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

Senate Judiciary Committee
Subcommittee on Crime and Terrorism
Hearing on Law Enforcement Access to Data Stored Across Borders:
Facilitating Cooperation and Protecting Rights

May 10, 2017

Chairman Graham, Ranking Member Whitehouse, and Members of the Subcommittee, thank you for the opportunity to provide Microsoft's perspective on the important issues raised by the need for law enforcement to access digital information across national borders, and how we can best facilitate cooperation and protect rights in accomplishing that important goal.

Microsoft is a global technology company that supports more than one billion customers in 90 markets around the world. The U.S. technology industry—companies big and small—not only retains a large portion of the market share, but continues to drive innovation in emerging fields from cloud computing to the Internet of Things, from autonomous vehicles to artificial intelligence. Despite the historical concentration of leading technology companies inside the United States, it is important to remember that less than five percent of the world's population lives in our country. Like other leading U.S. technology firms, we are a global company, offering products and services to people and businesses around the world.

Our customers—from individual consumers to large multinational corporations—increasingly store their most sensitive information in our datacenters around the world. To succeed in the global marketplace, U.S. technology companies must earn and preserve the trust and confidence of our customers worldwide. A critical element of maintaining that trust is that we protect the privacy and confidentiality of our customers' data and we comply with the laws and respect the rights of consumers and companies in the countries in which we do business. This, however, has become increasingly difficult to do.

The United States is not alone in focusing on the topics at the center of this hearing; these very same issues are the subject of intense debate and policymaking in capitals around the world. National governments, understanding both the sensitive nature of the information their citizens are entrusting to technology companies and the increasing importance of digital evidence in criminal investigations, are enacting new laws or reinterpreting old laws to reach evidence extraterritorially, as well as to protect the privacy and personal safety of their citizens. Regrettably, nations are taking these steps often without understanding the complexity or the implications of applying them to modern, global technology. As a result, technology companies confront an increasingly chaotic legal environment, a patchwork of conflicting blocking statutes and disclosure obligations. And because many of these steps have been taken unilaterally—rather than through existing treaty-based mechanisms or a new, modern international framework—technology companies increasingly encounter situations in which law enforcement in one country unilaterally demand access to digital information in another, while the laws and sovereignty of the other country prohibit disclosure.

The principal U.S. law regulating governmental access to digital information—the Electronic Communications Privacy Act ("ECPA")—is more than 30 years old. Recognizing that the laws in this country and the world are outdated in many respects, Congress has an opportunity to lead, to set an example that is worthy of emulation by other governments across the globe. In doing so, Congress must be clear-eyed about the complexity of the challenges presented by law enforcement's need for cross-border access to data. It is a mistake to assume this is a simple problem that calls for a simple solution. Papering over the complexity with a legislative "quick fix" will exacerbate the problems already caused by our outdated laws, and ultimately will fail to serve anyone's interests—from law enforcement to our customers.

This increasingly common combination of unilateral assertions of extraterritorial access and overbroad blocking statutes creates several significant problems:

- *The current legal framework undermines law enforcement's ability to obtain information over the long term.* Until recently, policymakers have been presented with two options—use the Mutual Legal Assistance Treaty ("MLAT") process or adopt broad or unlimited authorities to access information. Law enforcement has credibly complained that the first option does not permit them to operate at the speed necessary to confront modern threats, from international terrorism to cybercrime. The second option, meanwhile, undeniably results in international friction, stifles law enforcement cooperation, and promotes digital protectionism. In the end, neither option will produce the best results for law enforcement authorities, so the only sensible approach is to develop a comprehensive, modern international legal framework.

- *The current legal framework creates conflicting legal obligations.* Unilateral demands lead to conflicts of law insofar as they require technology companies to produce digital information to authorities in one country when those same companies are barred from doing so by the law of another country. Those conflicts put technology companies in the impossible position of choosing which country's law to obey and which to violate. While this may seem trivial to some, I can attest that the threat of significant fines or imprisonment—in the United States and in other countries where we operate—are very real.

- *The current legal framework ultimately undermines the privacy of U.S. citizens*. When the United States claims the unlimited extraterritorial access to seize digital evidence, other countries are emboldened to do the same to us, without respecting U.S. laws safeguarding that U.S. citizen's private information. This puts the privacy of American consumers and businesses at risk.

