granting the same rights to Americans?

It does not make much sense to give rights to foreign citizens that they are not willing to give to us. We often do not know the nationality of the target. So, how do we deal with the situation where somebody is distributing child pornography but using the anonymity of the internet to prevent it? And, perhaps, most importantly, we need a system that is going to work swiftly and efficiently in order to get us the evidence that we need in order to protect Americans.

So, a lot of steps and confusion and notification and delay. It is not what we would favor in our position.

Mr. CONYERS. I thank the witnesses, and I thank the chairman.

Mr. ISSA [presiding]. Thank you, sir. I will now recognize myself for a round. I picked up on your statement you did not think we should have a treaty. We have an extradition treaty with the United Kingdom, right, Mr. McGuinness?

Mr. MCGUINNESS. Yes, you do.

Mr. ISSA. And why is this not an extradition of an asset of an entity? Why is it so different, particularly when our laws are not harmonized and not likely to be harmonized as to privacy?

Mr. MCGUINNESS. So, the reason why we have come to this is because of an important dialogue.

Mr. ISSA. No, no, no. That was not the question. I apologize. The question is, why not a treaty? The bar is higher. The standard is higher. It has to be ratified. But, you know, there are about 214 ambassadors. But let's call it 194 countries that the United Nations more or less deals with, 80 or so of which we have no extradition treaties with.

So, slightly more than half the world, at least relative to the United States, has agreed to a procedure for extradition. And I will just briefly go through Mexico. In Mexico, we waive the death penalty when we want somebody who has fled who is accused of a capital crime. We waive it in order to get them back. It is part of our treaty process.

So, when we look at the likelihood that European Union and Britain collectively and now separately will have different standards sooner or later, always almost, in some way for the nuances of how you have to treat data both of U.S. persons and British persons. Are not we in a situation in which a treaty is a better binding and more appropriate bilateral agreement? And I do not want to belabor it. It is the Senate's job. But, you know, is there any particular justification other than not doing a treaty is quicker and easier?

Mr. MCGUINNESS. So, I do not believe this is analogous with extradition. It is absolutely not that.

Mr. ISSA. OK, well, let's go through that. The data that is being sought can put somebody in the gas chamber in this country. The data being sought can cause people to be asked for extradition. Often, the information that is being looked for will lead to extradition. Let's put it this way: the Fourth Amendment looks to unreasonable search and seizure. It is specific and it has the same power as the other nine in our country.

So, when I look at these inherent protections, and I will get past treaty for a moment, but when we look at a bilateral agreement of any sort between our two Nations you are going to want to protect British persons at a level that you specifically protect British persons. And we are going to want to protect U.S. persons at a level that we want to protect them. And then, we are going to agree based on disparate standards in all likelihood that we are going to exchange data under certain circumstances, correct?

Mr. MCGUINNESS. It sounds right.

Mr. ISSA. And you did a great job of explaining in detail how you would come to produce this subpoena or warrant and send it to us.

But I can tell you from this committee, that there are processes in this country that are virtually invisible that are done administratively that could lead to a request for data that currently we are not comfortable with sometimes in the U.S.

So, let me ask you a real question. Britain and the United States could not be closer, probably than any other two countries when it comes to our general view of what is right and wrong in the world. But are we not held to whatever we do between our two countries, to be, if you will, the form. The block on which we are supposed to build other bilateral agreements.

And so, when I look at nations like Cuba, North Korea, Afghanistan, the list is long that we do not have extradition with. What am I going to do when they want data for their persons? How am I going to look at countries who do not necessarily have the same standards and the same rule of law and yet will insist that they have gone through a process, and I need to give them the information they want?

Mr. MCGUINNESS. If I may, you are going to hold them to the very high standards that are proposed in this proposal that have come to you here in Congress. And I long to see the day, when in North Korea, or Cuba, or any of the States you mention, they have the kind of protections you have in the United Kingdom.

So, there absolutely is a mechanism for leading States along the road. And I would observe that one of the drivers for the revision of the judicial oversight of our warranty where we had a different system prior to the November 2016 Act, was the fact that we knew that it would satisfy the companies who are advocates of this agreement and the United States.

Mr. ISSA. By the way, the Vatican is on that list that we do not have extradition with.

So, I will close by saying I am deeply concerned that we do have to be cognizant that, with 80 countries that we cannot agree to extradition with, the question of whether those 80 countries, if we fail to reach a more common standard, one that we could reciprocate with everyone on, they are going to tend to say, "Gee, it is a wonderful world. We want our data located in our country." And it will be an excuse for China, Libya, the Vatican to each have their own servers. And, although I trust the Vatican's business model is such that the server data will be limited, I cannot say so of China. Thank you.

And we now go to the ranking member of the Intellectual Property Subcommittee, Mr. Nadler.

Mr. NADLER. Thank you very much, Mr. Chairman. Mr. Downing, before I get to the specifics here, I want to have a couple of preparatory questions. It has been reported recently that it is now the policy of the executive branch not to answer questions from minority party members of Congress on any subject whatsoever and to routinely ignore them. So, my question is, is it the policy of your Department, the Department of Justice, not to respond to congressional inquiries from Democratic members?

Mr. DOWNING. I am afraid I do not have an answer for you either way on that. I do not know whether that would be binding on us or where our position is on that.

Mr. ISSA. If the gentleman would yield?

Mr. NADLER. Sure.

Mr. ISSA. I would be pleased to say that, in fact, in parliamentary systems, including Great Britain, the minority right is extensive.

Mr. NADLER. I am glad to hear that, but I am concerned right now with the congressional system designed by Mr. Madison. Mr. Downing, if I ask you a question today, which I will do in a moment, you will presumably answer it.

Mr. DOWNING. I will.

Mr. NADLER. Thank you. But if I put the same question in writing and send it to you, will you answer it?

Mr. DOWNING. I will do my best to answer all the questions for the record that come forward from the committee.

Mr. NADLER. Despite what we hear is the new policy of the administration?

Mr. DOWNING. I, as I said, do not have a strict answer for you on that particular question.

Mr. NADLER. OK. Let the record reflect that that was not answered, and that is very disturbing that you cannot answer the question in the negative, to put it mildly.

Let me ask Mr. McGuinness, you described the system in Britain of proportionality and necessity. We have the system of probable cause. Could you tell us how they would differ in a given case, I mean how you would look at proportionality and necessity in a different way than we might look at probable cause? I mean, what is the practical impact of this?

Mr. MCGUINNESS. So, as I said in my opening statement, I am not a lawyer, and I am certainly not an academic lawyer. And my ability, frankly, to compare between different legal systems and the standard within them is somewhat limited.

So, I am going to just reflect that necessity and proportionality are a very high standard analogous, I believe, to much that is in probable cause, and, certainly, established in the British legal system and a basis for testing and sometimes refusing proposals for warranty and for action by the State.

Mr. NADLER. Well, since you are not a lawyer, I cannot ask you the next question, which I will simply state for the record as a matter of curiosity. And that is, what happened to probably cause in British legal history since I thought it was there in the 1760s? But we will worry about that at a different time. I am concerned the proposed legislation would allow foreign governments to request assistance from the U.S. providers to intercept communications in real time without requiring compliance with Wiretap Act standards. Mr. Downing, could you comment on that and the implications of that?

Mr. DOWNING. Absolutely. I think it is important to start with a baseline that has been discussed, these kinds of orders would not be targeting U.S. persons. So, you have got to picture the paradigm case here as a——

Mr. NADLER. Excuse me. It would not be targeting, but if information was collected on U.S. persons, that could be given back as a section 702 problem?

Mr. DOWNING. It is possible that U.S. person information could be intercepted. But if you think about the paradigm case of an or-

ganized crime boss who is setting up a hit and is talking to people, and the U.K. needs that information, it is pure fortuity that the data happens to be stored in the U.S. And so, the U.S. interest in the application of our law is at a minimum.

Nevertheless, the agreement that we have proposed would create strong baseline rules. There would have to be articulable and credible facts and particularity, which are ideas, which are another way in some ways of saying probable cause. There have to be the exhaustion of alternatives. The necessity idea. There has to be for a limited duration. So, all these things are in play and I think it is important that we understand that there are real restrictions as well. And I think, if I may, one final point. The U.K., like the U.S., believes that wiretapping is a critical part of being able to protect our public safety. If we do not address this problem as part of this——

Mr. NADLER. Yeah, we have clearly got to address the problem just looking at these standards. In my little time left, might you be better qualified to answer the question I asked Mr. McGuinness about the difference between the British concepts of proportionality and what did he say? Proportionality and——

Mr. DOWNING. Probable cause?

Mr. NADLER. Proportionality and necessity on the one hand versus probable cause on the other.

Mr. DOWNING. I am afraid I am, of course, steeped in the U.S. legal system and not so much on the U.K. side. However, I would agree with Mr. McGuinness that I think those ideas achieve the same kinds of goals. They need to be real problems, real faced with proportional consequences. They are analogous, if not identical. But I do think it is important to recognize that we cannot have a system where every country has to have exactly the U.S. rules, or we are never going to get anywhere with this. It is important that we have baseline rules; everybody is respecting of privacy and we have rules.

Mr. NADLER. In other words, we can be imperialistic, but not that imperialistic.

Mr. DOWNING. That is right. We would not like it very much if they imposed their rules on us. I think we need to be at least a little bit balanced about it.

Mr. NADLER. Thank you, my time has expired. Thank you, Mr. Chairman.

Mr. ISSA. Thank you. We now go to the chairman of the Oversight Committee, Mr. Chaffetz.

Mr. CHAFFETZ. Thank you. I do appreciate it, former chairman, but——

Mr. ISSA. You will always be a chairman to me, Jason.

Mr. CHAFFETZ. All right, thank you. Mr. McGuinness, we cherish our relationship with the U.K., and we thank you, personally, for what you do and for the relationship between the two countries.

Mr. Downing, I think it is important for us to understand sort of the baseline, because if we are going to be trying to do things in other countries, I am still concerned about what we do and do not do in this country. So, first, help me understand geolocation. What does the Department of Justice's position on geolocation? My concern is and question for you is does the Department of Justice

consider that metadata, or is that content? How do you view geolocation?

Mr. DOWNING. Thank you for the question. Geolocation is a difficult and complex topic, as I am sure we understand. And we have had discussions about this in the past as well. There are different kinds of geolocation that could be content or could be non-content. It could be content if it is, say, the location data that is embedded inside of a picture file and is being passed as part of an attachment to an email.

It could be non-content if it is simply information that the provider is gathering about its customers' use of cell towers. It does not actually have any content-full value in that situation. It is simply an observation of the company about which tower a particular phone is pinging off of when it is being used. So, I think——

Mr. CHAFFETZ. There are times when geolocation is content, correct?

Mr. DOWNING. There can be times, yes.

Mr. CHAFFETZ. I mean, have you written this out? Is there some sort of definition that the Department of Justice is taking on the nuances of what geolocation is and is not? Because I would argue that, by and large, geolocation is content. It is the content of my life. If you can tell where I am going with this phone all of the time, you can pretty much tell the content of my life. And yet I worry about what you are gathering and not gathering, and I do not understand the definition.

Mr. DOWNING. So, our view of the rules that apply when we are gathering geolocation information vary depending on what type of geolocation it is. Our position has been that, if we are merely talking about what cell tower your phone is pinging off of, that that is covered by the Stored Communications Act and would require a court order before we are able to obtain it. This is an issue, actually, that the Supreme Court has just recently decided to serve petition on. And so, it will be very interesting to see how they resolve that question.

There are other kinds of geolocation information such as GPS, which is very specific and generally gathered prospectively. In those situations, I think as you know, we use a warrant for that. So, I think we use a nuanced approach. We look at the law that applies and try to do our best to comply with that law. It varies.

Mr. CHAFFETZ. Well, I do not know that every department and agency, even within the Department of Justice, uses that same standards. And, certainly, when you start to look at Homeland Security and others, they do not necessarily follow those same standards. And so, I guess what I am looking for in writing the definition of what that is.

Let me ask you very quickly: on social media, is it the position of the Department of Justice, particularly in the hiring and the monitoring of existing security clearances, to look at social media? Is that fair game or not fair game?

Mr. DOWNING. You know, I am afraid I do not know the answer to that question, but I would be happy to take it back to get you an answer.

Mr. CHAFFETZ. I think it is important. It has been a struggle, particularly in the realms of security clearances, even to get our

own Federal employees to be able to look at, you know, when they are assessing security clearances, to look at their social media and what not. And the last thing I want ask you about is facial recognition. We know the Department of Justice, specifically the FBI, is building a database of facial recognition. What direction is this going? Where are the standards? What is happening or not happening in the building of the facial recognition database?

Mr. DOWNING. So, I am not intimately familiar with what the FBI is doing in that regard. My general impression is that they are developing a database similar as they would with fingerprints and other things of people who were of interest in an investigation, who were arrested in order to be able to better——

Mr. CHAFFETZ. OK, but please do look at this because that is not what they are doing. If they were looking at criminals, people who were incarcerated, people who committed crimes, that would be one thing. But what they are doing is now more than one out of every two members of our society are in the database or they have access to that database, I should say, because their proactively going and gathering all the pictures that are on driver's licenses.

A lot of States have MOUs with these States. And the FBI was supposed to provide some notification. They did not do that. I have a fundamental problem and challenge in taking innocent, suspicion-less Americans and building a database because we have shown we cannot protect our databases. So, I think we need to ferret that out as a committee. I will not be here much longer, but I do think that is something the committee should take a much closer look at. With that, I yield back.

Mr. ISSA. I thank the gentleman. And, Mr. Chaffetz, in case we do not get another public opportunity on this committee to thank you for your service for so many years and for your championing peoples' privacy rights including geolocation. It is something that on this side of the day is center and left. We are all noting that someone is going to have to pick up that chalice on your behalf.

Mr. CHAFFETZ. Well, thank you. I am honored to serve. So, thank you. I appreciate it.

Mr. ISSA. Thank you. And with that, we go to the gentlelady from San Jose, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman, and thanks to the two witnesses, especially our friend from Great Britain for his long travel to be here this morning. And it is a pleasure to hear your viewpoint.

Obviously, our country and yours are close partners in the fight against crime as well as the fight against terrorism. So, your words mean a lot to us, and we weigh them carefully as well as, of course, our own Department of Justice. You come here at a time, however, when we are very much reviewing our own due process rules, and also some of the other issues that are post challenges, not only to our government but to our people.

