Department of Justice

STATEMENT OF

RICHARD W. DOWNING
ACTING DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

FOR A HEARING ENTITLED

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

PRESENTED

JUNE 15, 2017

Statement of
Richard W. Downing
Acting Deputy Assistant Attorney General
Department of Justice

Before the
Committee on the Judiciary
U.S. House of Representatives

At a Hearing Entitled
"Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era"

June 15, 2017

Good afternoon Chairman Goodlatte, Ranking Member Conyers, and distinguished Members of the Committee, and thank you for the opportunity to testify on behalf of the Department of Justice. Americans' safety and privacy is under attack by criminals who use the Internet to communicate and conspire, to commit serious criminal offenses, and to hide evidence. The need for effective, efficient, and lawful access to data in criminal investigations is paramount in the digital age. Obstacles to obtaining such electronic evidence jeopardize investigations into every category of criminal activity – including terrorism, financial fraud, drug trafficking, child sexual exploitation, human trafficking, and computer hacking.

A recent case from the Second Circuit has effectively hamstrung the ability of law enforcement to obtain data from U.S. communications service providers who store data outside the United States. This is a tremendous problem that is becoming more acute by the day. In my testimony today, I will outline the substantial harms to public safety that the Second Circuit's decision in *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016) has created.

The United States is not alone in facing obstacles to obtaining electronic evidence outside its territory by providers serving millions of its residents. Countries around the world rely on data held by U.S. communications service providers to protect their legitimate public safety interests. However, the Stored Communications Act may preclude U.S. service providers from disclosing U.S.-stored data to foreign countries pursuant to lawful foreign orders. In these instances, the foreign authority would likely use the formal mutual legal assistance process to obtain the data. Yet the Second Circuit's decision has hindered our ability to obtain content data from U.S. providers on behalf of our foreign partners, just as it has in U.S. investigations.

We welcome Congress's attention to this important problem that endangers our public safety and national security. We appreciate the complexities of this issue, and hope to work with you, industry, and the relevant stakeholders to find the best solution. What we must avoid, however, are proposed solutions that do not provide investigators with effective and timely

access to digital evidence or cede control over U.S. investigations to foreign governments. Any solution must also address the serious challenges that our allies have in gaining access to data stored in the United States for their criminal investigations, while also seeking to protect legitimate privacy interests. Additionally, several prominent U.S. companies have expressed that conflicts of law that arise from foreign orders for disclosure of content data is a serious problem that can present an obstacle to their ability to compete for business abroad, and we believe it is important to address these concerns in any legal regime that is developed.

Therefore, on May 24, 2017, the Department, on behalf of the Administration, transmitted a legislative proposal to Congress to build a new framework for effective, efficient cross-border access to data that protects both legitimate privacy interests and our public safety and national security, and benefits U.S. business interests as well. That proposal can be found in Appendix A. In my testimony today, I will discuss the legislative foundation for this new international framework which begins with legislation to fix the problems created by the *Microsoft* decision.

I. Obstacles to Access of Electronic Evidence Across Borders

A. The *Microsoft* decision and U.S. access to foreign-stored data

For over thirty years, U.S. courts have issued warrants under the Stored Communications Act ("SCA", 18 U.S.C. §§ 2701, *et seq.*) that require U.S. providers (such as Google and Microsoft) to disclose emails and other electronic information in their custody to U.S. authorities to be searched for evidence of crime. In July 2016, the Court of Appeals for the Second Circuit for the first time held that Congress did not intend the SCA to require providers to disclose information in their custody that is stored on computers outside the United States. *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016). Therefore the government was unable to compel Microsoft to produce data it had stored in Ireland, even though the magistrate judge had found probable cause to believe that evidence of a crime would be found. In January 2017, the Second Circuit (in a rare 4-4 split decision in which all four dissenting judges wrote separately) decided not to rehear the case *en banc*. However, all opinions filed, including those of judges who voted against rehearing, emphasized that the result was unsatisfactory and that Congress should address the issue. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft*, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017).