- *The current legal framework drives customers to foreign competitors.* Whether it is the result of diminished trust, legal restrictions mandating data localization, or procurement requirements, recent developments risk putting American companies at a competitive disadvantage globally.

- *The current legal framework impedes American allies' legitimate law enforcement investigations.* ECPA precludes U.S. technology companies from responding to lawful requests for stored content from foreign law enforcement agencies, even when the

requesting countries have strong privacy and human rights records and are only seeking data about their own citizens. Forcing our foreign partners to rely entirely on the MLAT system to obtain digital evidence constrains their ability to protect the public and is not sustainable.

All of these problems are real, and they must be taken into account in any legislation. I discuss them further below. But in short, Congress should resist the false promise of any simplistic or "quick fix." Failure to enact a modern comprehensive legislative framework will ultimately undermine U.S. interests, including the interests of law enforcement and our customers. Microsoft and others in the technology industry are ready and willing to engage constructively with Congress and the Administration on these issues. It is critical for all stakeholders to come together around a legislative solution—such as the proposals currently under consideration. Our laws can no longer ignore the technological progress made over the past three decades. We need a comprehensive framework that accounts for today's globally interconnected economy and can serve as a durable, lasting solution to each of these challenges.

I. The United States continues to be the world's technological leader.

The United States has long been the world's leader in developing innovative new technologies that create jobs, increase productivity, and empower businesses and individuals worldwide. Globally, five of the ten most valuable companies in the world, as measured by market capitalization, are American technology companies – Apple, Alphabet, Microsoft, Amazon.com, and Facebook.[1] Measured by revenue, seven of the world's ten largest technology companies hail from the United States, including Apple, Microsoft, Alphabet, Intel, IBM, Cisco Systems, and Oracle.[2] U.S. companies are well-positioned to continue leading in this sector—including in the rapidly growing cloud computing market. Eight of the top ten fastest growing cloud companies are headquartered in the United States, according to a recent study by PWC.[3]

This is important for the U.S. economy, jobs, and broader interests. In the United States alone, the software industry supports nearly 10 million jobs nationwide, according to a 2016 report by BSA | The Software Alliance.[4] Technology creates jobs for a wide range of professionals across the U.S. economy, including not only those persons directly employed by software companies but also the jobs the software industry supports through indirect and induced

---

[1] *See* Stephen Gandel, *These Are the 10 Most Valuable Companies in the Fortune 500*, Fortune, (Feb. 4, 2016), *available at* http://fortune.com/2016/02/04/most-valuable-companies-fortune-500-apple/.

[2] *See* Samantha Sharf, *The World's Largest Tech Companies 2016*, Forbes, May 26, 2016, https://www.forbes.com/sites/ samanthasharf/2016/05/26/the-worlds-largest-tech-companies-2016-apple-bests-samsung-microsoft-and-alphabet/#295561e6b661.

[3] *See* PWC, 25 Fastest Growing Cloud Companies (2016), *available at* https://www.pwc.com/gx/en/technology/publications/global-software-100-leaders/assets/25-fastest-growing-cloud-companies.pdf.

[4] *See* BSA | The Software Alliance, *The $1 Trillion Economic Impact of Software*, June 2016, *available at* http://softwareimpact.bsa.org/pdf/Economic_Impact_of_Software_Report.pdf.

impacts. Software innovation adds more than a trillion dollars a year to the U.S. economy, according to BSA.

Outside the technology sector, a wide range of businesses and individuals increasingly rely on technology providers to store their most sensitive digital information—and to ensure that information can be accessed seamlessly, from anywhere in the world. Indeed, cloud computing is quickly becoming the norm for American technology users. For individuals, the cloud can be as simple as using Facebook or Gmail or Yahoo or Outlook.com, through which people entrust technology providers to store their private communications on the provider's own server, to be accessed remotely from any computer or device connected to the Internet. For businesses, the cloud also enables new innovations like artificial intelligence, machine learning, and big data analytics, which will become the basis of future revolutions in technological progress.

More important, this technology enables all U.S. companies, big and small, to drive innovation in their sectors. From farming to heating and cooling, we are seeing businesses of all kinds leverage the powerful data analytics made possible by the cloud to revolutionize their industries or offer new products and services. We are still in the early stages of adoption of cloud computing, which gives small-to-medium sized enterprises access to sophisticated capabilities once only available to huge multinationals.[5] The cloud enhances businesses' ability to access reliable and scalable infrastructure resources, use configurable platforms that allow for integration with vendors or customers, and improve their IT capabilities.[6] Ultimately, the cloud enables businesses of all sizes to serve wider markets more efficiently and effectively—even as they reduce costs.