One of the things I wanted to raise, I understand that you are here for the best of motives, but we have a new General Data Protection Regulation that the European Union passed in April of last year, not of last year; it was 2016. It goes into effect in May 2018. And here is my understanding of it, and correct me if you think I am wrong.

The GDPR requirement will be the data stored in the EU can only be transmitted to a non-EU country, for example the United States, in response to a law enforcement request through a process that is ratified in a treaty. In fact, we would not use an MLAT, which we all agree is inadequate, due to it is complexity and the time.

But I think we are going to have to have a situation next year where American companies are going to violate the law no matter what they do. And I am concerned about that, that you are here for this matter, but this is going to hit the fan next spring. And I do not think it is fair to set up a situation that great American companies are going to be in violation of the law no matter what they do, and we just ignore that.

So, could either one of you comment on that?

Mr. DOWNING. Do you want to go first?

Mr. MCGUINNESS. So, I should say that that is not our understanding of the GDPR, the General Data Protection Regulation. And the implementation of it is being worked through, at the moments at European Union level and in individual member States. So, we are working on that at the moment. And when we look at Article 48, which would appear to have that effect, we see that it has been nuanced.

And it is our belief, both that the provisions we have, and, I think it is clause 53 of our Investigative Panels Act, which allows for the reciprocity, which I described. Both that, and the GD pair itself would allow for transfer under the kind of agreement that we are working on here. That is our belief.

Mr. DOWNING. If I could just add, I concur with that. We have been having some discussions with your national data privacy experts and with the European Commission, and as a result of those discussions, the Department believes that the concerns that have been raised are inaccurate and over stated. We do not believe that the GDPR will pose significant conflicts for U.S. companies to comply with U.S. demands.

Ms. LOFGREN. Well, you know what I would really like from both of you following this hearing? I would like a statement that is definitive on that, that companies could take to the bank and that they could give to a court and as a shield, that they have relied on in good faith, the representations.

I, personally, think we ought to do a treaty that clarifies this, but I do not think there is much activity on that more that there should be. I am, actually, I will be honest, a little bit reluctant to take action until this other matter is addressed. And I do not think the administration, from what I have heard, is actively pursuing it which I think is a mistake. I will just lay that out. And I think I am not the only member who has that concern.

But if you could provide those definite statements from the highest levels of your government, that would be very helpful I think to all of us. And certainly, to American companies that feel really kind of stuck at this point. Mr. Chairman, I see my time has expired.

Mr. ISSA. If the gentlelady would let me have her 14 seconds. Mr. Downing, I am going to ask you the follow-up question to hers. If I were the Attorney General and I asked you to make the case

based on the European Union order, that you did have that authority, would you not be able to make that case or at least in good conscience you would plead it? Because the ordinary reading, certainly, would allow you to make that case.

Mr. DOWNING. Make the case? I am sorry, I am not following you.

Mr. ISSA. Make the case that you could not transfer to the U.S. that data as a non-U.S. entity based on the simple reading that the gentlelady from San Jose alluded to.

Mr. DOWNING. Well, I cannot say that I know the intimate details of the different articles of the GDPR. But in speaking with people it seems fairly clear that there are a number of exceptions and loopholes, and changes, and whatnot, that apply in this kind of situation——

Mr. ISSA. There is always fertile ground for attorneys to make a case in a court.

Mr. DOWNING. Well, I certainly agree that having a clear and definitive from the European Union about this would be helpful. But I just want to be clear, we have to be careful about basing our legislation on concerns which may be completely empty.

Mr. ISSA. Well, I join with the gentlelady in making the belief that, until it is clear, crystal clear, it would be a fool's errand to create a situation in which companies would be damned if they do and damned if they do not.

Ms. LOFGREN. If I reclaim my 14 seconds, Mr. Chairman?

Mr. ISSA. Of course. Yes, ma'am.

Ms. LOFGREN. I just think that we ought to have some further discussion on this point. And perhaps we could stimulate some useful activity on the part of the administration to get something positive done here.

Mr. ISSA. I would be happy to join with the gentlelady in that. We now go to the gentleman from Ohio, who has been patiently waiting, Mr. Jordan.

Mr. JORDAN. I thank you, Mr. Chairman. Mr. Downing, how long have you been at the Department of Justice?

Mr. DOWNING. Coming up on 18 years.

Mr. JORDAN. OK, 18 years. We appreciate your service. A week ago, former FBI Director, Mr. Comey, testified that then Attorney General Loretta Lynch told him when he discussed the Clinton investigation to call it a matter not an investigation. Do you recall that testimony from Mr. Comey?

Mr. DOWNING. I have heard news reports of that.

Mr. JORDAN. OK, were you a part of the discussion and decision at the Justice Department to instruct the FBI Director not to call an investigation an investigation?

Mr. DOWNING. No, sir. I am a career employee of the Justice Department, and I was not involved in any of that level.

Mr. JORDAN. Do you agree with that decision that was made and, frankly, implemented by the FBI Director?

Mr. DOWNING. I am afraid, sir, I do not have an opinion one way or the other on that.

Mr. JORDAN. Do you know if that has ever happened before, where the Attorney General tells the FBI Director to portray some-

thing differently than what is actually happening, i.e. not to call an investigation an investigation?

Mr. DOWNING. I am afraid I have no information for you on that.

Mr. JORDAN. Were you part of any decision by the Justice Department to allow the perception to continue that President Trump was under investigation, when, in fact, he was not and was told three times by the FBI Director that he was not?

Mr. DOWNING. I am trying to make clear, I am not involved in decisions of that level, and I have no information about it.

Mr. JORDAN. Do you think it is wise for the Justice Department to mislead the American people?

Mr. DOWNING. Of course, the Justice Department should do its best not to mislead anyone.

Mr. JORDAN. And you would agree that, in both situations, the American people were misled?

Mr. DOWNING. I have no basis to answer that question.

Mr. JORDAN. Well, think about it. In one situation, it was an investigation and the FBI Director was instructed to call it something different, to call it a matter. And the other situation, the President of the United States was not under investigation and yet that would not be confirmed, not be stated. And the perception was allowed to exist that he was. Twice the American people were misled by the head of the Federal Bureau of Investigation. That is probably not a good thing, is it?

Mr. DOWNING. I have no opinion for you on that.

Mr. JORDAN. I mean, but, you know, you have served 18 years at the Justice Department. You went to Stanford Law School; you are a smart guy, a good lawyer. Is that normally how it operates at the Department of Justice? Well, let me ask you this, do you know of any other occasion where the Attorney General has instructed someone with an important job, like running the FBI, to mislead the American people?

Mr. DOWNING. I have no basis to believe that, no.

Mr. JORDAN. You do not think it has ever happened before? You do not know of any other time it has happened?

Mr. DOWNING. I do not have any opinion on that, no.

Mr. JORDAN. What about the leak? What about the idea that the head of the FBI decides to give information to a friend who is then going to pass it to The New York Times? Should that be something that actually takes place, even though, at the time, he was a former FBI Director? Is that appropriate for someone who has held that position to engage in that kind of activity?

Mr. DOWNING. I am afraid I also do not have an opinion on that.

Mr. JORDAN. But, again, as someone who has worked at the Department of Justice for 18 years, Stanford Law degree, you think that is the appropriate kind of conduct for someone who has served in the Justice Department? Not even as high level as you, but someone who has been head of the FBI?

Mr. DOWNING. I think I could say that the FBI Director is a higher level than me. No, I am sorry, sir, I do not have an opinion about these kinds of questions. I understand the motivation and the need to try to get to answers on these questions, but I am not the right person to be in a position to answer them for you, sir.

Mr. JORDAN. I appreciate you trying to respond, Mr. Downing. But what I also think the American people would appreciate is the highest officials at the Department of Justice should be straight with the American people. And that did not happen. No, if, and, buts about it. It did not happen. And they were misled at the direction of the Attorney General.

Mr. Comey's testimony was real clear. He even questioned, he said, do we really want to do that? Do we not want to tell the American people the truth? And yet he carried out the order from the Attorney General to mislead the American people and say it was a matter, not an investigation. And, of course, as I have said a couple of times, he allowed the perception to continue that our current President of the United States was under investigation when, in fact, he was not. And with that, Mr. Chairman.

Mr. ISSA. Will the gentleman yield?

Mr. JORDAN. I would be happy to yield to the chairman.

Mr. ISSA. Mr. Downing, I understand you cannot always speak about things that are your main wheelhouse, if you will. Have you ever spoken to the press off the record? Provided any information about an ongoing case to a press person?

Mr. DOWNING. I have certainly spoken to the press off the record, sir. Of course, we are very careful about what we disclose, and we try to do our best to stay within the lines, certainly at my level.

Mr. ISSA. OK. So, I will take that as a yes. Thank you. We now go to the gentlelady from Texas, Ms. Sheila Jackson Lee.

Ms. JACKSON LEE. We welcome both Mr. Downing and Mr. McGuinness and add my appreciation for coming across the pond to visit with us. Let me just take a moment to applaud my two colleagues from California and from Ohio. We have just seen, and I will not take long on this moment, but we have just seen an opening to begin an investigation into the President of the United States and the questions of the Russian collusion, obstruction of justice by the Judiciary Committee.

And I think we have been speaking about that for a very long period of time. And so, I would ask Mr. Jordan to convey to the leadership chairman and ranking member of this committee, so that we can begin to open these investigations that the gentleman from California seems to want to answer about leaks and individuals speaking off the record. Mr. Downing, you answered appropriately; you are here for a particular topic. And thank you for your courtesies in responding to my colleague.

But I think now that we have now put on record that Republicans are interested in getting to the truth of what has happened and restoring the integrity of our government. And certainly, the number of witnesses are beyond even our imagination that could come before the Judiciary Committee to ensure that all of us have that chance to have questions asked and answered.

I would hope that that we can begin that post haste, and also I hope that we can secure from the Justice Department the many documents that we have asked for. And I hope that we can do that.

Let me indicate my interest in this topic and ask unanimous consent to put into the record, to the chairman, a letter from EPIC, Electronic Privacy Information Center, which is an organization that routinely files Amicus briefs in Federal courts regarding gov-

ernment cases, defends consumer privacy, organizes conferences for NGOs, but generally just understands the burdens of our providers and the whole question of releasing data.

Even though this does not have anything to do particularly with the PATRIOT Act, I remember that discussion after 9/11. And the bill was rejected initially because we did not secure the privacy rights of Americans sufficiently. I maintain that this is my position continuously, even as we move into enormous levels of data seemingly everywhere. And so, I ask consent to put this letter into the record.

Mr. KING [presiding]. Hearing no objections, so ordered.

Ms. JACKSON LEE. Thank you. So, I have two questions. One deals with the negotiations between the U.S. and U.K. The rules are different; I just came back from a Malta meeting with the European Union, Parliamentarians, and we always discuss issues addressing cybersecurity data. And we know that, collectively, obviously Great Britain is in the middle of Brexit. But, the point is that the rules were different, and that means that our companies here in the United States, in this agreement between the U.S. and U.K., may have some difficult obligations to meet with.

So, my first question is, why the secrecy and when will the U.S.-U.K. surveillance agreement be made public or aspects of it? And the second part is, what role of oversight do you believe the Congress of the United States, particularly, that is, in fact, the peoples' representatives, should engage with this agreement? Obviously, there are oversight and approvals that will come through, but ongoing responsibilities. So, first, when is this agreement going to be made public?

Mr. DOWNING. So, I do not have a particular deadline or timeline for you for when it would be made public. Frankly, we are in a bit of a hiatus in any discussions around it because we are waiting to see what action Congress may take on the legislation that would enable and authorize this kind of agreement. We expect close collaboration though with Congress. That is our goal.

We view this as an important piece of this. We have been working, of course, with the committee staff on both the Senate and the House and on the Foreign Relations Committee, and the Judiciary Committee, to try to make clear what we are doing. And we want to make sure that congressional role is strong.

Indeed, in passing of legislation, would set all of the guidelines and the floor for what could be done under these agreements. And, as I mentioned before, also, an additional role at the end of the process if we were to conclude with an agreement with the U.K., there would be a waiting period at the end where Congress would have an opportunity to consider it and to weigh in if it chose to.

So, I think you have my commitment that we are very interested in working carefully with Congress and that we are not going to be out doing crazy things by ourselves. This is very much a collaborative effort.

Ms. JACKSON LEE. Mr. McGuinness, though you come from across the pond you understand the vital role of Congress and the protection of the privacy rights of the American people.

Mr. MCGUINNESS. Yeah, I have the upmost respect for the U.S. Constitution and its protection of U.S. citizens. And of the role of

the Congress in that. I have observed, in this case, we have something which the companies have come to us and said, this is a potential solution to a problem we face. And on that basis, we have gone forward. This is not going to work if it is just done between governments. Tech companies, which have brought us such wonders are critical partners in this and they have been good partners in preparing it.

Ms. JACKSON LEE. That is my very point. Mr. Chairman, I want to conclude. That is my very point the burden that the tech companies will have to face. But, Mr. Chairman, I would think that it might be appropriate that we have, as we move forward, a classified briefing or opportunity to have the Justice Department back and begin to hear about just the levels of data that might be subject to the treaty as they are going forward.

I would like to ask more pointed questions, and probably, it would be necessary in a classified setting. I would like to put that on the record. With that, I yield back. Thank you for your answers. Thank you.

Mr. KING. The gentlelady's observation or request is duly noted. And since she has yielded back the balance of her time, the chair will now recognize the gentleman from Pennsylvania, Mr. Marino.

Mr. MARINO. Thank you, Mr. Chairman. Gentlemen, welcome. As a former district attorney and a United States attorney, I personally understand the complexities of modern day investigation and criminal prosecutions. I understand the need for law enforcement to be able to get timely access to important information, particularly in the abduction of children.

For the past several years, I have introduced legislation addressing the issue of law enforcement being able to legally access information that is stored overseas. This year, I have been working with my colleague, Mr. Jeffries, to continue improving this legislation framework.

Current legal framework, the Electronic Communications Privacy Act, more commonly known as ECPA, is insufficient for addressing the need of the technology and society of the 21st century. ECPA is over 30 years old, and the original drafters on ECPA could not have envisioned the interconnected lives we live in today's digital world. And the Second Circuit said as much in its ruling in Microsoft, you know.

Deputy Attorney General, and I do not mean to put you on the spot here because I just happen to glance at some of the opinions also, could you expand on the DOJ's opposition to the Second Circuit's decision in Microsoft, the Second Circuit Appellate Court, and your legal basis of, I think it has been, two and maybe three Federal Magistrates Courts' opinions that appear to me to be disagreeing with the Second Circuit's decision in Microsoft v. U.S.?