The Second Circuit's decision, as Judge Gerard Lynch wrote in his concurrence to the panel decision, should not "be regarded as a rational policy outcome." On the contrary, as four judges observed in dissenting from the denial of rehearing *en banc*, it "has substantially burdened the government's legitimate law enforcement efforts, created a roadmap for the facilitation of criminal activity, and impeded programs to protect the national security of the United States and its allies." *Microsoft*, 2017 WL 362765, at *2-3 (Cabranes, J., *dissenting*). The decision also does not enhance privacy. It involved a warrant that met all of the

constitutional and statutory protections built into U.S. law. Indeed, requiring foreign legal process to access the data—as the court's opinion suggests is required—would not enhance privacy protections for U.S. persons. Foreign legal standards are no more demanding—and often are less demanding—than U.S. standards.

Although the *Microsoft* decision is binding only in the Second Circuit, Microsoft and a number of other providers are applying the decision on a nationwide basis, and refusing to turn over data stored on their servers abroad in response to SCA warrants. The decision has already prevented the U.S. government from obtaining data necessary for criminal investigations across the United States and for our foreign partners pursuant to mutual legal assistance requests. The Department urges Congress to re-examine this issue and pass legislation that clarifies that compliance with SCA warrants requires providers to disclose data in their custody and control, wherever it is located.

The Department has responded by filing a series of motions in districts outside of the Second Circuit seeking to enforce court orders requiring the disclosure of data without regard to where a provider chooses to move it. Other judges examining the Second Circuit's ruling have concluded that its reasoning is flawed and creates results that Congress could not have intended. In all of the cases decided thus far, the government has prevailed.

- On February 3, 2017, the Department received its first ruling in this series of challenges—a decision rejecting the Second Circuit's position from Magistrate Judge Rueter of the Eastern District of Pennsylvania. Judge Rueter declined to follow the *Microsoft* ruling, noting that the decision would entirely foreclose the government from obtaining foreign stored data from Google—a result that Congress could not have intended. *See In re Search Warrant No. 16-960-M-01 to Google,* No. 16-1061-M, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017).

- On February 21, 2017, Magistrate Judge Duffin of the Eastern District of Wisconsin authorized warrants under the SCA for one Yahoo and two Google accounts. In authorizing the warrants, Judge Duffin issued a public opinion stating that when a "service provider is subject to the jurisdiction of the court, the court may lawfully order that service provider to disclose, consistent with the SCA, that which it can access and deliver within the United States" and that it "is immaterial where the service provider chooses to store its customer's data; what matters is the location of service provider." *In re: Information associated with one Yahoo email address that is stored at premises controlled by Yahoo and In re: Two email accounts stored at Google, Inc.*, 2017 WL 706307 (E.D.Wisc. Feb. 21, 2017).

- On April 7, 2017, Magistrate Judge Smith of the Middle District of Florida similarly issued an order authorizing the issuance of a warrant under the SCA for information associated with a Yahoo account. Judge Smith held that the Second Circuit ruling was

wrongly decided, reasoning that, "[b]ecause the focus of § 2703 [of the SCA] is on compelled disclosure, and the compulsion takes place in the United States, I find the application of § 2703 in this case is not extraterritorial." *In the matter of the search of premises located at: [redacted]@yahoo.com, stored at premises owned, maintained, controlled, or operated by Yahoo, Inc.*, Case No. 6:17-mj-1238 (M.D. Fla. Apr. 7, 2017).

- On April 19, 2017, Magistrate Judge Beeler of the Northern District of California also declined to follow the Second Circuit, instead agreeing with the four judges who dissented from the denial of rehearing *en banc* that the disclosure of information from a company's United States headquarters is a domestic application of the SCA. Judge Beeler reasoned, "[e]ven if the SCA's focus is privacy, the warrant requirement – with its attendant requirement of probable cause – protects privacy. Moreover, an SCA warrant is not a search warrant in the classic sense: the government does not search a location or seize evidence. Instead, the conduct relevant to the focus – and what the SCA seeks to regulate – is disclosure of the data in the service provider's possession." *In the matter of the search of content that is stored at premises controlled by Google*, Case No. 16-mc-80263 (N.D. Cal. Apr. 19, 2017).