U.S. companies serving customers worldwide are able to leverage our innovative and competitive domestic marketplace, high levels of expertise and talent, name recognition and first-mover advantages.[7] Still, U.S. technology companies face strong global competitors, including foreign-based competitors—companies that often have solid or growing stakes in their home countries.[8] And our competitors are aided by concerns overseas about U.S. government access to data stored with U.S. providers. As a report published last April by the International Trade Administration observed, "many foreign buyers have expressed concerns about who might

---

[5] *See* Deloitte, 2017 Technology Industry Outlook, at 2, *available at* https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-technology-industry-outlook.pdf.

[6] *See* McKinsey, Winning in the SMB Cloud, at 3, July 2011, *available at* http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/High%20Tech/PDFs/Winning_in_the_SMB_Cloud.aspx.

[7] *See* International Trade Administration, *A Market Assessment Tool for U.S. Exporters*, April 2016, at 9 *available at* http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf.

[8] *Id.*

(continued…)

have access to their data."[9] "[T]rust-related issues have increasingly caused hesitations among those considering purchasing of cloud service from U.S. vendors."[10]

II. Microsoft's Second Circuit litigation illustrates that laws governing access to digital evidence are outdated.

We believe that customers' data should be disclosed to governments only with clear legal authority. Reflecting this, Microsoft sought guidance from courts on the extraterritorial reach of U.S. search warrants under ECPA. On December 18, 2013, we brought a lawsuit challenging the validity of a warrant issued by federal prosecutors seeking email content stored in our Dublin, Ireland, datacenter. We were supported in our challenge by numerous groups that filed amicus briefs in the case, including 29 technology and media companies, 23 trade associations and advocacy groups, 35 leading computer scientists, and the government of Ireland. On July 14, 2016, the U.S. Court of Appeals for the Second Circuit ruled unanimously in our favor, finding that a warrant issued under ECPA cannot lawfully compel a company like Microsoft to produce the contents of a customer email account stored outside the United States.

This case was never intended to provide all the answers. No single lawsuit could possibly do that. At its heart, the case illustrates how technology has evolved over the past three decades—but the law has not. As we argued in the case, the Second Circuit was called upon to apply ECPA to a technological scenario that did not exist and never was imagined when the law was written. And while the Second Circuit's interpretation of current law was, in Microsoft's view, correct, the clear need remains for Congress now to move the law forward.

This is a proposition that finds unanimous support. On January 24, 2017, the Second Circuit denied the government's request to re-hear the case en banc. Four judges dissented from that decision. Yet every judge who considered the case agreed on one thing: ECPA should be updated to reflect the extraordinary technological changes that have occurred since 1986. As the judge who authored the court's decision explained, the statute "has been left behind by technology" and is "overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose."[11]

III. Outdated laws do not serve law enforcement, technology users, or the tech industry.

Today's outdated law serves no one. In its reliance on unilateral demands, it risks leading to the balkanization of the Internet, which will increasingly deprive law enforcement of information it needs to investigate crimes and to keep the country safe. It harms technology users in the United States and around the world, including American citizens who are put at risk

---

[9] *Id.*

[10] *Id.*

[11] *See In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, No. 14-2985, Dkt. 328 (2d Cir. Jan. 24, 2017) (Carney, J., concurring in denial of rehearing en banc).

of reciprocal incursions by foreign governments that may compromise the privacy of their digital information, and who are given little clarity about the legal protections afforded to the sensitive information they entrust to technology providers. And it harms U.S. technology companies, which all too often are left in the impossible position of choosing between two conflicting laws—one that requires the company to produce information in response to a unilateral demand, and one that forbids it from doing so. These problems are a direct result of the outdated framework that governs cross-border law enforcement access to data.

A. Outdated laws do not serve law enforcement.

Law enforcement has an important need for digital evidence to keep our country safe. Microsoft supports this important principle. And we recognize that there are times when law enforcement needs information about individuals abroad who have committed crimes in the United States or harmed U.S. persons. But law enforcement is ill-served by today's outdated laws, which encourage unilateralism across borders. Unilateral law enforcement access creates incentives for other countries to engage in digital protectionism, hoarding data within their borders, balkanizing the internet, and reducing cooperation through treaty-based frameworks.