Mr. DOWNING. Certainly, sir. There are actually five, now, lower court decisions in different circuits that disagree with that opinion. Our position is a fairly simple one: we believe that the execution of a warrant by a U.S. provider, inside the U.S. is a domestic application of the Stored Communication Act.

That is, the order is issued by a U.S. court; it is served on the U.S. provider; and a person inside the United States maintains that data, even it is stored outside. And the moment of disclosure,

which is where the privacy issue may be involved, is inside the United States. It is then reviewed by officers inside the United States.

So, our position is that this is not an extra territorial, under the rules of the legal doctrine of extraterritoriality. And, therefore, it is perfectly proper for the companies to do it, to disclose that information to us. And, of course, as I have mentioned, it is so critical that we get this information in order to solve very real crimes, as you yourself pointed out.

Mr. MARINO. Thank you. Deputy McGuinness, welcome. I have had the opportunity to be a guest in England, in London, of Scotland Yard. And I was out on the street with the agents, and it was quite exciting, very similar to our legal system here of prosecution. But it is good to see you here. We have about 196 countries in the world, and many of them will not cooperate with a democracy like yours and ours. Would you agree with me that it would be virtually impossible to have one universal treaty and are bilaterals more realistic and less complex to achieve however cumbersome because of the numbers that would be required? Do you understand my question?

Mr. MCGUINNESS. I would strongly agree with that.

Mr. MARINO. What approach would you, specifically, if you would not mind expanding on it, because I know we have been working on one together? Do you see a large portion of that bilateral agreement that would fit concerning other countries? And do you see many objections coming forward from those other countries, based on what we have been working on? The Justice Department, I might add, Justice has been working on us on this.

Mr. MCGUINNESS. So, the work we have been doing, building on advice from the tech companies about what they felt would be workable and would provide a root to solve this problem of conflict of laws. The work we have been doing has both the effect of resolving the immediate issue with States that have shared standards, shall we say. But also roots to improve the behavior of other States. Now, that, clearly, is a matter ultimately for the United States, which is to use agreements to do that. But the United Kingdom is strongly supportive of it. And we are also most wary of data localization which we see as a really pernicious effect. So, we do see a way through this.

It is hard to say, it is hard to exaggerate just how significant this data is for keeping citizens safe. And that provides a very powerful driver in any jurisdiction for a changing behavior and a compliance with the terms that should be laid in something like this bilateral agreement. It is striking to me that in the exchanges that newly elected President Macron and newly elected Prime Minister May had in Paris only 2 nights ago.

That in the very front of their mind was this question of what is to be done about securing data in order to secure citizens. So, there is an enormous urgency to resolve this issue and to get onto a proper footing. And I think I put that urgency before you as being one of the reasons to choose one vehicle over another for seeing through this business.

Mr. MARINO. And I am glad to see that we all agree that the tech industry has to be a part of this. You know, they have a dog in this

hunt just as well as we do. But I do want to add, in conclusion, I see I have run over the time now, that many of the most serious cases that I prosecuted and where we reached convictions were based on using the 21st century technology that we have today. Thank you, and I yield back.

Mr. KING. The gentleman returns his time. The chair will now recognize the gentleman from Georgia, Mr. Johnson.

Mr. JOHNSON of Georgia. Thank you, Mr. Chairman. Mr. Downing, Mr. McGuinness, welcome. Mr. McGuinness, welcome from across the pond, as has been stated. And we do value the historic relationship that we have maintained with Great Britain and want that relationship to remain as strong as it has always been and actually strengthen it in this time of mutual threat, or threats that affect us mutually. As well as the rest of the world, but these two countries have led the world, and we need to continue to do that.

I want to ask a question Mr. Downing, in the event of a bilateral agreement between the U.K. and the U.S. that would permit U.S. companies to provide electronic data in response to U.K. orders targeting non-U.S. persons located outside of the United States, while affording the United States reciprocal rights regarding electronic data of companies storing data in the United Kingdom, what role do you foresee that Congress would have in approving, rejecting, or amending such an agreement?

Mr. DOWNING. As I mentioned before, I see a close collaboration between the Department and Congress as being an important part of this process. And, in particular, Congress' role at the very beginning in passing the enabling legislation is a particularly strong rule since it sets the framework and the guidelines, the requirements, of any sort of agreement that comes forward. There is also an important role under our proposal for Congress on the back end.

That is, that once an agreement has been worked out it would be provided to Congress for notice and, of course, at that point, Congress could take steps if it chose to. But it is very much our expectation that we would be in close collaboration with Congress as these kinds of agreements begin to be worked out, assuming that we move beyond the first one with the United Kingdom.

Mr. JOHNSON of Georgia. So, under the framework submitted by the Department to Congress for this proposed bilateral agreement to be negotiated: do you see a role of Congress in terms of vetoing the agreement once it is reached possibly? Would Congress have that authority under the terms of the legislation that you have submitted to us?

Mr. DOWNING. So, I may not be the best expert on congressional vetoes, but it is my understanding that we cannot write into the legislation an explicit veto. That that has been found to be not constitutional. However, Congress would have the ability at the conclusion of such an agreement to pass a law, if it chose to. That could obviate that agreement. So, Congress has an option, a decision that could be made, you could think of it a little bit like the way the Rules Enabling Act works where there is a period of time when Congress can choose to negate what has happened. But it is not an explicit veto you know written into the agreement. Because I believe that is not a permissible use of a statute.

Mr. JOHNSON of Georgia. All right. With that Mr. Chairman, I will yield back. Thank you.

Mr. KING. The gentleman from Georgia yields or returns his time. The chair will now recognize the gentleman from Florida, Mr. Rutherford for 5 minutes. And welcome to the committee, Mr. Rutherford.

Mr. RUTHERFORD. Thank you, Mr. Chairman. I appreciate that. Mr. Downing, if I could go back just a moment to something you said earlier. You talked about U.K. law should control when the elements are in the U.K. and only the data is stored in the U.S. And then, you talked about some standards that the U.K. has. Mr. McGuinness talked about necessity proportionality, the double lock process.

If we are going to use a bilateral agreement as kind of a template for other agreements down the road, could you talk about some of the other standards that you think should be met before the U.S. should consider entering into a bilateral agreement with other countries? Particularly, surrounding privacy rights.

Mr. DOWNING. Certainly, sir. The legislation that we have proposed would create a number of these kinds of restrictions that I think set a very robust standard for privacy protections. They include things like orders have to be for specific persons; you cannot do bulk collection under the agreement. It would require that any order be based on particularity and legality and credible evidence, for example. It has to be approved or supervised by a judge.

There are a number of different types of rules like that we tried to make sure that this would only apply to those kinds of countries that have a really robust system that respects privacy, civil liberties, and rule of law. And, frankly, would not be available probably to every country in the world by any stretch. It is going to be a strong system that only countries that have similar, not identical, but similar kinds of procedures and processes in their legal systems as we do.

Mr. RUTHERFORD. So, would you envision that through these negotiations we would, you know, meet the standard of probable cause for a warrant by agreeing that you know maybe a necessity and proportionality do qualify as probable cause? Is that kind of how you see this going forward?

Mr. DOWNING. Well, I guess I would not characterize it as that there is a requirement that other countries use the words "probable cause" or to have that exact concept. Frankly, I do not know of any other country in the world that uses that exact wording.

Mr. RUTHERFORD. No, but I mean within the body of the bilateral agreement, we would have some firm that would be necessity and proportionality and probable cause and we would all agree that meets the law of both parties in the bilateral agreement. Is that your intention?

Mr. DOWNING. Yeah. No, in the enabling legislation it actually set out those kinds of rules. And one of the requirements, for example, is that the orders be based on articulable and credible facts or evidence. So, it is not exactly the wording of probable cause, nor is it exactly the wording in that. But it is the idea that you have to have a justification that is based on objective evidence.

Mr. RUTHERFORD. I want to get back also to the issue that was brought up earlier. Would you make clear the difference between the requested data that requires a court order versus the type of data that requires a warrant and probable cause?

Mr. DOWNING. For, I am sorry, under U.S. law?

Mr. RUTHERFORD. Yes.

Mr. DOWNING. So, under the Stored Communications Act, there is a range of different kinds of data that can be obtained. For the more sensitive information, like the content of communications, the Department of Justice generally uses a warrant when obtaining that kind of information.

On the other end of the spectrum, there might be just the name and the address of the person who registered the account. That kind of information generally does not require a warrant, instead you could use a subpoena or perhaps a lesser court order to obtain it. So, there is actually a range under U.S. law, but it is loosely based on the idea that more sensitive information gets better protection.

Mr. RUTHERFORD. And law enforcement has been using that difference for a long time.

Mr. DOWNING. Since 1986, yes.

Mr. RUTHERFORD. Mr. McGuinness, we have talked about it a little bit, but the incidentally collected communications that involve foreign persons. Can you talk a little bit more about that? You have not said really specifically, for example, if a U.K. subject communicates via e-mail with a U.S. person, what is done to safeguard the privacy concerns of the U.S. person's communications?

Mr. MCGUINNESS. So, under the proposals that you have here, you can see the stub, the beginning of what will be negotiated between us should Congress agree that there should be such an agreement. And what is clear there is that there will be protections for U.S. persons, whether than be a U.S. citizen or a person in the United States, physically in the United States.

A U.S. citizen wherever they maybe and any person within the United States and there shall not be collection of them. And if we come across incidental collection, we will stop collections and delete the data. So, that is the conception. That this is not aimed, in any way, at U.S. citizens, wherever they may be and U.S. persons in the sense of anybody in the United States.

Mr. RUTHERFORD. Mr. Downing, I assume the retention laws all still apply?

Mr. DOWNING. I am sorry, the retention laws?

Mr. KING. The allotted time has expired. The gentleman will be allowed to answer the question.

Mr. RUTHERFORD. Thank you, Mr. Chairman.

Mr. DOWNING. So, yes, as Mr. McGuinness pointed out the data would be minimized and not used. And I would also point out that we as part of the agreement would have the ability to audit the U.K.'s practices as they would have the ability to audit ours. And we expect that to be a robust process to make sure that both parties are complying with their obligations under the agreement.

Mr. RUTHERFORD. Thank you.

Mr. KING. The gentleman yields back. The chair will now recognize the gentleman from Florida, Mr. Deutch for 5 minutes.

Mr. DEUTCH. And I thank the chairman. Mr. Chairman, I would start just by reflecting upon the comments of my friend from Ohio a little earlier. Where he asked Mr. Downing some questions that were not appropriately to be asked of you and were not appropriately to be asked in this particular hearing.

But I hope that my friend from Ohio and my other friends on the other side of the aisle in this committee, will seize upon the questioning that Mr. Jordan started this morning, and will recognize that it is, in fact, the House Judiciary Committee that provides oversight of the Department of Justice. It is the House Judiciary Committee that provides oversight of the administration of justice in this country. It is the House Judiciary Committee that, in fact, historically has waded into important matters where obstruction of justice claims have arisen with respect to the President of the United States.

And so, I hope while this is a terribly important issue and I hope I get to my questions, I wanted to follow up on my friend from Ohio to simply suggest, that it is appropriate for him to ask those questions.

I know we have a lot of questions that we would like to ask as well and, in fact, should be asking. As members of the Judiciary Committee, of former Director Comey, of Attorney General Sessions, of the Deputy Attorney General, Deputy Attorney General Rosenstein, of the Acting FBI Director. All of the sorts of questions that arise following just yesterday's headlines, last evening headlines that the Special Council is now looking at obstruction of justice claims.

This committee, Mr. Chairman, has a responsibility to the American people to hold hearings. Yes, it is important for the investigation being conducted by the Intelligence Committee and the House and Senate to continue, vitally important. Yes, it is important for the Special Council to pursue his investigation.

But when it comes to the administration of justice in the United States, that falls squarely within the purview of the United States House Judiciary Committee. And my hope, Mr. Chairman, is that we will be able to come together to hold that hearing that the American people so desperately want us to hold.

With that said, I thank you for your participation here today, to our witnesses. And while a lot has happened between today and last February Congress still has not sorted out what is a nationally complex issue, and I appreciate the chance that we have here to restart that work today.

As I said before, we have a long overdue and hugely important set of questions that we have to resolve as a country about how continuing evolving technology and privacy interact with the needs of law enforcement. And when we expand out these issues for our interconnected world, it only serves to highlight how many more questions we have than answers, that is what we are getting at today. And I think that really needs to change, and we have to do it fast.

In my mind, there are two distinct problems here. First, how do we increase efficiency in cross-border data flow where the laws of the relevant countries are in agreement? That looks like either a patchwork of bilateral agreements to shortcut the MLAT process or

comprehensive reform of MLAT's or doing both. We have been talking about some of that this morning.

Second is what do we do where the laws are in direct conflict or where it is not clear which countries are the relevant ones in a given case? It is all too easy to envision a scenario where data stored in one country is requested by law enforcement in another regarding the information of a national of a third country. And while there is much more that I would like to say, let me start with that and ask our witnesses to respond. What would you do in that situation?

Mr. DOWNING. I am sorry, in the situation where there is data of a third party?

Mr. DEUTCH. It is one country, the law enforcement in a second country, and the national in a third county.

Mr. DOWNING. So, that is unfortunately quite common. In the case of Ireland, Microsoft stores data in Ireland, but much of the data there is not going to be about Irish citizens it is going to be about many people, including Americans who might have their data stored there. Our view is that we need to have robust authority to get that data. It is critical for solving terrorism cases, solving child exploitation cases. Having quick and efficient means of getting it is particularly critical after the Microsoft decision. And we are seeking quick congressional action to try to deal with that problem.

Mr. DEUTCH. And before I wrap up: I just asked the question, so, department decisions that the government should be able to obtain data stored abroad by applying ECPA to companies based in the United States. What would the position be if another country made the argument? How would the Department react if the Chinese government required a Chinese company, like Ali Baba for example, which maintains a data center in the United States, to produce account information that belongs to U.S. citizens?

Mr. DOWNING. So, I think it is important to understand, sir, that it is in some sense the norm that countries claim the authority to gather data even it is stored outside of the country. If there is a person within the country who has access to it.

So I have read a report, for example, that showed that countries as diverse as Canada and Mexico, Ireland, and France, Australia, and Norway, they all, like the United States, claim the right to obtain information if it is stored outside of the borders as long as there is a person, like, the company is based inside the country. So, it is not the case that the Chinese are going crazy. This is actually kind of the norm. And how to deal with it is an important problem.