- On June 2, 2017, Magistrate Judge G. Michael Harvey of the District of the District of Columbia issued an order holding that the Government can, pursuant to a SCA warrant, require Google to produce information within its possession, custody, or control regardless of whether such data is stored within the territorial boundaries of the United States. The court reasoned that because the SCA requires providers to disclose information in response to a valid warrant, and that disclosure occurs in the United States, such disclosure is a domestic application of the statute regardless of from where a provider must retrieve the information. The court noted that application of the Second Circuit's decision to Google "would effectively leave law enforcement with no means of obtaining data stored on Google's foreign-based servers," which would "not only obstruct the efforts of law enforcement in the United States, but also the efforts of foreign investigative bodies seeking evidence on Google's servers outside the United States to advance their own investigations." *In re Search of Information Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc.*, Case No. 16-mj-757 (GMH) (D.D.C. June 2, 2017)

As every judge outside the Second Circuit to write an opinion on the issue has recognized, the principal flaw in the *Microsoft* decision is the court's finding that requiring Microsoft to gather data from its servers abroad would constitute an extraterritorial application of the SCA. Because the required disclosure of data in the *Microsoft* case would occur in the United States, the enforcement of the warrant is, in fact, a *domestic* application of the SCA. The government applied for the warrant in the United States, the magistrate judge issued it in the United States, and it was served on Microsoft in the United States. Moreover, the data sought in

the warrant is readily accessible to Microsoft's domestic employees using a computer in the United States and, once produced, would be reviewed by the FBI in the United States.

Although the government has prevailed in all of the more recent cases in lower courts, the providers continue to adhere to the Second Circuit's ruling and have appealed other decisions. In the meantime, the providers are still withholding access to data that they have chosen to store overseas that law enforcement needs for criminal investigations across the country.

In litigation with the Department, Google has acknowledged that data on its network is in near-constant transit and is moved between servers and across borders automatically. Google has also conceded that data associated with a single Google account is frequently stored across numerous servers in different countries. In a recent case, Google responded to a Department-issued SCA warrant by providing email messages stripped of many attachments, explaining that while the bodies of the emails were stored domestically, the attachments were stored abroad. The Department's inability to compel Google – as well as any other provider that structures its network similarly to Google's – to produce the full content of user accounts is a sea change that continues to harm countless law enforcement investigations.

The Department is aware of dozens of investigations, across the country, in every judicial circuit, in which the impact of the *Microsoft* decision has frustrated those investigations and risked thwarting the pursuit of justice.

- In a drug trafficking investigation involving targets in the United States, Canada, and China, a search warrant issued to and served on Microsoft returned no email content, and Microsoft indicated that it had stored the content overseas. Investigators need the content to identify suppliers and customers.

- In the investigation of a person in the U.S. suspected of sex trafficking by force, fraud and coercion, the defendant was arrested and his phone searched pursuant to a warrant, which revealed photos and videos depicting beatings of trafficked women. A warrant was issued to and served on Google for the content of the defendant's account, and Google withheld the content of photo and video albums in the information returned. The defendant ultimately pleaded guilty, but the withheld Google content would have been vital had the defendant successfully moved to suppress the evidence obtained during the phone search. Despite the fact that there is probable cause to believe that relevant evidence is in the custody of a U.S.-based service provider, Google, the true extent of the evidence of criminal acts contained in the defendant's Google account is unknown.

- In a child exploitation case, a U.S. defendant was arrested and a search warrant was issued to Google for the content of the defendant's account. Google withheld

image attachments in the information returned. The investigators need the photos to identify and locate child victims.