Microsoft's case in the Second Circuit provides a concrete illustration of the challenges to international relations caused by unilateral demands. In response to the U.S. Government's position that a U.S. warrant unilaterally should reach customer emails stored in Ireland, the European Commission stated that "personal data held by private companies in the EU should not, in principle, be directly accessed by or transferred to foreign enforcement authorities outside of formal channels of cooperation, such as … Mutual Legal Assistance Treaties."[12] In addition, Europe's "Article 29 Working Party"—composed of all 28 Member State Data Protection Authorities—issued a joint statement that, "[a]s a rule, a public authority in a non-EU country should not have unrestricted direct access to the data of individuals processed under EU jurisdiction," so "[f]oreign requests must not be served directly to companies under EU jurisdiction."[13] Companies faced with such a definitive prohibitions comply with unilateral demands at their peril.

Foreign governments are not only reacting to specific cases in which unilateral demands are issued. They are also enacting laws that systematically resist unilateral demands on the national level. One of the clearest illustrations of this phenomenon is the European Union's General Data Protection Regulation ("GDPR"), which will apply to organizations inside and outside of Europe when it comes into effect in May of next year.

---

[12] *See* European Parliament, Parliamentary Questions, No. E-010602-14 (Mar. 4, 2015), *available at* http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-010602&language=EN.

[13] *See* Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, at 3 (Nov. 26, 2014) (emphasis omitted), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2014/wp227_en.pdf.

(continued…)

Under the GDPR, orders for disclosure issued by non-EU courts or authorities are not "recognizable" or "enforceable" in the EU unless domesticated through an MLAT or other international framework.[14] Though European data protection authorities have not yet issued clear and definitive guidance on this point, the GDPR on its face makes compliance with a unilateral U.S. search warrant unlawful. In so doing, the European Union has codified an approach similar to the one long taken by the United States in ECPA, which prohibits the disclosure of customer content in response to legal process from other countries.

As a result, U.S. law enforcement will be significantly restricted in its ability to obtain digital information covered by the GDPR unless it issues demands through international processes, instead of using unilateral, U.S.-based warrants. The significant fines available under the GDPR underscore the risk to U.S. companies if they were to comply with unilateral U.S. warrants covered by the GDPR. Among other penalties, EU Member State privacy regulators can levy penalties of up to 4 percent of a company's annual worldwide revenue for violations of the GDPR.

Continued use of unilateral demands also undermines efforts to develop international frameworks that govern cross-border data access. By using a U.S. warrant to seek digital information overseas, law enforcement effectively sidesteps the host of international agreements that already govern how it may access evidence located abroad. Those agreements are critical to ensuring that governments can and will cooperate in international investigations, which are increasingly common in our globally-connected society. Over the long term, the short-circuiting of these agreements risks undermining the international collaboration that is a cornerstone for the protection of public safety.

Finally, unilateral demands risk placing digital information beyond the reach of U.S. law enforcement altogether. Countries that fear U.S. unilateral law enforcement action will seek to protect their citizens and their local service providers by localizing cloud services and data storage—to the disadvantage of U.S. providers *and* U.S. law enforcement. If U.S. providers are required to comply with U.S. warrants in all circumstances, even for digital information of a foreign citizen that is stored in that foreign citizen's home country, foreign technology competitors will be able to argue persuasively that storing digital information with a U.S. company will grant unfettered access to U.S. law enforcement. Not only would this trend undermine customer trust and threaten the U.S. technology sector's position as a leader in important global markets, it would also put digital information beyond the reach of U.S. law enforcement.

B. Outdated laws harm technology users.

Outdated laws also harm the millions of individuals and businesses that today rely on technology providers to store their most sensitive personal information. The chaotic legal environment created by unilateralism puts U.S. customers at risk by encouraging other governments to circumvent U.S. laws safeguarding the privacy of their digital information. It also creates uncertainty about which laws will govern access to the users' digital information,

[14] *See* Article 48 of the General Data Protection Regulation (Regulation 2016/679).

leaving individuals and businesses to wonder what laws govern the data they store in the cloud and whether their privacy will be adequately protected.