Of course, ECPA, our rules, would prevent China in many cases from getting that. And it is that conflict which is, unfortunately, causing problems for our providers. That is why we look to situations like an agreement under the U.S.-U.K. framework, which would ease that burden. And to make sure that we are doing it with appropriate countries we have safeguards in place to make sure that that is the case.

Mr. DEUTCH. That is an important discussion. Thank you, Mr. Chairman.

Mr. KING. Thank you. The gentleman's time has expired. The chair will now recognize the gentleman from Arizona, Mr. Biggs, for 5 minutes.

Mr. BIGGS. Thank you, Mr. Chairman. Thank you, gentlemen. I was reading, Mr. Downing, your statement and listening to your comments today. And I want to take you to one particular paragraph that you wrote in here, it says, "in particular we recommend enacting and implementing legislation for this framework." And you talk about as long as there is an adequate protection of privacy and civil liberties, right. And so, and you alluded to a term in kind of the framework that you have proposed, and I believe you used the term articulable suspicion or something.

Mr. DOWNING. Articulable and creditable facts, I think is the word.

Mr. BIGGS. Yes, articulable, and creditable facts. OK, so, it led me back to this idea: that seems distinctive from the apparently American notion of probable cause. And it seems like a lesser standard. Tell me about that. And I think of the interesting term reasonable articulable suspicion which is used in law enforcement in terms of probable cause. And in this kind of unique term that you have couched here, tell me about that and how that protects rights and how that would adequately protect privacy and civil liberties.

Mr. DOWNING. So, I think as I mentioned before, we are seeking to figure out what an appropriate baseline level is, not to exactly mirror the way U.S. law works. To start with the premise here that we are not targeting Americans, that is, that this is an event, for example, of a murder investigation in the U.K.

So, having some deference to the other countries laws, I think, is appropriate here where it is really only the fortuity of where the data is located that cause us to have any interest at all in the case. If it were not stored here, U.K. law would straight apply.

So, I think it is important that we have appropriate safeguards, but they should not be so stringent or frankly so requiring that they mimic ours. That we end up with a situation where no other country can seem to qualify. I think we should find an appropriate level. I think we have created a really robust level of protections.

I notice one of the statements for the record of the second panel here, says, we should not have any rules there should just be any countries involved. I think we have come to the conclusion that it is valuable to have a robust level of standards. Not identical to ours, but ones that I think would be appropriate and that we would have faith in as well.

Mr. BIGGS. A U.S.-U.K. bilateral agreement has been described as allowing wiretaps; I do not know if we have covered this today by, the U.K. Government. And traditionally we think of that as listening into telephone calls and whatnot. But here, we are talking about updating to you know live I suppose emails, chats, and texting, et cetera; is that a fair understanding?

Mr. DOWNING. That is right. Well, it would cover any range of communications, yes.

Mr. BIGGS. So, Mr. McGuinness, I guess my question for you is why is that important in this relationship, in this agreement, and yeah?

Mr. MCGUINNESS. So, thank you, that is a really helpful question, and this is a vital area. We are not only talking here about crimes that have occurred, investigating them, and bringing people to justice. We are also taking about preventing crimes, including terrorism, child abuse, and other things. And in that context, live interception is a vital part of the toolkit.

I have specific examples. An example would be from our National Crime Agency, they cite a gang of people who were selling live feed child abuse online. And in order to identify both the people doing it and the children and the location where it was being done, you needed to be able to cover the actual event happening live, because it was not going to be stored data. So, in that case live intercept was a vital tool to get coverage there.

The same can be said of terrorism incidents. If one is tracking people as they build towards an attack. And one of the things that I would say to the committee—very loudly, as an experience we have had in the United Kingdom in the last 3 months—is that speed is an issue. It is about the speed with which the internet is exploited by terrorists and that is the speed with which people can move from the thought of an attack to an attack if they are using knives and a heavy vehicle that they hire for cash. And we have seen that in France. We have seen that in the United Kingdom.

So, there is a question about speed and what tool you need to deal with speed. I would note that, like the United States, we see live intercept as a particularly intrusive power.

As I take you back to the point I made earlier about proportionality. So, if it is possible to gain the investigative advantage, if it is necessary, to gain the necessary investigative advantage by a less intrusive means, we will do so. But live intercept sometimes is vital if we are to prevent people being killed or abused.

Mr. BIGGS. And, Mr. Downing, back to you. We are using this, effectively, as a template for bilateral arrangements with other Nations. And you have discussed it a little bit, but as Mr. McGuinness said, we are from the same root ball of civil liberties going forward. Can you tell me you know what is going to look like, what is Congresses role in your mind going forward as we receive perhaps in other bilateral arrangements and negotiations?

Mr. DOWNING. So, I perceive that we would seek to be in close coordination with Congress as we move forward. If it works out with the U.K., and we look to do it with other countries we would do that. Congress of course has a critical role at the beginning of setting up the rules. What are the rules? And, in the case of wiretaps, the rules that we are proposing Congress pass would include things like an exhaustion of alternatives, that you cannot do it if a lesser thing would be possible. And to have a bunch of rules in there that would set an important floor for that.

And then, as I mentioned, there is a waiting period at the end. If we were to include an agreement with the U.K. or any other country, then there would be notification back to Congress and a delay before that agreement would go into effect. And Congress could act at that time if they chose to. So, we see this as an important partnership in getting these kinds of frameworks in place. And I think that is sort of an appropriate way for us to precede.

Mr. BIGGS. Thank you, my time has expired. Thank you, Mr. Chairman.

Mr. KING. The gentleman's time has expired or he has returned his time. The chair will now recognize the gentleman from Louisiana, Mr. Jeffries for 5 minutes.

Mr. JEFFRIES. From New York, Mr. Chairman. I thank the distinguished witnesses for their presence here today. And let me thank Mr. McGuinness, first of all, for your thoughtful and heartfelt words at the beginning of your testimony in terms of the calamity that we experienced here in Congress, yesterday. And, obviously, those thoughts are felt mutually in terms of what you are going through right now throughout Great Britain in terms of your citizens.

In terms of Mr. Downing, I wanted to get your perspective on one, this Second Circuit decision: is the Department of Justice's position that Congress should take steps to reverse the holding in the Second Circuit? It that correct?

Mr. DOWNING. That is what we have proposed.

Mr. JEFFRIES. And can you explain why you believe that is a proper course of action?

Mr. DOWNING. You mean, as compared to having the Supreme Court settle the matter?

Mr. JEFFRIES. Sure.

Mr. DOWNING. Yes, we are, as I have mentioned, experiencing a very serious problem in gathering critical evidence in a whole range of our cases. And so, we have been trying to seek whatever course is available to correct this problem, and our efforts to litigate it and to get the law changed through interpretation in the court continue. Unfortunately, it is a slow process. And even in the best of circumstances, the Supreme Court would probably take a whole other year before it resolved it.

Therefore, we are also seeking action in Congress. I do not see those as mutually exclusive from our perspective this is a critical problem that we need solved, and so having Congress act would be a perfectly proper solution to the problem.

Mr. JEFFRIES. ECPA was first passed in 1986 is that right?

Mr. DOWNING. ECPA was first passed, correct.

Mr. JEFFRIES. That was 31 years ago. Since that moment the United States has sort of emerged as a cradle of innovation throughout the world, is that fair to say?

Mr. DOWNING. I think that is fair yes.

Mr. JEFFRIES. And in the 21st century, we live in a global economy, correct?

Mr. DOWNING. We do.

Mr. JEFFRIES. And there are U.S.-based tech companies that operate throughout the world, is that right?

Mr. DOWNING. They do, yes.

Mr. JEFFRIES. Would you say that is a good thing for the American people and our economy?

Mr. DOWNING. There have been many benefits for the United States as a result of that, yes.

Mr. JEFFRIES. So, it is fair to say that these companies, in terms of our own national economic interest, can remain viable and com-

petitive internationally in the current digital landscape that we operate, true?

Mr. DOWNING. Yes, that is true. And that is absolutely the case.

Mr. JEFFRIES. Now, placing United States companies in a position where they could be forced to violate the privacy laws of another country would also be problematic, correct?

Mr. DOWNING. Yes, I have sympathy for the situation that companies are in when faced with competing legal demands. It is true, actually, of many different kinds of U.S. industry and has been true, frankly, for many years outside of the context of telecommunications providers. There are, of course, rules to try to resolve those questions. But it is a fact of life for big multinational companies in any of our industries that they may have to deal with conflicting legal demands.

Mr. JEFFRIES. And I just want to drill down on this point in terms of competitive disadvantage and conflicting legal demands. If we place our own companies in an adverse position in terms of these competing legal demands and the possibility of conflicts of laws and violating privacy laws of other countries, are those countries being skeptical of our ability to match their privacy standards? Does that not ultimately implicate the United States economic interest?

Mr. DOWNING. Yes, I think that is true. It ultimately does have that impact. But, of course, economic interests are not the only ones here. I do not mean to be combative with you, but, of course, we also have to take into account our public safety interest. And if we are doing things that benefit our industry, but that have the impact, like the Microsoft decision on the protection of children and the American public, I think we have to make sure we are taking both of those things into account.

Mr. JEFFRIES. Right, no, I just want to establish that there is a range of interests that are important in terms of what we as Congress should consider moving forward. National security interest, privacy interest, abroad and foreign, as well as our own competitive economic interests, is that correct?

Mr. DOWNING. Absolutely, I think looking for a solution that meets all of these needs would be the best path forward.

Mr. JEFFRIES. And, in fact, I think Article I, Section 8, Clause 3 of the Constitution states that it is Congress that shall have the power to regulate commerce with foreign countries; is that right?

Mr. DOWNING. That is true, yes.

Mr. JEFFRIES. And so, when you take all of this into account, is it not fair to say Congress should be intimately involved in whatever framework is developed from a bilateral standpoint or multilateral standpoint in terms of dealing with data sharing?

Mr. DOWNING. Absolutely. As I mentioned before, we see close coordination with Congress as important. And, of course, setting up the whole framework is a role that we are asking Congress to take on in terms of U.S.-U.K., to be able to set up the rules that we would have to follow in passing any kinds of future agreements with other countries.

Mr. JEFFRIES. My time has expired. One, I want to thank Congressman Marino for his leadership in this area. And also point out that, you know, close coordination is a vague phrase. I think we are

going to have to drill down on specifics as it relates to the power to accept, reject, or amend, and what form that takes either in the treaty context or in, you know, the administrative review context as it has been used in other incidences is going to be important for us to move forward; would you agree?

Mr. DOWNING. Yeah, no, it certainly——

Mr. KING. The gentleman's time has expired. The gentleman will be allowed to answer the question.

Mr. DOWNING [continuing]. I will simply say, yes. It is an important question that we are going to have to resolve.

Mr. JEFFRIES. Thank you. I yield back.

Mr. KING. Thank you. The gentleman from New York has returned his time with apologizes to the chairman. Now, I recognize the gentleman from Texas, Mr. Ratcliffe, for his 5 minutes.

Mr. RATCLIFFE. Thank you, Mr. Chairman. I appreciate the witnesses being here today. I have been bouncing between meetings and other hearings, and so I apologize in advance if I am going to ask you something that may seem repetitive to you.

Mr. Downing, if I understand correctly, certain proposals for addressing the issues that we are examining today would be to focus less on the location of the data itself and more on the citizenship and physical location of the individual about whom the information is being sought. Does it concern you, from a law enforcement perspective, about a scenario where a U.S. company does not know the citizenship or physical location of the individual and so declines to turn over the evidence? Or, I guess, related to that, feels that the government has not sufficiently established the citizenship and still declines?

Mr. DOWNING. That is absolutely a concern of ours. If we have a rule which is based solely on the citizenship of the person, and it does not take into account the very common situation where we do not know that person's citizenship, and that blocks us from getting evidence, that is a very serious problem. We often are in a situation where we have, let's say, a hacker or a child sexual exploiter who is hidden from us by the anonymity that is provided by the internet. It cannot be we do not get to access that information simply because we do not know the person is yet.

Mr. RATCLIFFE. OK. I was out walking and someone was asking you about wiretaps as a former prosecutor, you know, my perspective on wiretaps is they are traditionally thought of as listening in to phone calls in real time. The request from the U.K. here, with respect to the U.S.-U.K. bilateral agreement, would not be to do that, correct?

Mr. DOWNING. I am sorry. The rules that we are proposing would be that if there is a targeting of an investigation which is not a U.S. person, if it is a U.K. person, for example, and they need to get a wiretap for that person, but the only place that the wiretap could be effectuated is in the United States, then it would be part of the agreement that they could use their own wiretap law, their own wiretap order, with their own restrictions. And then, the U.S. company would comply with that foreign legal process.

Mr. RATCLIFFE. OK. And so, would it also apply in the context of text messaging and other features like that?

Mr. DOWNING. Yes, absolutely, it would be for all kinds of communications not just verbal ones.

Mr. RATCLIFFE. OK. So, then, let me ask you, Mr. McGuinness. and I appreciate you traveling all the way here and I represent east Texas and I have enjoyed listening to your far east Texas accent this morning. But one of the topics that is the subject of debate and, ultimately, reauthorization here in this country will be tools like 702 of our FISA Amendment Act that a tool that can result in the incidental collection on U.S. persons. So, how does the U.K. treat incidentally-collected communications that involve foreign persons under this?

Mr. MCGUINNESS. Let me say, first of all, my family in East Texas, I hope you are looking after them well, my aunt, and uncle, and cousins. So, to be clear, I think we said it, but it is worth saying again. The proposed U.K.-U.S. framework that we are talking about is not about U.S. citizens and not about persons in the United States; categorically, not. When we talk about foreign persons and how they are protected in this, it is U.S. persons who are protected.

Other foreign citizens are not. That is because the conspiracies that we look at for almost everything that we look at under serious crime, unless there is a single actor, involved people of multiple nationalities. And that is true if we are looking at are known Albanian crime groups, trafficking people into the U.K. That is true if we are looking at recent conspirators and attackers in the United Kingdom who carried out attacks. There are multiple nationalities, multiple connections, externally.

And we covered this a little bit earlier, but it is worth repeating; we, within this agreement and within the language that has been sent by the administration of the Congress, there is a very clear protection for the rights of U.S. citizens and U.S. persons; an expectation that, should we inadvertently collect the communications of a U.S. person, that as soon as that is evident, we will desist, and we will delete the data; we will minimize the data. So, that protections are in place. That is, obviously, something the exact detail of how we do that is to be discussed if you agree there should be an agreement. But I am confident that we can set a very high standard.