- In an investigation involving a foreign national located in the U.S. who was unlawfully accessing a Federal Government database using stolen identities, investigators obtained a search warrant for several Microsoft email accounts believed to contain stolen means of identification and information used to commit Federal tax refund fraud. Microsoft withheld some responsive content, and informed investigators that the missing content was stored overseas. Based on data obtained from other service providers, investigators believe the missing Microsoft data would provide additional evidence of criminal activity and assist with identifying other co-conspirators in the scheme.

- In another child exploitation investigation, the court issued and investigators served a warrant to Google, and Google withheld images stored in the suspect's Google Drive. Investigators need the withheld images to test the veracity of the suspect's statement that he did not possess any child pornography images of the minor child with whom he had been living. The target is in the U.S.

- In the investigation of a fugitive wanted for cutting off his electronic monitoring device and absconding before trial in a child pornography case, investigators issued a search warrant to Google for email and other content that could prove helpful in locating the fugitive. Google withheld all content, and stated in a cover letter that it had stored the fugitive's content outside the United States. The fugitive remains at large.

- In yet another child exploitation investigation, a search warrant issued to Google resulted in returned information that included several images and videos of child sexual exploitation. The target was indicted and arrested based on this information, and consented to a search of his email account. That search revealed a trove of additional images of child exploitation that had not been turned over by Google, including images of infant rape.

This is merely a sampling of the many investigations frustrated by the effect of the *Microsoft* decision. The impacted investigations run the gamut – from child exploitation and human trafficking, to firearms and drug smuggling, to tax fraud, computer fraud, and identity theft. These cases directly affect public safety and may even affect national security. While the most obvious impact of the *Microsoft* decision may be to frustrate investigations of foreign nationals targeting U.S. victims, these examples make clear that the *Microsoft* decision also thwarts or delays investigations *even where the victim, the offender, and the account holder are all within the United States.*

Some have looked at the international mutual legal assistance ("MLA") process as an alternative means for the government to obtain the overseas data it seeks. Pursuant to the MLA process, U.S. investigators can ask foreign authorities to gather evidence in their home countries and supply it to us. However, the United States maintains bilateral MLA treaties with less than one-half of the world's countries. Moreover, even when a treaty is in place, the MLA process can lack the requisite efficiency for time-sensitive investigations and other emergencies, making it an impractical alternative to SCA warrants in many cases. Among other hurdles, some domestic providers—including Google—permit only their U.S.-based personnel to access user data in response to law enforcement requests. This renders MLA requests futile because foreign authorities have no ability to obtain the evidence on our behalf. As I will discuss in more detail, other countries do not restrict their own ability to demand data stored outside their borders, and in fact the *Microsoft* decision takes us outside established international norms in this respect.

B. Access by foreign governments to U.S.-located data

The United States is not alone in confronting serious challenges to gathering the electronic evidence necessary to enforce essential laws in an increasingly international and digital age. Foreign governments investigating criminal activity taking place within their borders are increasingly concerned about their ability to obtain access to electronic evidence from U.S. companies that provide electronic communications services to millions of their citizens and residents. In fact, the Committee supporting the Budapest Cybercrime Convention is considering whether an additional Protocol to that Convention is necessary to address these issues. Often this data is stored or accessible only in the United States, where U.S. law, including the SCA, limits the companies' ability to disclose it.

The MLA process has frequently been the only mechanism that can provide foreign countries with access to this data, though its structure was not devised to handle the growing demands for digital evidence. Already, the Department faces significant challenges in responding to the enormous volume of foreign demands with the requisite speed. Moreover, the MLA process has been further frustrated by the *Microsoft* decision which impedes the ability of our foreign partners to obtain evidence needed to protect their law enforcement and national security interests. For example, in response to an MLA request from a foreign authority, the U.S. has no way to issue orders to U.S. providers to obtain data that they control but may be stored abroad. Our foreign law enforcement partners are increasingly frustrated that U.S. providers often cannot be compelled by the United States to produce data they seek for important criminal investigations and prosecutions, especially when the providers cannot even tell them where the data they require is stored.