If the United States claims an unlimited power to issue extraterritorial warrants and reach across borders, it will invite foreign governments to do the same—thereby undermining U.S. laws that protect the digital information of U.S. persons. For example, the United States would have no principled argument to stop another government from simply going to a local office of a global technology company and demanding personal, confidential, or proprietary information of a U.S. customer from a U.S. server. Those actions would undercut U.S. laws—including ECPA—designed to protect U.S. citizens' rights to own, control, and protect their own private papers. U.S. citizens and companies would be outraged at the notion that foreign governments could unilaterally obtain access to their confidential and privileged business documents merely because they are stored with a cloud provider that operates internationally. But it is this very conduct that unilateralism invites—weakening the protection of our borders and undermining the rule of law.

Unilateralism leaves technology users uncertain of which laws will safeguard the private information they entrust to global technology providers. Just as our customers in the U.S. expect their data to be protected by U.S. law, our users in other parts of the world reasonably expect their information to be protected by the laws of their own countries. But when one country claims the authority to demand any and all information from cloud providers, without regard for the laws of other countries, our customers are left to question whether their privacy will be adequately protected. When U.S. law enforcement simply ignores the data protection and privacy laws of other countries, foreign customers' trust in global cloud providers, and technology more broadly, is undermined.

C. Outdated laws adversely affect U.S. businesses.

Our outdated laws also put technology companies in the untenable position of choosing between conflicting legal obligations. As global companies, U.S.-based technology providers like Microsoft must respect the laws of all countries in which we do business. But when a country unilaterally claims the power to access digital evidence extraterritorially, it puts technology companies in the impossible position of choosing between two conflicting laws. Complying with a unilateral request of one country can violate the law of another. As noted above, these conflicts will sometimes result in U.S. law enforcement being unable to obtain information they seek through unilateral process when technology companies determine that a conflict bars them from complying with one country's legal demand because of another country's data privacy restriction.

For example, Brazilian courts have repeatedly asserted authority to compel U.S. technology companies to disclose the contents of users' communications to Brazilian law enforcement, even when the communications are located in other countries. The Brazilian government in 2014 enacted new legislation that reaffirms this point.[15] When Microsoft has

[15] *See* Article 10(3) of the Marco Civil Da Internet (a law enacted on April 23, 2014), which in certain cases empowers administrative authorities (including public prosecutors and police) to (continued…)

refused to comply with such orders—because they conflict with U.S. laws—government authorities in Brazil levied fines against Microsoft's local subsidiary – more than $5 million since January 2016 – and in one case even arrested and criminally charged a local employee.[16] Another U.S. company, WhatsApp, reportedly had its services temporarily suspended in Brazil in 2015, also for refusing to comply with an order from a Brazilian judge to disclose user data that allegedly could have caused WhatsApp to violate ECPA.[17]

Unfortunately, such scenarios are proliferating. In October 2016, to take another example, a Belgian court issued a decision against Skype Communications SARL, a Microsoft subsidiary. Belgian authorities had demanded that Skype implement a wiretap. In addition to technical limitations on Skype's ability to comply with such an order, the company argued that doing so would have needed to be set up on Skype's infrastructure *located in Luxembourg*—where such wiretaps would have been prohibited except where authorized by Luxembourg law.[18] In other words, even if Skype had been capable of complying, it would have been forced to choose between complying with the Belgian wiretap order—which required it to implement the wiretap—and Luxembourg law, which effectively forbids it from complying. Skype is now appealing the Belgian court's decision, but this is another illustration of the patchwork of conflicting laws that are emerging internationally.

These conflicts force technology companies into the role of policymakers—requiring them to choose which law to comply with and which to violate. This is a recipe for chaos and uncertainty. Companies caught between two countries' laws are likely to react in a variety of ways based on a wide range of considerations. For example, companies may consider in each case the size of relevant markets, the potential severity of penalties for non-compliance, and other fact-specific concerns. This undermines the predictability and clarity of legal protections, and harms customers, who reasonably expect certainty about which laws will protect their digital information. This uncertainty also hurts law enforcement, which deserves to know how companies will respond to legal demands in order to obtain the information they need to fight crime. And, ultimately, it is undemocratic. Elected policymakers, not technology companies, should strike the proper balance between safety, privacy, and digital sovereignty.

---

order service providers to disclose personal data without a judicial warrant, and without any limitation based on potential conflicts of law with countries other than Brazil.