Mr. RATCLIFFE. OK, and my time has expired, but that would apply, for instance, if a U.K. subject communicates via email with a U.S. person? You are talking about applying those privacy safeguards to the U.S. person?

Mr. MCGUINNESS. Indeed, if I write to my cousins.

Mr. RATCLIFFE. OK. Very good. I appreciate that. Thank you. I yield back.

Mr. KING. The gentleman yields back his time. The chair now recognizes the gentleman from Rhode Island, Mr. Cicilline.

Mr. CICILLINE. Thank you, Mr. Chairman, and thank you to our witnesses. Mr. McGuinness. in particular, welcome. We appreciate your long travel and thank you for your thoughtful words at the beginning of your testimony. And I hope you feel the same prayers and thoughts of all of the American people with respect to the citizens of the U.K., in particular, the families of the loved ones who were killed or injured in those attacks in your own country.

I think there is broad consensus in our committee that we need to urgently respond to the issues that both of the witnesses have raised. And I think our committee took up the Email Privacy Act in the hope of developing and implementing a uniform domestic standard for law enforcement based on probable cause, a standard we are familiar with here in the United States. But that we also need a uniform standard that provides clear guidance to all parties for overseas applications of electronic information.

And I think, as the gentlelady from California mentioned, it is of particular concern to American companies. We do not want to put them in a position where, despite their best efforts to comply with prevailing law, that they are in a position of, by any action, either complying with one law and inadvertently or unintentionally violating another, and it puts them in an impossible position. So, I think it really underscores the urgency of our work.

And so, I guess my first question is kind of what your sense is, that is both of you, with respect to the current MLAT process, you know, there has been a lot of talk about reform. Is it mostly that we have to figure out ways to accelerate the decision making and application process? Does it mostly strike the right balance, or beyond sort of the speed and efficiency of it, are there other reforms that you think are critical?

And, particularly, your thoughts on the legislation that was introduced in the last Congress by Ms. DelBene and Mr. Marino. Did that strike the right balance and address all or most of your concerns?

Mr. DOWNING. So, I want to be clear that the MLAT process is an important tool, but I think it is also clear that, as we have entered a global and internet-connected world, that it is not a sufficient tool that we can use in all the times and situations that we need. That is why we are looking at faster processes such as the U.S.-U.K. agreement.

That being said, I think we are not going to ever reach a point where we have bilateral agreements with every country in the world. And even if we did, there is still going to be the need for mutual legal assistance treaty processes, for example, when the U.K. needs information about a criminal in the United States.

However, the MLAT process will be benefited, interestingly, by bilateral agreements, because it will take some of the pressure off of it. Some of the cases could be handled in that way.

You have to think about the MLAT process in two directions. One is our outbound requests, how quickly other countries are complying with that. Unfortunately, it is often very slow and cumbersome, and, of course, we do not have MLATs with some countries. As far as the inbound requests, we at the Department of Justice are taking a lot of steps to try to do a better job of it. Unfortunately, the requests, especially for electronic evidence, have just risen massively over the last decade, and resources have not necessarily kept pace with that.

We have done a number of reforms, though. We have created a whole cyber team to focus on these kinds of requests in particular. We have improved efficiency by focusing our efforts by going to the courts here in the District of Columbia rather than spreading these out all over the country.

And we have really made some substantial gains. I had a couple of figures prepared. In the 2013 to 2016 timeframe, we saw our increase in our requests go up by 175 percent, but the number of ones that we were able to resolve went up by 532 percent. So, we are cutting into the backlog. We are doing a better job of it. However, there are still a lot of hurdles.

In particular, this was partly accomplished by a one-time transfer of funding from one pot to another. And without a sustainable amount of resources to put into this problem, we actually hired a number of attorneys; we need to be able to support them if we are going to continue to make progress on this. So, I think there are opportunities for improvement. We will continue to work hard on that and hopefully we will also be able to see improvement when we make our requests going out, which is consistently also an issue that we are going to have to grapple with as well.

Mr. CICILLINE. Thank you. Mr. McGuinness.

Mr. MCGUINNESS. So I would strongly endorse what Mr. Downing has said about the importance of MLATs, both, actually, bilaterally between the U.K. and the U.S., but also as a mechanism that will allow us to deal with countries that cannot reach the high standards that are being set by this proposal here. MLATs are too slow. Well, we need to do work on that. We need to relieve the pressure on them, absolutely.

They also are backward-looking. And I think we would all agree that in some of the egregious crimes that we are looking at, these terrorist attacks and conspiracies that we have, child sexual exploitation, trafficking of human beings, that actually, we want to get into stopping it and preventing it. And the MLAT will not really allow you to do that except in prosecuting some of the people doing it. So, this agreement allows us to do more of that preventative work to our mutual benefit.

Mr. CICILLINE. Thank you. I see my time has expired. Thank you both.

Mr. DOWNING. Thank you.

Mr. KING. The gentleman from Rhode Island has returned his time. The chair will now recognize himself for 5 minutes. And I would first turn to Mr. Downing and thank you for your testimony. And I wanted to understand how a section 2703 warrant is actually issued, the functionality of that. Could you explain that to the panel?

Mr. DOWNING. Absolutely. 2703 warrants are actually executed much more like a subpoena. The officer would swear out the warrant before the court, supply probable cause, do all the steps, and have the judge sign it. And then, that is simply provided to the provider. Under 2703(a) it says that the warrant may compel the production. That is, it is a compulsion order, not a situation where the officer goes to Google's headquarters with a gun and says, "Stand away from the keyboards. I am here to seize the evidence." Instead——

Mr. KING. How does it actually arrive, then? How is it actually presented to, say, Microsoft in Ireland? How does it get there?

Mr. DOWNING. So, we would normally not present it to Microsoft in Ireland. We would present it to the domestic service provider. It varies between providers. In the old days, we would fax them.

Now, there are electronic means of transferring the information. But——

Mr. KING. So, I get that. Then you swear out a warrant; the judge approves it; and then the document, perhaps a PDF document, is emailed, then, to the company that is in control of the information you are seeking?

Mr. DOWNING. That is correct.

Mr. KING. And if that company is domiciled in Ireland rather than the United States, is there a legal difference?

Mr. DOWNING. Domiciled? No. I mean, if the company is in the United States doing business in the United States, employees in the United States——

Mr. KING. A U.S. presence.

Mr. DOWNING [continuing]. We would regard that as being under the jurisdiction of the court.

Mr. KING. OK. So, any company domiciled anywhere that has a U.S. presence, then, is subject to a 2703 warrant?

Mr. DOWNING. Any company that would be inside the jurisdiction of the court, yes.

Mr. KING. OK. And if that company then holds that information in Ireland, as a topic we are discussing here, and you do not review that data until it is back inside the domestic boundaries of the United States?

Mr. DOWNING. That is true, yes. It would be disclosed to us here.

Mr. KING. That is how you qualify that a warrant then is valid and can be applied under these circumstances we are discussing?

Mr. DOWNING. Well, it would have to be that the company not only has a presence here, but that there is a person inside the United States who has possession or control over the information. So, in the case of Microsoft, for example, the employees here have——

Mr. KING. Or access to that information that might be held in a foreign country.

Mr. DOWNING. Or access to? I am sorry.

Mr. KING. Well, as I understand this case with Microsoft, the data was in Ireland.

Mr. DOWNING. That is true.

Mr. KING. And the warrant was served, we think, to the Microsoft officials here in the United States——

Mr. DOWNING. That is correct.

Mr. KING [continuing]. Who, then, were compelled by the court to access that information and deliver it to justice.

Mr. DOWNING. That is correct. They had possession and control, those are the sort of legal words of this——

Mr. KING. OK. Let's just say you had a justice official in Ireland that could walk into the headquarters in Ireland of Microsoft, and that warrant was served electronically and emailed over there to Ireland. Under this warrant, could they hand them the data off of their hard drive, let's say, in a thumb drive condition?

Mr. DOWNING. I am sorry; I lost you on that hypothetical. It is a——

Mr. KING. I am just intrigued by this legal technicality of, if the data is in a foreign country and there is a U.S. presence for that company, the warrant can be served in America, but you cannot

look at the data until it gets back into America. That seems to me a very finely-split legal hair, and I am trying to understand that rationale. We have seen some of these finely-split legal hairs rationale in the past before this committee, and they do not always hold up.

Mr. DOWNING. I guess I do not see it as a legal hair. Over the last many decades, we have had situations where we serve a subpoena on a company and the paper documents might be located overseas; perhaps they are bank records, and we have required the company to comply with that subpoena. And we have a whole doctrine to deal with the potential conflicts of law.

If the company comes forward and says, "I cannot do it because there is a real conflict," then the courts would balance that kind of conflict. I would expect that kind of analysis would be what would happen in this situation as well.

Mr. KING. Mr. Downing, my time is clicking down. But I just was caught by perfectly proper, and I will dig into that perhaps a little later. But I wanted to take this opportunity to thank Mr. Paddy McGuinness for his presence here, and I want the committee to know that you rolled out significant hospitality to myself and Chairman Goodlatte and several others almost a year ago, around June 25 or so last year, shortly after the Brexit vote.

We had a deep and engaging discussion and were very well-informed by yourself and a number of other persons that were there in the briefing table. And the intent that flowed from that discussion seems to also flow from your testimony here today. And I want to thank you formally for your efforts on this. And my sense of what we have negotiated so far is in keeping with those things that we saw and discussed in London almost a year ago, and any final words you would like to say, Mr. McGuinness, I would like to hear them.

Mr. MCGUINNESS. Thank you very much. Can I say, first of all, I am most grateful for the engagement of this committee in this business? This is vital interest to the United Kingdom. This will enable us to keep ourselves and our American allies safer, and so I am most grateful for it.

I am also really grateful, and we have been heartened and our resolve strengthened, by the practical support we have received from the United States, but also the moral support, and I heard some of it here today, in the face of what has happened to us over the recent months. And I suppose my last message, apart from being grateful, is simply to say that we are resilient and are confident to our ability to see through this slightly difficult period and get to a better place, not least with your help.

Mr. KING. We have fought together through much more difficult endeavors in the past. We will demonstrate that to the world, Mr. McGuinness. Thank you very much. And I see my time has expired. Now, I would recognize the gentleman from Maryland, Mr. Raskin, for 5 minutes.

Mr. RASKIN. Mr. Chairman, thank you very much. And Mr. Downing, Mr. McGuinness, welcome. Thank you for your excellent testimony. Mr. McGuinness, let me just echo my colleagues in saying we thank you for your words of solidarity and encouragement, and we return them to you and the people of the United Kingdom

as you deal with the violence and terror that have beset the people of your country.

I am persuaded, very much, by the testimony that the laws governing law enforcement access to data across borders are in critical need of revision and modernization at this point. And because of the Second Circuit decision in Microsoft Ireland, the U.S. law enforcement is blocked from accessing data in legitimate investigations based simply on the fortuity of where the data happens to be held. And the mirror image problem applies to foreign countries in trying to access data that you need in order to solve and prevent crimes. So, the suggestion, as I understand it, is for a bilateral agreement between the U.S. and the U.K., and then perhaps a series of bilateral agreements with other countries.

I want to make sure that both of you agree that such agreements should only be undertaken where both sides respect basic rule of law principles and basic human rights principles. Am I correct in saying that?

Mr. DOWNING. Absolutely, yes.

Mr. RASKIN. And, Mr. McGuinness, you agree?

Mr. MCGUINNESS. Strongly so.

Mr. RASKIN. In other words, we are very happy to guarantee the mutual transmission of law enforcement data when we know it is not going to be abused, when we know that the government that obtains it will respect the rule of law, the ability of people to defend themselves, have notice and opportunity to be heard and so on, and where basic human rights norms are, in fact, being observed.

Does it follow, then, that the countries with which we engage in such mutual bilateral agreements themselves should also not turn over any law enforcement data to authoritarian regimes or regimes that fall outside of a rule of law or human rights framework? Does that follow?

Mr. DOWNING. I think I would not be quite so categorical about that. It is also possible that authoritarian regimes have their own perfectly legitimate crime and security problems, and there may be situations where evidence lawfully gathered could be used to prevent a serious terrorist attack in another country.

Nevertheless, your basic premise is right, that there should be appropriate restrictions on the sharing of information and that it should not be used as a free ride or a way of getting any benefit that would not normally be there.

Mr. MCGUINNESS. So, if I may, so far, clearly we have been having, in principle, discussions of what an agreement might be like rather than what an agreement will be, because we do not have your agreement that there should be an agreement. But our understanding has been, our expectation is, that there will not be onward passage of data that is provided through this reciprocal agreement.

So, let us say we are investigating an Albanian crime group. We get coverage of it and we learn of a harm that is occurring in a third country that does not have appropriate human rights standards or privacy respect, or whatever it is. We would still want to tell them of the harm and enable them to deal with it, and we would go and do that. We just simply would not give them the

data. So, we would give them the result of the investigation, and I think that provides us with some protection.

Mr. RASKIN. And that is for the purposes of crime prevention?

Mr. MCGUINNESS. Yeah, for the purposes of crime prevention, for instance.

Mr. RASKIN. What is the scope of the agreement in terms of which crimes are incorporated within it? I think I saw someplace that serious crimes. But is there any definition of that? Is that what we call felonies in the United States?

Mr. MCGUINNESS. So, the definition we have been working on in the United Kingdom is a crime which gets a mandatory sentence of three years or more. So, that provides us with a baseline, and then we go above that, and that covers the range of crimes that we have been using in our testimony today.

Mr. RASKIN. Got you. And to what extent do we need a multilateral treaty to deal with this? And could such a multilateral treaty actually advance rule of law and due process concerns in countries where it is in danger?

Mr. DOWNING. So, I think the idea that other countries may be willing to raise their standards in order to meet the obligations under this in order to get access to this type of agreement is very much one thing that we have given some thought to and, I think, an advantage of the system that we have. We are open to all sorts of ways of thinking about this and doing it efficiently.

So, having a multilateral agreement could be a way forward, so long as all the countries that were in that group met the basic rules that we are setting out, that Congress would set out if they were to pass the proposal as we suggested it. So, it would have to be that they all meet that robust standard, but having a more efficient way of doing it on a faster basis, that is something we would certainly be open to.

Mr. RASKIN. OK. I have gone over, Mr. Chairman. I yield back. Thank you.

Chairman GOODLATTE. The gentleman from Georgia, Mr. Collins, is recognized for 5 minutes.