This situation is one of several concerns that encourages countries to adopt data localization policies, which place a significant burden on American providers and disadvantage U.S. law enforcement. Moreover, the United States is not the only country that has recognized the legitimate need to compel providers subject to its jurisdiction to provide evidence from

abroad in investigations of serious crime. Even before the *Microsoft* decision, foreign countries across the globe have passed their own domestic laws to compel providers with customers in their territory—including U.S. companies—to disclose data. In the absence of a *Microsoft* fix, the pressure foreign countries face to implement and utilize such laws will only increase.

This dynamic presents challenges. Our companies may face conflicting legal obligations when foreign governments require them to disclose electronic data in the United States that U.S. law prohibits them from disclosing. This legal conflict can occur even if the request is made pursuant to lawful process in the foreign country, involves communications between foreign nationals abroad, and concerns criminal activities outside the United States with no relation to this country other than the fact that the service provider stores the data in the United States. In addition to harming our allies' efforts to investigate terrorism and other serious crimes, this can put our companies in a difficult position. They must either comply with a foreign order, and risk a violation of U.S. law, or refuse to comply and risk violating a foreign law.

The experience of the United Kingdom illustrates why this scenario can be so problematic. A significant portion of the electronic communications service providers used by the U.K. public are based in, and store their data in, the United States (or elsewhere outside the United Kingdom). As a result, U.K. authorities must frequently come to the United States to access data located here, even if it is relevant to the investigation of conduct taking place entirely outside of the United States and is not related to any U.S. persons. If the data happens to be stored in the United States, U.S. law would control the manner in which that data is available to U.K. authorities, even if only British citizens are involved, the threat is directly to the United Kingdom, and the conduct is taking place entirely outside the United States. U.K. investigators may find their investigations delayed by the cumbersome MLA process even despite the U.S. Government's best efforts to process requests expeditiously. Or, it may be thwarted altogether by the *Microsoft* decision.

The effects of such conflicts are felt acutely by many of our foreign law enforcement partners. They also present unique challenges for U.S. providers who wish to compete for overseas customers, but store data in the United States. Our foreign partners and many U.S. communications providers continue to voice concern that the status quo is unsustainable. It undermines efforts by our foreign partners to protect their citizens, just as it would for U.S. authorities to protect Americans. It gives other countries strong incentives to require data localization. And it exposes U.S. providers to potential enforcement actions and fines by foreign countries for adhering to U.S. law. The *Microsoft* decision compounds all of these harms.

II. The Path Forward

The current situation presents significant challenges. As all of the judges involved in the Second Circuit decision indicated, Congress should address the ongoing and substantial damage to public safety caused by the *Microsoft* decision, and it should act swiftly. However, the

Department has significant concerns about some efforts that have been contemplated to address the problem. The issue is complex, and solutions must take into consideration the possible ramifications and consequences. I will discuss some of these concerns in my remaining testimony. Then, I will describe our work on a solution to collectively address both the urgent need of U.S. investigators to access data outside the United States *and* that of foreign countries to access data held by U.S. providers.

A. Principles that Should Govern a Solution

When crafting a solution to the problems created by the Second Circuit's *Microsoft* decision, we believe Congress should be guided by several principles. In the Department's view, some previous legislative proposals attempting to address this solution have not fully addressed these concerns:

- First, a solution must permit law enforcement investigators effectively to obtain digital evidence without undue delay. Waiting months for evidence critical to solving fast-moving investigations – such as terrorism, computer intrusion, and child sexual exploitation cases, just to name a few – is dangerous and harmful to the safety and security of Americans.

- Second, reliance solely on the MLA process cannot be the solution. Even with our closest partners, lengthy delays occur. For example, Ireland—where Microsoft has indicated it stores its European customers' data—has reported that the average response times for routine requests are 15-18 *months*. And we do not have MLA treaties with many countries. The MLA process nonetheless remains a vital tool, and we look forward to continuing to work with you to improve its efficiency and effectiveness.

