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

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

February 25, 2016

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

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

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

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

This is good news.

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

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

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

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

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

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

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

I. The International Situation is Worsening.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

II. Our Electronic Privacy Laws Are Outdated.

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

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

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

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

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

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

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

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

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

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

---

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

[5] *Id.*

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

[7] *Id.*

[8] *Id.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. MLATs Should be Modernized.

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

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

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

B. Creation of a Modern International Framework.

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

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

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

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

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

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

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

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

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

---

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

* * *

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