Mr. COLLINS. Thank you, Mr. Chairman. I think one of the things we have seen here, and, Mr. McGuinness, thank you for being a part of this. I want to start with you and then I am going to come to Mr. Downing. In the treaty perspective, and I know there has been some discussion and we just handle this sort of in a treaty mode if we do it bilaterally, which I think with one of our greatest friends, you know, the U.K., would be not a problem. But the reality here is that this is a subject that spans far more borders than just this.

And I think following up a little bit on my friend from Maryland's question, is how do we see this with other players, China, others, you know, where these markets or even in the EU, working to that? Really, bilateral is a good step, but it is not really addressing completely this issue, would you think?

Mr. MCGUINNESS. So, if I may, I think I have a couple of thoughts for you. The first thought I have is that this way forward is one we have worked up with the close support of the major U.S. tech companies who see this as a way out of the bind that they are

in. And they see it as a way we can build incrementally into a better space. First thought.

Second thought, when I go and talk to European colleagues, as I do regularly, they are, like, people in a closed room with no exit, where they are suffering from crime, or in the case particularly of northwestern Europe, they are facing terrorism of a kind that they find it very hard to deal with, and they have not got the data that they need. And they are thinking of solutions within their national boundaries, data localization and the rest, and this agreement is a way out of that position.

And so, it may be that you do it individually with them. It may be eventually you are able to do it more broadly. But what we need, as I think the Justice Department have said, is we show there is a way of doing this. If we show there is a way of doing it, we will see it through.

Lastly, in terms of China, I think, as we had a question earlier about standards in North Korea and Cuba and various other states, it will be a wonderful thing if we can get them to raise their respect for freedom of expression and privacy and the rights of the citizen. There are other mechanisms for providing data to them, and we talked about MLAT here, and I think we are just going to have to have a multiplicity of ways of dealing with the more difficult jurisdictions. But, actually, we have that anyway in our interactions with them.

Mr. COLLINS. Well, look, I am very sympathetic. Our tech companies especially here in the U.S. are outstanding, and they have, you know, they model and they go around the world. I think there is some issues, I think not only raising security, privacy, but also protection and content. There is a lot of other issues here that we could get into with this situation.

Mr. Downing, though, I do believe there is an issue here, and it has been addressed here and we are looking at from a legislative standpoint, and then based on the written testimony, it is safe to assume that your belief is the government should be able to obtain this information regardless, correct? In the United States, regardless of the data's location.

Mr. DOWNING. That is correct. That is our proposal.

Mr. COLLINS. OK. Well, and just hypothetically here, if so, how would we, I guess, as a country, react if we adopted this position? For example, if the Chinese government required a Chinese company, like Alibaba, which maintains data centers in the U.S., to produce information that belongs to a U.S. citizen? Would that not jeopardize individual's interest here in companies here in the U.S.?

Mr. DOWNING. It is already the case that the Chinese government claims that right, as do, frankly, as I mentioned, many countries around the world: Canada, Mexico, Ireland, Australia——

Mr. COLLINS. But we are sort of the buffer at this point to say, "Hang on a second." That is why this Congress legislatively should be looking at this, because, you know, again, I think that is the question I am saying is, are we tactically going down a road that is not, at this point, lining up with the privacy needs and privacy interests with our companies and with our citizenry in regard to regimes that we would never agree to this on any circumstance?

Mr. DOWNING. So, with respect to, say, a country that we would not be willing to enter into a bilateral agreement: for them, the restrictions on disclosure under ECPA would not be lifted, and therefore, the Chinese court orders would likely not be complied with by the U.S. companies. So, we are interested in reducing those conflicts of law for our companies, but doing it in a selective and positive way with countries that we can agree have a respect and a robust protection for civil liberties and the rights of their people.

Mr. COLLINS. And I think that is, you know, as we get to do here in hearings and even with the second panel and others which I will be in and out of a lot, that is the ideal. But we also have to reel in the realities of data in companies in the U.S. and others and where they store the data and how they move their data and how some of these are applicable interests, and I think that has to be given some deference to these tech companies.

And the growth: we are still even in their expansion that we have seen in the last little bit are still at that area of growth that people more and more depend on this privacy, more and more expect this privacy, and I think that has been said even 10 years ago.

This is the next big debate that we have to have, and I think it is something that I am very concerned about, especially dealing with our companies who are providing this. And it is a balance.

And so, for me, it is just really a concern here that the DOJ look at it also from our perspective as well, and when we legislatively fix this, it is not just a, "We are not going to go here. We believe this," but there is a balance that we need to strike. And that is the thing I believe. And I think our tech companies deserve that, but more importantly, the American people deserve it, and then from a citizenry and citizenry of the world with our friends across Europe and other places. So, with that, Mr. Chairman, I yield back.

Chairman GOODLATTE. The chair thanks the gentleman and recognizes the gentlewoman from Washington, Ms. Jayapal for 5 minutes.

Ms. JAYAPAL. Thank you very much, Mr. Chairman. And I just want to again extend my thanks to both of you, and, specifically, to Mr. McGuinness for making the journey at a very difficult time. You know that the United States stands in firm alliance and solidarity with the United Kingdom.

I absolutely agree that we need a comprehensive framework that takes into account our very global, interconnected economy and, at the same time, balances our many needs. And, of course, we are very proud in Washington State of our extremely innovative tech sector. We want to make sure that the economic benefits of our digital economy continue to come to the United States and benefit the United States.

We also want to make sure that we are protecting the global, national, and domestic security, and protecting our civil liberties and privacy rights of U.S. citizens. And I agree with our ranking member when he said at the very beginning that we do need to make sure that we get our details right.

Mr. Downing, I wanted to just follow up on Mr. Raskin's question about what constitutes serious crimes, because obviously, public discussion is centered around investigations into serious crimes. I know Mr. McGuinness defined it as anything that gives you three

years or more. But can you give me a little bit more detail in terms of how we would assess what is truly serious crime?

And would these agreements also apply to less-specific national security threats? And with regard to the serious crimes, because of the way our justice system works, we have a lot of mandatory minimums, we have other things that put certain crimes into a framework that may not comport with the United Kingdom. Can you just give a little bit of insight into that?

Mr. DOWNING. So, we were choosing the framing of serious crime in order to provide at least a little bit of flexibility as different countries, as you correctly point out, have slightly different approaches to sentencing in their different countries, and what might constitute a particularly severe sentence in the U.K., may not be quite regarded in the same way.

I would see, for our law, it would be, you know, felony crimes would be probably a rough-and-ready way of looking at it. But the reason we did not try to specify it with even greater specificity in the proposed framework is that there may be a need for some flexibility.

With respect to national security threats, I want to be clear, this is not an intelligence-gathering tool. The agreement is aimed at the investigation and prevention of crime. Of course, there are some national security threats such as terrorist threats that also are crimes, and so would be covered here. But it is not intended as a sort of counterintelligence or other national security work. It is a provision oriented toward solving and preventing crime.

Ms. JAYAPAL. That is helpful. Thank you. And in the proposed legislation from the department, you talk about orders issued by a foreign government must be subject to review or oversight. Can you clarify exactly what you mean by oversight? What would Congress's role be in that? How do you foresee Congress having that very active role in oversight that I believe we should have?

Mr. DOWNING. So, I think the provision that you are referring to talks about the oversight of legal process that is issued within one of the two parties. That is, when the British police officer is investigating an organized crime group, there needs to be oversight of the application for that court order.

Slightly different question, I think, is what is Congress' role in overseeing this entire process of developing a framework and an agreement? And as I have said, I think our expectation is that there will be close collaboration with Congress. We certainly worked hard over the last year to try to be involved with committee staff on both sides of the House and the Senate.

We also see a strong congressional role in setting up this whole framework. It is very much a congressional choice to be able to figure out what the rules ought to be for these agreements going forward. And then, there would be notice to Congress before any agreement goes into effect to make sure that Congress has a role at that stage as well.

Ms. JAYAPAL. And so, you would be willing to subject these agreements to a vote by Congress?

Mr. DOWNING. So, the proposal does not formally create a requirement that there be a vote by Congress. This is more like, I suppose——

Ms. JAYAPAL. But would you be willing to agree to that, though?

Mr. DOWNING. I am not sure what you mean, a vote by Congress. I think Congress is, of course, always able to pass a law that would block this kind of thing, so that does not need to be said, I suppose, if you like, that Congress has that authority to do so.

Ms. JAYAPAL. Thank you. Mr. McGuinness, one of the chief concerns underlying this discussion has been the move towards data localization, and I know my time has expired, but if you could just quickly say, economically and politically, what are some of the harms of data localization laws?

Mr. MCGUINNESS. So, the United Kingdom, Her Majesty's government, is opposed to data localization. And we are opposed to it because we think it undoes the good that has been done economically and in terms of our ability finally to live our lives that we get from network systems that are agnostic about where data is and where it goes. So, we are opposed to it.

We see data localization, and the companies are better to speak to this, and I think you have colleagues from Google coming afterwards, but we see it as, frankly, slowing down the functioning of the internet in itself, perhaps technically, but also, frankly, potentially limiting the value of commerce through the internet. And also, frankly, it is going to lead to many more difficulties about ownership of data and the working system, so we are opposed to it. It is a matter of policy.

Chairman GOODLATTE. Well, I want to thank both of you for your participation and forbearance. We have been going for over 2 hours, and we thank you both for very interesting testimony and very important issue.

So, thank you, Mr. McGuinness, for coming across the pond, as they say, to join us today, and Mr. Downing, you did not have to travel quite as far, but it is important that the two of you be working together on finding ways to solve this problem. And we will definitely be playing a role up front and as we move forward. So, thank you both and we will excuse you——

Mr. DOWNING. Thank you very much. We look forward to working with you.

Chairman GOODLATTE. We excuse you and move to our second panel. And for those of you who may be wondering, we are going to go right into this second panel. So, if Mr. Salgado and Mr. Littlehale and Mr. Calabrese and Mr. Woods would come forward, we will get started right away.

While you are still standing, why not remain standing so I can swear you in? And then, I will introduce all of you. So, if you would raise your right hand.

Do you and each of you solemnly 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?

Let the record reflect that all of the witnesses responded in the affirmative.

And I will begin by introducing Mr. Salgado. Mr. Richard Salgado is the director of Law Enforcement and Information Security for Google. Previously, Mr. Salgado was with Yahoo, focusing on international security and compliance work. Mr. Salgado has

also served as senior counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice.

At the Department of Justice, Mr. Salgado specialized in investigating and prosecuting computer network cases that dealt with technology-driven privacy crimes. He has served as a legal lecturer at Stanford Law School, adjunct law professor at Georgetown University Law Center, and George Mason Law School, and as a faculty member of the National Judicial College. He is a graduate of the University of New Mexico and Yale Law School.

Mr. Richard Littlehale is the Special Agent in Charge of the Technical Services Unit at the Tennessee Bureau of Investigation. Mr. Littlehale coordinates and supervises a wide range of advanced technologies in support of law enforcement operations. Mr. Littlehale, along with TBI special agents, specialize in developing evidence from communications records in a wide range of cases, including homicides, internet crimes against children, and computer intrusions.

Mr. Littlehale has also served as a legal adviser to the Tennessee Bureau's Drug Investigation Division. In this role, he was responsible for providing field and office legal support for TBI criminal investigators and their supervisors. Mr. Littlehale is a graduate of Bowdoin College and Vanderbilt Law School.

Mr. Chris Calabrese is the vice president of Policy at the Center for Democracy and Technology. Mr. Calabrese has long been an advocate for privacy protections, having testified before Congress and appeared in many news media outlets discussing technology and privacy issues. Previously, Mr. Calabrese served as legislative counsel at the American Civil Liberties Union, Washington Legislative Office.

While at the ACLU, Mr. Calabrese led the office's advocacy efforts related to privacy by developing proactive strategies on pending Federal legislation concerning privacy and new technology. Prior to joining the ACLU, he served as legal counsel to the Massachusetts Senate majority leader. As legal counsel, Mr. Calabrese helped on legislation pertaining to privacy and antidiscrimination laws. He is a graduate of Harvard University and Georgetown University Law Center.

Professor Andrew Keane Woods is an assistant professor of law at the University of Kentucky College of Law. His teaching and scholarship include cybersecurity and the regulation of technology, contract law, international law, and empirical legal studies. Previously, Professor Woods was a post-doctoral fellow at Stanford University at the Center for International Security and Cooperation. Prior to that, he was a fellow at Harvard Law School. Professor Woods is a graduate of Brown University, Harvard Law School, and was a Gates Scholar at the University of Cambridge where he received his Ph.D. in politics.

I want to welcome all of you. Your written statement will be entered into the record in its entirety, and we ask that you summarize your testimony in 5 minutes. 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 your testimony. When the light turns red, that is it. Your time is up. And

we will start with Mr. Salgado. Yeah, we will start with Mr. Salgado. Welcome.

STATEMENTS OF RICHARD SALGADO, DIRECTOR, LAW ENFORCEMENT AND INFORMATION SECURITY, GOOGLE; RICHARD LITTLEHALE, SPECIAL AGENT IN CHARGE, TECHNICAL SERVICES UNIT, TENNESSEE BUREAU OF INVESTIGATION; CHRIS CALABRESE, VICE PRESIDENT, POLICY, CENTER FOR DEMOCRACY & TECHNOLOGY; AND ANDREW WOODS, ASSISTANT PROFESSOR OF LAW, UNIVERSITY OF KENTUCKY COLLEGE OF LAW

STATEMENT OF RICHARD SALGADO

Mr. SALGADO. Chairman Goodlatte and members of the committee, thank you for the opportunity to appear before you this afternoon to discuss the issue of cross-border law enforcement requests for user data.

Today, I want to discuss two distinct but related challenges that confront law enforcement agencies and service providers alike. These challenges arise from the fact that ECPA, a statute that has been vital for decades, has become antiquated in some key respects. This has left courts to interpret the statute in the context of facts that Congress could not have anticipated in 1986 when ECPA was passed.

It also leaves law enforcement agencies around the world looking for mechanisms to circumvent the statute. Some of those mechanisms are aggressive and even dangerous, but can also be made entirely unnecessary if we just modernize the law.

First, applying well-established rules of statutory interpretation, the Second Circuit Court of Appeals last year held that warrants issued under ECPA cannot compel service providers to search for, seize, and produce data that is stored outside the United States.

This, of course, has presented challenges to law enforcement, as you have heard from the Department of Justice. Other cases pending around the country that raise the same issues have judges working to understand what Congress intended in the statute that was enacted well before providers like Google and Facebook even existed.