- Third, a solution cannot grant foreign governments a veto authority over U.S. criminal investigations. It makes no sense to allow China or Russia, for example, the authority to prevent U.S. officers from obtaining data pursuant to SCA warrants in relation to violations of U.S. criminal law committed by their nationals and/or persons located in their jurisdictions.

- Fourth, a solution must take into account the reality that investigators often will not know the identity, nationality, or location of the account holder. Suspects commonly use the anonymity provided by internet tools to conceal themselves and their locations. The use of warrants under the SCA is often aimed at uncovering these critical facts.

- Fifth, a solution should avoid creating an incentive for other countries to create "data localization" laws. Such laws are burdensome on U.S. providers, limit access to

evidence needed to assure public safety, and have been called out by the U.S. Trade Representative as a key barrier to trade. (For example, see the March 2017 Fact Sheet by the Office of the U.S. Trade Representative ("USTR") available online at: https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade.)

- Sixth, a solution should not grant benefits or protections to foreigners that are not also granted to U.S. citizens and residents. We believe that some proposals that have been advanced would afford protections to non-U.S. citizens and residents that exceed those afforded to U.S. citizens and residents.

The Department believes that these principles can guide a legislative solution that protects public safety and national security, allows U.S. industry to compete globally, and provides a clear set of rules to guide access to data by both domestic law enforcement and our international partners.

B. Proposed Solutions

Some countries, like the United States, may have privacy laws that prevent disclosure of electronic data in response to foreign legal process. Conflicts of law in this area are traditionally avoided through mechanisms such as prosecutorial discretion, court supervision, diplomacy, and economic considerations. Strictly limiting the reach of U.S. law to avoid potential conflicts with foreign laws would thus not be consistent with international practice; to the contrary, it would make the United States an outlier by unilaterally hobbling our own public safety functions, including in scenarios where no conflict is presented.

Accordingly, Congress should consider targeted amendments to the SCA that will provide for the legitimate needs of law enforcement agencies in the United States to obtain, through lawful process, electronic communications stored abroad that are relevant to U.S. criminal investigations, as well as address foreign countries' legitimate public safety needs. At the same time, it should reduce the chance that providers will be caught in conflicting obligations between U.S. and foreign laws.

To address the first issue, we recommend a simple legislative fix to make clear that SCA warrants can be used to obtain data under a provider's custody or control, even if it is stored abroad. To address the needs of foreign countries and providers facing a conflict of laws, we recommend a new bilateral data-sharing framework that would protect both American and foreign citizens' privacy interests.

Legislative solution to the Microsoft decision

As the *Microsoft* decision fundamentally rests on statutory interpretation, Congress can correct it through a clarifying amendment to the statute. The Department has proposed a simple

legislative amendment, a new proposed section 2713 of Title 18, that would make clear that SCA warrants can be used to obtain data under a provider's custody or control, even if it is located abroad. This amendment can be found in Appendix A. For years, providers routinely complied with SCA warrants, even for data that was stored outside the United States. The amendment would restore that practice by explicitly requiring providers subject to the jurisdiction of the United States to produce data pursuant to appropriate SCA process, even if the provider chooses to store that data outside the United States. In this manner, the amendment would ensure that SCA warrants remain subject to the traditional rules for compulsory process, under which "[t]he test for the production of documents is control, not location." *In re Grand Jury Subpoena Directed to Marc Rich & Co., A.G.*, 707 F.2d 663, 667 (2d Cir. 1983), *cert. denied*, 463 U.S. 1215 (1983). This amendment would affirm the domestic application of the SCA and clarify that responding to lawful process for data under a provider's custody or control does not constitute an extraterritorial application of the SCA.

Arguments against legislative solutions

Many, including providers like Microsoft, have argued that the use of SCA warrants to compel disclosure of data under a provider's custody or control, regardless of location, would place providers in an untenable position because of conflicting laws in other jurisdictions, but that concern is overstated for several reasons. First, in many cases, where the foreign country's law does not prohibit the production of data stored in its territory, American providers would not face any conflict of law if required to produce data stored outside the United States to American law enforcement authorities pursuant to SCA process. In the years prior to the *Microsoft* decision, the Department is not aware of any instance in which a provider has informed the Department or a court that production pursuant to the SCA of data stored outside the United States would place the provider in conflict with local law.