[16] *See* Brad Smith, *In the Cloud We Trust*, Microsoft Story Labs, *available at* https://news.microsoft.com/stories/inthecloudwetrust.

[17] *See WhatsApp in Brazil back in action after suspension* BBC News, July 20, 2016, *available at* http://www.bbc.com/news/world-latin-america-36836674.

[18] *See Skype Luxembourg condemned in Belgium for refusing to set up wiretap*, Stibbe, February 24, 2017, *available at* https://www.stibbe.com/en/news/2017/february/skype-luxembourg-condemned-in-belgium-for-refusing-to-set-up-wiretap.

IV. A new framework is needed to govern international data access.

We recognize that litigation is not a substitute for policymaking. That is why Microsoft believes Congress should make the decisions about how to update ECPA to account for cross-border data requests—not judges or prosecutors, and not technology companies. Indeed, our Second Circuit litigation focuses only on the narrow question of how *today's* outdated law applies to modern technology. It does not address the much broader—and more significant—question of what the law should be *in the future*. Congress is the appropriate body to answer that question, which requires policy judgments reserved to the legislative branch.

Merely enacting a law that says the U.S. government can use warrants for every person's emails—even if those emails are stored overseas—is not the answer. Such a simplistic "quick fix" response to the Second Circuit's decision, premised on unilateralism, would not resolve the complicated issues that arise from cross-border requests and would leave us with the same problems that exist under today's law. Like today's outdated framework, a simplistic "quick fix" approach would harm law enforcement by placing ever more data outside its reach, harm U.S. citizens by encouraging reciprocal actions by foreign governments, and leave technology companies in the impossible position of choosing which laws to comply with and which to violate. This approach would effectively double-down on our outdated unilateral legal framework—without recognizing the realities of the global cloud economy. We must design laws to account for today's modern technology, not to ignore it.

Rather than revert to legal rules stuck in the past, we need legislation that reflects the current and future ways people and businesses use technology. At the same time, it's important to be sensitive to the needs of law enforcement to address the ways criminals, too, have evolved in their use of technology. We would suggest Congress consider legislation that advances at least three important goals.

First, Congress should create a modern, streamlined international legal framework that permits the gathering of digital evidence in appropriate circumstances across international borders. As Internet-based communications become more ubiquitous, digital evidence has become increasingly important to the investigation and prosecution of suspected criminals. Principled efforts to seek legal guidance from our courts have, at times, been misconstrued as being born of a desire to impede law enforcement. Just like other members of the public, Microsoft and its customers rely on law enforcement to keep us and our online services safe. This is not something we take for granted, but rather something we greatly value. Our position on these issues has been focused on ensuring that law enforcement follows the right process, and to drive a constructive discourse about charting a better course for the future.

This framework should not be a one-way street. As noted earlier in my testimony, ECPA prohibits the disclosure of the contents of communications to foreign governments, even in response to valid legal orders seeking information belonging to their own citizens. With an overburdened MLAT process as the only mechanism for these governments to obtain this information, frustration has begun to boil over and is causing other governments to resort to unilateralism themselves. Recognizing their legitimate investigative interests, there should be a mechanism for countries with strong privacy and human rights protections to obtain evidence

directly in investigations of serious criminal activity, freeing up the MLAT process to handle other requests that cannot be made directly to cloud providers.

Second, this modern legal framework should ensure that there are clear and robust legal protections for the privacy of the sensitive digital information customers entrust to their cloud providers. Confidence in the legal protections afforded to our most sensitive information is essential to preserving trust in modern technology, and has two components— strong legal protections under domestic laws, and respect for other countries' laws protecting the privacy of their citizens' information.

When it comes to domestic legal protections, the warrant-for-content rule remains the gold standard. It is critical to ensuring that digital documents and communications receive the same legal protections that their precursors did before the advent of modern Internet-based technology. Though other countries may accomplish this with slightly different rules, the concepts of a high standard of proof and a mechanism for independent oversight and authorization are areas where the United States should maintain its leadership.

At the same time, governments should respect the legitimate interests that other countries have in protecting the privacy rights of their own citizens. Just as U.S. citizens reasonably expect that U.S. legal protections will apply to their email and other private online information, citizens of other countries reasonably expect that their home countries' laws will protect their data. Our laws should recognize this expectation, both here and abroad. And this is not simply due to the respect that is rightly owed to the sovereign interests of other nations that seek to protect the privacy of their own citizens. It is also because we know that whatever rules we establish for U.S. law enforcement access are likely to be replicated by other countries. Ultimately, unrestrained unilateralism will undermine our ability to protect the privacy of U.S. citizens.