Courts are being asked to resolve these disputes in ways that are divorced from sound policy solutions without the opportunity for robust debate among the stakeholders, and indeed, potentially entirely in closed courtrooms. This is hardly the path for appropriately addressing the equities of users, law enforcement agencies, service providers in addressing international comity. The source of all of this is a statute that needs to be updated to reflect the technical, business, and other realities of our time.

Second, ECPA includes a broad, so-called blocking provision that restricts the circumstances in which U.S. service providers may disclose the content of users' communications to government agencies outside the United States. There are legitimate reasons that a country may wish to control how and to whom data can be disclosed.

For example, to prevent disclosure of information to countries with poor human rights records. A broad blocking statute that is

divorced from these sorts of concerns and lacking nuance, however, can leave governments that have a legitimate need for information looking for alternative means of acquisition that unnecessarily redound to the detriment of users' privacy and civil liberties.

The blocking provision in ECPA is a source of enormous frustration for democratic countries that respect the rule of law and maintain robust, substantive, and procedural protections of civil liberties. These countries may be unable to obtain timely access to digital evidence, solely because it is retained by a U.S. service provider subject to ECPA, even for crimes that are wholly domestic in nature. The inability to obtain this data creates incentives for these countries to seek other unilateral techniques to get the information, including enforcement of their surveillance laws extraterritorially, even in the face of conflicting U.S. law.

It also creates incentives for enactment of data localization laws and aggressive investigation efforts that can undermine security in general. It is quite clear that the status quo is unsustainable as technology involves and has flourished and services offered by the U.S. internet companies are being used by people outside the U.S. Key assumptions around ECPA are obsolete. Congress should holistically modernize ECPA to address the many challenges that have emerged in recent years.

We respectfully recommend that an effort to update ECPA include the following three changes. First, require government entities in the U.S. to obtain a search warrant to compel the production of communications content from providers.

Second, provide clear mechanisms for the U.S. Government to obtain user data from service providers wherever the data may be stored, but with protections built in for certain cases when the U.S. Government seeks contents of users who are nationals of other countries or located abroad. Third, lift the blocking provision in ECPA to permit U.S. providers to disclose data to certain foreign governments in response to appropriate legal process in serious cases when the domestic laws of those foreign countries provide baseline privacy, due process, and human rights guarantees.

There is no panacea for the range of challenges presented by aging legal regimes. But we believe that these three steps ensure that ECPA's foundational construction is on the basis of sound policy principles that reflect the equity of users, law enforcement, service providers, and international comity. Thank you for your time, and I would be happy to answer questions.

Mr. COLLINS. The chair now recognizes Mr. Littlehale.

STATEMENT OF RICHARD LITTLEHALE

Mr. LITTLEHALE. Mr. Chairman, Ranking Member Conyers, members of the committee, thank you for inviting me to testify. I am a technical investigator in Tennessee, and I chair the Technology and Digital Evidence Committee of the Association of State Criminal Investigative Agencies.

For more than 20 years, I have helped criminal investigators obtain and use communications records for use in both technical investigations, like internet crimes against children in cyber cases, and in the range of other criminal cases that we support.

My community faces a range of barriers that impede our lawful access to digital evidence, and the problem is growing as mobile apps and internet-connected devices proliferate. We are told it is a golden age of surveillance, but those of us in the trenches doing investigations and protecting the public see things differently as we are turned away empty-handed from one source of critical evidence after another.

The challenge that brings us here today is the Second Circuit's Microsoft/Ireland decision, which is a growing problem for the State and local law enforcement community. Despite grave concerns expressed by concurring and dissenting judges, despite district court judges in five other circuits who have declined to follow the ruling, many tech companies continue to apply the standard across the board and reject legal demands everywhere in the U.S., creating another blind spot in State and local law enforcement's ability to access digital evidence.

Let me give a couple of examples to show you why this practice is so frustrating for us. In testimony before the Senate Judiciary Committee last month, one of my peers from Massachusetts described a California case involving the disappearance and suspected murder of a young girl.

The investigators developed information that the contents of an account maintained with a cloud service provider could help them determine what happened to the girl and where to look for additional evidence. A court agreed and issued a search warrant. The service provider objected to the production of any contents stored outside the U.S., which according to the investigators, included the categories of records most likely to be useful in that case.

A second example comes from the State of Mississippi. A service provider advised the National Center for Missing and Exploited Children that an unknown party had uploaded child exploitation images to a cloud account. The investigator, who got the case from NCMEC, sought a search warrant for the contents of the account. While waiting for the service provider to respond, the investigator was able to identify and confront a suspect, who confessed that it was his practice to meet people online and share child pornography images in order to receive similar images in return.

When asked whether he received any pictures that made him think the senders were actively molesting children, he stated he did not know, but that he was talking with "some very bad people." The investigator received a foreign evidence denial as to some of the requested account contents, though everything points to the suspect accessing the account from within Mississippi. The investigator sent two further requests for information on how to obtain the content that might lead to unknown minor victims. As of yesterday, the investigator has not received a response.

When investigators face foreign evidence denials like these, their only option is to pursue the mutual legal assistance treaty process, which is widely regarded in the law enforcement community as too cumbersome to be effective. Delays run from many months to years.

This simply does not allow investigators to obtain the evidence that they need in a timeframe that is useful. All of that assumes,

of course, that the service provider tells the agency what country to direct the MLAT to, which does not always happen.

Everyone agrees that this situation is problematic. Evidence that can help solve crimes committed in the U.S. by people in the U.S. against victims in the U.S. is often unavailable even after a judge signs an appropriate legal demand. In Judge Lynch's concurrence to the Microsoft Ireland panel decision, he writes, "Without any illusion that the result should be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy."

We agree, and we hope that Congress can take quick action, carefully weighing public safety needs alongside the business interests of providers and the privacy concerns of their customers. Public safety should not be an afterthought or side issue as technology advances. My peers and I are eager to help where we can in collaboration with our fellow Federal partners.

To wrap up, Mr. Chairman, State and local law enforcement investigators see this issue of evidence stored abroad as part of a broader policy challenge which includes, among other things, the lack of a legal framework around service provider response to legal demands, data retention, and a lack of good information about what evidence is even available on service provider networks. We agree that laws intended to provide law enforcement access to digital evidence like ECPA and CALEA need to be updated to make sense in the 21st century, but those updates must be balanced to address the very real needs of the law enforcement community and crime victims to avoid unnecessary barriers to investigations. We greatly appreciate this committee's ongoing solicitation of our input, and I look forward to your questions.

Mr. COLLINS. Thank you, sir. Mr. Calabrese.

STATEMENT OF CHRIS CALABRESE

Mr. CALABRESE. Thank you, Chairman Goodlatte, Ranking Member Conyers, members of the committee. First, let me just say how happy I am to see everyone here safe and sound after yesterday's tragic events. Our thoughts and prayers go out to the victims, but I am just glad to see so many friendly faces here safe and well. Thank you.

We appreciate the opportunity to testify on behalf of the Center for Democracy and Technology. CDT is a nonpartisan advocacy organization dedicated to protecting privacy, free speech, and innovation online. We applaud the committee for holding this hearing today. There is no question that the system for sharing information across borders is in need of reform. Law enforcement is correct that it is slow and sometimes frustrating.

U.S. service providers rightly worry about being caught up in a conflict of laws. However, it is worth noting the system does have benefits. The most notable is that in many cases, citizens around the world are protected by the strong privacy guarantees of the U.S. Constitution, specifically the warrant requirement of the Fourth Amendment. We must not lose that commitment to privacy even as we reform the broken elements of the system.

CDT believes the best way to achieve reform is through a package of legislative changes, specifically, passage of the Email Privacy Act, adoption of a structure for privacy-protective bilateral agree-

ments, mutual legal assistance treaty reform, and enactment of a version of the International Communications Privacy Act, ICPA.

First, Congress must set a privacy baseline in the U.S. in U.S. law by passing the Email Privacy Act. This committee is intimately familiar with this bill, having stewarded it through unanimous House passage over the last two Congresses. While a warrant for content is generally assumed to be the default, including by the Department of Justice in its testimony today, as the committee knows, that is not what ECPA says.

Because the law was passed in 1986 and has not been substantially updated since, in many cases, it authorizes access to content with the use of a simple subpoena with notice. Service providers are to be commended for insisting on a warrant pursuant to the Sixth Circuit decision in Warshak, and DOJ has stated that seeking a warrant is their policy in criminal cases. But appellate court decisions and Department policies are not a substitute for Federal statutory reform.

Second, once we have a baseline in U.S. law, we must extend it to other rights-respecting Nations through a strong privacy-protective framework of bilateral agreements between Nations. These agreements would be safety valves, allowing speedy access for law enforcement, reducing conflicts of law, and reducing pressure on the MLAT system. The Department of Justice has made a good start in laying out such a framework.

There are, however, important areas where it must improve, including how the proposal handles which Nations will qualify as partners, enhancements to legal standards for accessing information, and limitations on privacy-invasive techniques like the use of metadata and wiretapping. With these improvements, bilateral agreements can speed law enforcement access, respect national law, and improve privacy.

Third, since not every Nation will qualify for a bilateral agreement, Congress should reform the existing MLAT process. ICPA contains important reforms that should be adopted to speed the process. In addition, the European Union is developing materials to educate their local law enforcement on how to best meet the U.S. probable cause standard. Those materials can and should be used globally.

Finally, any proposal should include the principles embodied in ICPA when U.S. law enforcement seeks to access communications. ICPA rightly moves away from the use of location of data as a standard and towards the nationality of individuals under investigation. It also respects the interests of other Nations by deferring to them in cases where MLAT agreements are in place. This framework is not perfect.

Specifically, it may result in adoption of extraterritorial warrants by other Nations or unintentionally allow some Nations to slow investigations. CDT is happy to work with the committee to address these concerns and is encouraged by the number of positive ideas already under discussion, including a mandatory comity analysis by courts and reciprocal notice and control provisions for other Nations.

While none of these solutions will be enough on their own, CDT believes that collectively, they can safeguard international comity,

assist law enforcement, and most importantly, protect individual privacy.

Mr. COLLINS. Thank you, sir. Now, Professor Woods.

STATEMENT OF ANDREW WOODS

Mr. WOODS. Thank you, Chairman Goodlatte, Ranking Member Conyers, members of the committee. Thank you for inviting me to testify here today.

ECPA is the single leading cause of conflicts of laws in the tech world today, so I am grateful that committee has shown great leadership in this context. The good news is that this is actually a pretty easy problem to fix.

ECPA operates, as you have heard, as a blocking statute, standing in the way of American tech firms' compliance with lawful government requests for data both here and abroad. Remove those blocking features, and you solve the bulk of the problem. Now, this means two things. First, reverse the Second Circuit's recent decision so that a production order under ECPA can compel a U.S. firm to comply, regardless of where they choose to store their data. And second, allow U.S. firms to voluntarily comply with foreign law enforcement requests wherever they choose to operate.

On this second point, I actually think the solution may be simpler than DOJ has made it out to be. You need not specify which countries can enforce their laws against American tech firms, nor the conditions under which they do so. I used to think that was a really good idea. After all, if you care about privacy, surely you would want to clarify how and when and which foreign governments can access internet content.

But I am less sure about the wisdom of telling other countries how to behave today. You do not tell Citibank and Costco under what conditions they can comply with British law. Why tell Google and Microsoft? Indeed, if you were to propose to make it harder for American banks or America's retailers to do business in other countries, you would likely never hear the end of it. Not only does blocking foreign government interests make them mad, with all of the attendant diplomatic fallout, but I believe it makes the internet less secure.

When countries cannot enforce their laws, they do a number of unfortunate things, and in particular, three.

First, they make it hard on U.S. businesses, arresting their employees, increasing operating costs, often by demanding that data be stored locally.

Two, they increase their efforts at surveillance, often without court supervision.

And three, they threaten to retaliate against the United States by imposing their own ECPA-like blocking statutes. This last point is an underappreciated one. In a not-too-distant future, many Americans, perhaps most, will be running around with a foreign-made app on their phones.

In the wake of some crime, American law enforcement will seek access to data held by the foreign app maker doing business here in the U.S. If the app maker is from a country that has a blocking statute like ECPA or a country that is excluded from the bilateral

or multilateral club that DOJ has envisioned, our law enforcement agents will be in trouble.

These foreign government reactions to our blocking statute are unfortunate, but they are also understandable. Indeed, it is partly American law enforcement's own frustration here that has led them to call for back doors on encrypted services, the unregulated use of Stingrays, and other desperate and, in my view, foolish measures.

When I speak to prosecutors in Brazil and India and France, they ask one question: why should we need to follow American rules in order to enforce our own laws on our own soil? The answer, of course, is that they should not. The lodestar of conflicts of laws has always been the respect for sovereign interests, and if we craft a regime that does not do that, I fear we will regret it.

So, to briefly summarize, ECPA is easy to fix at home and abroad. The location of data should not matter. Rather, the location of the investigation should. Except in extreme circumstances, if a service provider is physically present in a jurisdiction providing services, making money there, they should be in a position to respond to lawful and legitimate law enforcement requests.

That is true here, and that is true abroad. This is the position nearly every other American company finds itself in, and tech firms should be no different. To make this a reality, you need to reverse the Second Circuit's decision, and you need to lift ECPA's blocking features.

Now, I just want to emphasize that I say this as someone who cares deeply about privacy and security on the internet. In my view, the only way to secure the future of a global internet is to provide room for governance differences around the world. Either the laws bend, or the technology will be bent and broken.

Keep in mind, we are not talking today about the hard stuff like warrantless surveillance, State efforts to weaken encryption or force data localization. Rather, we are talking about a simple step that you can take today to prevent those things. Thank you very much for your time, and I look forward to your questions.

Mr. COLLINS [presiding]. Thank you, Professor Woods. I will start the questioning here as we go.

Mr. Salgado, I have a question. From your perspective, how urgent is this problem? And are we talking only a handful of countries here that are enacting data production and data localization requirements? What are the impact, you know, if you can quickly sort of answer that, the impact of these laws?

Mr. SALGADO. Thank you for the question. I think it is quite urgent. The two issues that we are talking about here, both the blocking statute question about the ability to comply with requests outside the United States as well as being able to produce data that is stored outside of the United States to U.S. authorities, both of those are urgent matters. They are threats to public safety. They are threats to American companies.

Mr. COLLINS. OK. And also, then, it has been talked about a little bit here, some have argued that it should be nationality or location of the customer that determines the country's law, you know, which one controls. It is sort of a two-part question. One, is Google able to definitively determine the location of the customer? And

number two, are they definitively able to determine the nationality of a customer?