Second, in the event there were a true conflict of laws, the Department would have the discretion whether to make a request, and to narrow or modify the request in a manner that avoids the conflict. The Department often confronts such situations in its cross-border investigations, particularly those involving records held by large financial institutions, and has typically been able to resolve them through closer inquiry or good-faith negotiation. Thus, ensuring the ability to compel production of foreign stored data does not imply that such authority will be used in a manner that creates conflict with other countries; in practice, the power is exercised with great restraint and such conflicts are exceedingly rare.

And third, even in the small number of cases in which a resolution is not reached, neither the longstanding interpretation of the SCA nor our proposal would give the Department unilateral authority to compel production in the face of a conflict of laws. Rather, when considering whether to enforce compulsory process for information located outside the United States "where such production would violate the law of the state in which the documents are located," courts apply a multi-factor balancing test based on the Restatement of the Foreign

Relations Law of the United States. *United States v. Davis*, 767 F.2d 1025, 1033 (2d Cir. 1985). Under that test, courts balance factors such as "the vital national interests of each of the states", "the extent and the nature of the hardship that inconsistent enforcement actions would impose", "the extent to which the required conduct is to take place in the territory of the other state", "the nationality of the person", and "the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state." *Id.* at 1034. Those principles would continue to apply to SCA warrants, and would ensure appropriate respect for international comity without unnecessarily harming American public safety. By contrast, significantly impairing U.S. authorities' ability to obtain data stored outside the United States creates substantial harms even in cases where there is no colorable conflict of laws.

Nor would reinstating the *status quo* compromise international practice. As noted above, in many, if not most cases, enforcement of SCA process for data stored outside the United States would not create any conflict between American and foreign law, and would thus not implicate comity concerns in the first instance. But even if such a conflict may exist, the Executive Branch is well-suited to weigh international comity concerns and discern when to assert American interests, as it routinely does in cross-border contexts other than the SCA, such as subpoenas to financial institutions and other multi-national enterprises where foreign laws may restrict disclosure. Indeed, the Department has a rigorous internal review and approval process for requests by prosecutors to compel foreign companies subject to United States jurisdiction to produce records located outside the United States. *See* U.S. Attorneys' Manual 9-13.525; Criminal Resource Manual 279. This process takes into account such factors as the timely availability of alternative methods for obtaining the records, the indispensability of the records to the success of the investigation or prosecution, and the need to protect against the destruction of records located abroad.

In this manner, American law is similar to that of other countries around the world that assert authority to compel the production of data stored outside their territory, but that—like the U.S.—take a more calibrated approach when that authority may result in a conflict of laws. Thus, concerns that reinstating the status quo will result in a "Wild West" scenario are overstated. Countries including Australia, Belgium, Brazil, Canada, Colombia, Denmark, France, Ireland, Mexico, Montenegro, Norway, Peru, Portugal, Serbia, Spain, the United Kingdom, and others already assert the authority to compel production of data stored abroad under their own laws. *See, e.g.*, Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, 2-3 (Hogan Lovells) (Updated 18 July 2012) ("Notably, every single country that we examined vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders, provided there is some jurisdictional hook, such as the presence of a business within the country's borders."). Indeed, the 50 countries around the world – including the United States -- that have joined the Budapest Convention have agreed that national laws should contain the authority for legal process to compel providers in their territory that have possession and control

over digital evidence to disclose it, even when the provider chooses to store that data outside of the country. In the face of this widespread practice, restricting the United States' ability to obtain data stored abroad would amount to a unilateral limitation with considerable disadvantage and no benefit to the American people.