Third, this modern legal framework should avoid imposing conflicting legal obligations on cloud providers. By adopting an approach that provides for strong legal protections for sensitive data and respects the laws and interests of other countries, the United States can lead by example. When other countries that adhere to the rule of law, respect human rights, and protect individual privacy follow suit, the current patchwork will evolve into a more sensible, modern international legal framework that eliminates conflicts of laws governing access to digital evidence.

We appreciate that advancing all of these goals simultaneously may appear to be a tall task at first glance. However, based on our recent experience wrestling with these issues, we and our peers in the U.S. technology sector are increasingly optimistic that there is a sensible path forward.

Domestic legislation will necessarily continue to provide both the authority for governments to request information from online providers, as well as the privacy protections for sensitive data stored in the cloud. To fully accomplish the goals outlined above, ***domestic legislation should be coupled with international agreements***. The proposed bilateral agreement between the United States and the United Kingdom is a promising development, providing a sensible alternative to unilateral extraterritoriality. By bolstering domestic law with

complementary international agreements, there is an opportunity to enhance individual privacy, ensure respect for other countries' laws, eliminate conflicting legal obligations across jurisdictions, and promote trust in modern technology.

The most promising approach takes appropriate account of the nationality and location of the user. Though not the only relevant factors, nationality and location of the user should play an important role in whatever rules of thes road are established. Respect for other countries' legitimate interests in protecting the privacy of their citizens will lead to a more durable and comprehensive framework internationally, and will ultimately inure to the benefit of the U.S. when it comes to protecting the privacy of its own citizens.

Finally, this legal framework should provide reciprocal rights and protections to governments that have demonstrated their respect for the rule of law, have enacted strong privacy protections for digital information, and have a track record of respecting human rights. Rather than rely on an outdated and overburdened MLAT process, a comprehensive framework should be designed to ensure that law enforcement can obtain the information it requires to combat 21st-century crime at 21st-century speeds.

Congress has already taken steps to address this important issue. Last year, legislation was introduced by Senators Hatch and Coons and Representatives Marino and DelBene to create a more durable legal framework for cross-border access issues. That legislation, the International Communications Privacy Act ("ICPA"), would allow warrants issued under ECPA to reach outside the United States in certain circumstances, based on the nationality and the location of the account holder whose digital information is sought.[19] The legislation also included important privacy safeguards, such as a requirement that law enforcement use a warrant to obtain any email content, regardless of its age. We believe ICPA is a solid foundation for a legislative framework and understand the bill's sponsors are in the process of reintroducing the bill after receiving input from a range of stakeholders. While the specifics of a framework will evolve through the legislative process, the need for a framework is urgent, and we would encourage Congress to act.

Microsoft and other technology companies support Congress enacting a modern legal framework for international data requests.

I am not here today to say that I have all the answers to the many questions raised when law enforcement from one country legitimately needs to access digital information stored in another. However, Microsoft and others in the technology industry support Congress enacting a modern legal framework to govern international data requests. We look forward to continuing to work with Members on a comprehensive solution, building on the work done in the last session.

---

[19] ICPA has enjoyed broad support among the technology industry. Last July, nearly a dozen industry associations representing companies such as Facebook, Google, and Yahoo sent a letter to Senate and House leaders calling on Congress to pass the legislation as soon as possible. *See* July 14, 2016 Letter Re: International Communications Privacy Act (ICPA), S. 2986/H.R. 5323, to Charles E. Grassley, Patrick J. Leahy, Robert W. Goodlatte, John Conyers, *available at* http://actonline.org/wp-content/uploads/ICPA-Multi-Assn-Letter_071416.pdf.

And we call upon the Administration to work with Congress to develop a framework that addresses the needs of all stakeholders.

Congress now has an opportunity to modernize the outdated laws governing cross-border access to digital information. We need a new framework that accounts for law enforcement's needs, the realities of today's technology, and the manner in which people and businesses rely on that technology—now and into the future. I know I speak for many U.S. companies when I say that I hope this Subcommittee and Congress will act on this opportunity. I welcome the occasion to discuss how technology companies can assist in these efforts.