Mr. SALGADO. The answer is no. We very unlikely would be able to be determinative. We may have information that could inform a court that needs to decide whether notice, if that is the approach we are taking, needs to be given to the other jurisdiction.

So, a provider may have relevant information to help inform a decision like that. Law enforcement itself should probably bear the burden of being able to establish that they have at least gone through the steps to try to determine the location of the user to determine whether they are excused from other requirements.

Mr. COLLINS. And in some ways, would not the nationality actually be a slippery slope question for a tech company, or frankly, even law enforcement there, unless there is, you know, definitive kind of answers to that question?

Mr. SALGADO. There needs to be a standard. It may be that the standard is not definitive. It is something less than that, that there is credible evidence, you know, there is a whole list of possible standards.

Mr. COLLINS. Preponderance?

Mr. SALGADO. Preponderance, it could be——

Mr. COLLINS. OK.

Mr. SALGADO. Right, from mere evidence all the way to the full more likely than not.

Mr. COLLINS. Without doubt.

Mr. SALGADO. So, that would be an issue for debate to come up with what is the right level.

Mr. COLLINS. Great. Well, I will come back in just a second. Professor Woods, what kind of reforms to the MLAT process do you believe should be made? And you know, these impacts do you think would improve the process it would have on international conflict of laws that are being discussed?

Mr. WOODS. Yeah. So, as I say, the easiest way to resolve this problem is to allow countries that operate globally to respond to lawful requests where they receive them. I would emphasize lawful. I agree with my colleagues here that we may be able to parse out some countries we think do not operate by the rule of law.

But we want to be in a position where the MLAT system, which needs to be reformed in a number of ways, and I have got ideas about how to do that, happy to speak to that, but the MLAT system should not be the place where cross-border data requests are made.

Mr. COLLINS. OK.

Mr. WOODS. It is just not built for that.

Mr. COLLINS. OK. Granted with that. And again, this is not a small subject we can discuss. But I do have a specific maybe on this. What effect does data localization laws have on U.S. national security, the ability of U.S. intelligence community to collect the necessary intelligence to protect the homeland? Can you answer that maybe, briefly?

Mr. WOODS. My understanding is that it is considerably harder for U.S. law enforcement to get access to data when it is stored under a forced localization mandate abroad.

Mr. COLLINS. OK. All right. One question, and we have had this before when Mr. Littlehale has been here before, and we have had questions. But I do want to go back. And I understand the balance of law enforcement and the needs here. But in most examples, which, of course, would be the problems, Mr. Salgado, do you think that every example on a negative light that was given is where tech was not cooperating? I would like to at least hear the other side, because we have heard this before. Tech does cooperate with law enforcement, correct?

Mr. SALGADO. Oh, well, certainly. Speaking for Google, the rules are generally pretty clear about what it is we are required to do and what the legal process should look like, and it works pretty well. There is emergency situations where the law enforcement may not have time to go through legal process. We respond to those to save lives and to prevent physical injury when needed. I think in general, the ecosystem works pretty well.

The statute, though, is pretty aged at this point, and it is no longer reflecting what is really happening. And the result of that is that law enforcement is getting frustrated because of interpretations like what we saw out of the Second Circuit, and other jurisdictions are having to adopt to the limitations they are facing under U.S. law by engaging in sometimes unsavory techniques to try to be able to get the information.

Mr. COLLINS. So, really, from your perspective, at the end of the day, you know, you may have differences of opinion on protection of privacy from your business model and other standpoints, but at the end of the day, your company, in particular, but other tech companies as well who deal in this are more than willing to find a solution here that protects not only privacy business decisions, but also the needs of our security and our law enforcement?

Mr. SALGADO. Absolutely right. And, in fact, this is a situation where I think with these recommendations we have made today, we can actually increase privacy protections and enhance law enforcement access——

Mr. COLLINS. Right. So, any broad sweeping discussion, that is the more true answer, and there are exceptions to everything. But I think we are moving forward on an answer, and that is the good part.

With that, I am honored to turn over the questioning to my dear friend, the ranking member of this full committee, Mr. John Conyers.

Mr. CONYERS. Thank you, sir. And I appreciate the witnesses and their differing views. But let me start with Mr. Calabrese, please. Sir, in your view, what are the shortcomings of the administration's proposed criteria for admission into the bilateral framework?

Mr. CALABRESE. Thank you, Mr. Conyers. So, I think there are four. The first is the way the inclusion in the club is handled. So, first of all, we should not have factors to consider; we should have mandatory standards that have to be met. And we should also have a better process for lifting up the factual basis for making that determination, an APA-type process so we can get facts for whether you meet particular standards. The second is improvements to how we handle metadata.

Obviously, this is incredibly sensitive information. And ECPA currently allows the voluntary sharing of metadata with foreign countries, and I think we need to address that. The third is I think we need a bar on wiretapping. Wiretapping is among the most sensitive types of invasion we have in our legal system, and I do not think we should allow it willy-nilly to be done by foreign governments, almost certainly at a lower standard.

And finally, we need to look closely at the substantive standards and procedural requirements put in place by the bilateral agreement and look to raise them to be closer to a probable cause standard.

Mr. CONYERS. Thank you, sir. Let me ask you, in your opinion, must we hold other Nations to our Fourth Amendment standard for access to content? For example, a warrant based on probable cause, even that standard is wholly foreign to legal systems that on the whole have decent privacy regimes?

Mr. CALABRESE. It is a very fair question. I think the first thing we should do is hold ourselves, of course, to the probable cause standard and pass the Email Privacy Act. The second thing, I think what we need to look for is comparable legal regimes, comparable legal standards. And I do not think we should insist on, foreign governments having exactly the same rules we have. They need to be comparable privacy standards. They need to meet international norms, such as human rights standards. And if we can get that kind of normalization with our key allies, I think we will have real privacy improvements.

Mr. CONYERS. Anyone want to add anything to that? Yes, sir?

Mr. WOODS. It is a great question, and when I have looked at the burdens on the MLAT System, there are at least two distinct kinds of burdens. One is that foreign countries say, "Why should we have to go through this process and make the request to the United States, let alone just solve it here domestically in our courts?" If it is a Brazilian murder, a Brazilian crime, Brazilian victim, and everything happens in Rio, why are we contacting the U.S.?" That is crazy, right? Separate from that, wherever the request happens, whether it is international or not, there is a resentment of having to use an American standard.

And I fear that if we adopt a regime that relies, as you say, on an American standard like the Fourth Amendment standard, although it is the gold standard, we will incentivize States who resent being left out of the club or being forced to bow to that American standard, that they will do things like find ways to enforce their laws without our permission. And every single one of those possible ways to do that is worse than us negotiating a reasonable way for them to get lawful access to data.

Mr. CONYERS. Thank you. Mr. Salgado, has the Microsoft decision changed how your company responds to the government's demands for information under the Stored Communications Act?

Mr. SALGADO. Yes, sir. It certainly has. As I think the chairman said in the opening comments, the Second Circuit pointed out that there is a problem in the statute that really, until then, had not been pointed out, and that is that it appears that the statute does not cover data that is outside the United States and not in the United States or that the warrant requirement does not reach that

far. As a result, that means that the warrants we receive, actually, are not effective to reach the data that is stored outside the United States. And as a result, we do not produce that data in response to those warrants.

Mr. CONYERS. Thank you, Mr. Chairman.

Mr. COLLINS. Thank you for that. The chair now recognizes Mr. Marino. And just for the sake of the meeting, after Mr. Marino's question because votes have been called, we will be adjourning, in light of the situation, the rest of the day. So, Mr. Marino, your line of question.

Mr. MARINO. Thank you. I am going to cut right to the chase. First of all, without objection, I would like to introduce into the record the testimony of Microsoft's chief legal officer, Brad Smith, from the Senate Judiciary Committee's hearing on this same topic from May 10, 2017.

Mr. COLLINS. Without objection, so ordered.

This information is available at the Committee and can be accessed online at https://docs.house.gov/meetings/JU/JU00/20170615/106117/HHRG-115-JU00-20170615-SD002.pdf.

Mr. MARINO. Thank you. Excuse me, thank you for being here. Are you familiar with my legislation from over the last 2 years, the LEADS Act? Give me your opinion. Ms. DelBene and I, from across the aisle, put this together, and it just puts together a legal framework for U.S. law agencies to acquire evidence from overseas.

I always think something needs to be tweaked, but can each of you take a couple of seconds and address the LEADS Act and what might have to be added or taken out? Because I am a law enforcement guy, and I do like the idea that we have agreed, so far, I think we have agreed, that business and law enforcement have to sit down and work this out.

There has got to be give and take on each side, and from a law enforcement perspective, I have been in situations where children have been kidnapped. As a prosecutor, we know that we have to have evidence almost immediately or else within 48 hours because the chances of retrieving them after that are very small. And we cannot be in a position where we are waiting for someone to argue an issue brought before a court saying why we should or should not respond to something. So, could you please respond to that array of questions?

Mr. SALGADO. I guess we will start on this end. Yes, I think that there is an agreement here that we need to do something, that we are in an untenable situation, all of the stakeholders here, and I would include the courts in that. I think that the solution, though, is not in a statutory change that doubles down on location of data. I think we need to change the focus of the limits of the warrant requirement to the user rather than where the user's data is located.

And hence, the recommendation that we make, which is let's change the statute to reflect where the user is or where the user is a national, and focus on those equities rather than in the case of Google, where the intelligent, modern network has selected to store the data for some period of time.

Mr. MARINO. OK. Anyone else care to respond?

Mr. CALABRESE. Yeah. First of all, thank you. You clearly started an important debate with your legislation that is ongoing today. And I think we are getting closer to a solution, and it is a good piece of legislation. I mean, there were a couple of things I think concerned CDT. One was the one that Rick just mentioned, which is, sort of, you worry about embedding a technical solution or, you know, interfering with how a technical outcome would happen within an industry's systems with a legal standard.

I think the second one, and one that CDT is worried about, is potentially the impetus towards encouraging other countries to engage in extraterritorial warrants. And I think that is one of the reasons we have talked so much about bilateral agreements. I think they are a nice safety valve in this same context, right? Because they say, "That is fine. We want to give you the same deal that we have here, and here is how you do it. Here is the whole process." And I think that is an important safety valve, and I think, obviously, clearly be coupled with the work that you are already doing.

Mr. MARINO. We have to respect other countries' laws, but we cannot be put in a position where those laws are so in opposite in law enforcement to what ours are.

Mr. WOODS. I just want to echo Chris' point that you are at the forefront in starting to look at this with the LEADS Act, and I was excited when it was announced.

Mr. MARINO. I have got to give my staff credit for that. They are pretty much the brains of the outfit.

Mr. WOODS. I also want to echo Rick's concern about having anything turn on the location of the data. I think at the end of the day, the old-school principles of jurisdiction ought to apply; and that is to say, I think consistent with what you were saying, legitimate State interests.

When the United States has a legitimate interest in resolving a crime that has happened here in the United States, if a business is here in the United States, doing business, making money, availing itself of this forum, it ought to be responsive to law enforcement investigations. That is not about where they store their data. That is about where they operate and where the crime occurs.

Mr. LITTLEHALE. I would just very quickly point out that from our perspective, the real challenge comes in looking at reform in the area of all of these statutes where we are going to get the information in order to make the demonstrations that we are required to about where the particular, either the data is or the person is, nationality, and so forth.

Very often, in a time-sensitive environment, we are dealing with a limited pool of information where we can get information because, as was pointed out earlier in the hearing, we do not have the ability to go out and gather that evidence ourselves. We are dependent on what we can get by service of legal demands. So, I think any effort to look at that must take that set of realities into account. And we look forward to the conversation.

Mr. COLLINS. Thank you. This concludes today's hearing. Thanks to all the witnesses for attending and sitting through what has been a longer hearing. Without objection, all members will have 5 legislative days to submit additional written questions for the wit-

nesses and additional materials for the record. With that, the hearing is now adjourned.

[Whereupon, at 1:23 p.m., the committee was adjourned.]

July 5, 2017

Mr. Paddy McGuinness
UK Deputy National Security Advisor
Oxford, UK

Dear Mr. McGuinness,

The Committee on the Judiciary held a hearing on "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era" on Thursday, June 15, 2017 at 10:00 a.m. 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 to the Committee by Friday, September 1, 2017 via email to Alley.Adcock@mail.house.gov or postal mail to the Committee on the Judiciary, Attention: Alley Adcock, 2138 Rayburn House Office Building, Washington, DC, 20515. If you have any further questions or concerns, please contact Alley Adcock on my staff at 202-225-3951 or by email: Alley.Adcock@mail.house.gov.

Thank you again for your participation in the hearing.

Sincerely,

Bob Goodlatte
Chairman

Enclosure

Questions for the Record

Submitted by Rep. Zoe Lofgren

For **Mr. Paddy McGuinness**, Deputy National Security Advisor, Oxford, UK

2) In response to a question on the effect of the European Union's General Data Protection Regulation on non-E.U. law enforcement requests for data stored in an E.U. country, you testified that complying with U.K. law enforcement requests for data stored in the E.U. would not violate article 48 of the GDPR and create a conflict of laws issues for U.K. companies or U.S. companies with a U.K. presence.

   Could you please elaborate on your reasoning and provide a detailed analysis as to why such requests would not be a violation of article 48 of the GDPR?

July 5, 2017

Mr. Richard Downing
Acting Deputy Assistant Attorney General
Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Downing,

The Committee on the Judiciary held a hearing on "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era" on Thursday, June 15, 2017 at 10:00 a.m. 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 to the Committee by Friday September 1, 2017 via email to Alley.Adcock@mail.house.gov or postal mail to the Committee on the Judiciary, Attention: Alley Adcock, 2138 Rayburn House Office Building, Washington, DC, 20515. If you have any further questions or concerns, please contact Alley Adcock on my staff at 202-225-3951 or by email: Alley.Adcock@mail.house.gov.

Thank you again for your participation in the hearing.

Sincerely,

Bob Goodlatte
Chairman

Enclosure

Questions for the Record

Submitted by Rep. Zoe Lofgren

For **Mr. Richard Downing**, Acting Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice:

1) In response to a question on the effect of the European Union's General Data Protection Regulation on U.S. law enforcement requests for data stored in an E.U. country, you stated that "we do not believe that the GDPR will pose significant conflicts for US companies" when complying with US law enforcement requests for data stored in the E.U.

   Could you please elaborate on DOJ's reasoning and provide a detailed analysis as to why such requests would not be a violation of article 48 of the GDPR?