Bilateral frameworks for cross-border data sharing

Addressing the significant public safety consequences of the *Microsoft* decision is an urgent priority. But we must also do more to meet the legitimate public safety needs of other countries that require access to evidence that happens to be stored or accessible in the United States, without compromising users' legitimate privacy interests. And we must recognize that U.S. service providers seeking to compete in a global marketplace may, in some instances, face conflicting legal obligations from the many nations in which they choose to do business, and minimize those conflicts where possible. Finding solutions that satisfy both the American people and our allies may be difficult, but we are committed to improving current processes.

In particular, we recommend enacting and implementing legislation for a framework under which U.S. providers could disclose data directly to a foreign government for serious criminal investigations when that government is targeting accounts of non-U.S. persons outside the United States, provided that the United States has concluded that the foreign country's laws adequately protect privacy and civil liberties. The framework would require that the foreign government obtain authorization to access the data under its own legal system, which must include review or oversight by an independent authority, require sufficient cause and meet other legal requirements.

It would not permit bulk data collection and would not permit foreign-government targeting of any U.S. persons or persons known to be located in the United States. Moreover, it would not impose any new obligations on providers at all under U.S. law; instead, any requirement to comply with the foreign order would derive solely from the requesting country's law.

The framework would, in turn, permit reciprocal access for U.S. law enforcement to data stored abroad free of any legal barriers that foreign law might otherwise erect, provided that Congress first restores such authority. This access will become increasingly important for data located beyond U.S. borders and subject to foreign law. Under this approach, the United States and a foreign government can negotiate a bilateral agreement setting forth the terms for cross-border access to data, but only with those countries who share the United States' commitment to the rule of law and respect for privacy and civil liberties. These agreements would also be subject to audit and periodic renewal to ensure that they are being properly implemented.

The United States has for some time been working on a proposed agreement of this sort with the United Kingdom, which has made clear that its inability to access data from U.S.

providers in an efficient and effective way poses a very serious threat to public safety and national security in the United Kingdom. The United Kingdom has indicated that this framework is of utmost importance, which is underscored by the appearance and testimony of Paddy McGuinness at this hearing today. If the approach proves successful, we would consider it for other appropriate countries as well.

This approach would require amendments to U.S. law, the Wiretap Act, the Stored Communications Act, and the Pen Register Statute. The amendments would lift the statutory prohibition on disclosure of communications data for lawful requests from a foreign partner with which the United States has a satisfactory executive agreement.

To succeed, any framework must establish adequate baselines for protecting privacy and civil liberties, both through the agreement and implementing legislation. For example, legislation should require the foreign country's law to have in place appropriate substantive and procedural protections for privacy and civil liberties; it should require robust targeting and minimization procedures to prevent the targeting of, and ensure the protection of, U.S. person data; and it should require appropriate safeguards concerning the use of the data that is disclosed. In this way, the framework would ensure that there are sufficient protections for privacy and civil liberties, while permitting countries to maintain appropriate checks and balances for doing so within their existing legal framework. The framework would not require our foreign partners to adhere to standards that mirror the American legal system. However, we expect that one of the benefits of creating such a framework would be to encourage other interested countries to improve their legal protections for communications data to a higher level in order to be eligible for a similar arrangement. Thus, privacy standards abroad could be significantly enhanced.

There are a number of additional benefits to such a framework. Importantly, it would support our partners' ability to investigate serious crime, including terrorism and other transnational crimes—threats that may, in turn, also affect Americans at home and abroad. It is expected to decrease the existing burden on the MLA process. It would reduce the impetus for foreign countries to implement data localization policies, which would be harmful to U.S. commercial interests and public safety and national security, while encouraging them to develop stronger privacy protections. If Congress acts to address the Second Circuit's *Microsoft* decision, the new international framework would also help to secure reciprocal access for the United States to data abroad in an efficient, effective, and privacy-respecting manner. And it would help obviate a potential obstacle to U.S. communications service providers' ability to compete for global business by reducing the risk that providers face from potential international conflicts of laws.

* * *

The two-part legislative proposal that the Department has transmitted to Congress and that I have discussed here today represents an opportunity for Congress to meet the urgent public safety needs of the United States while furthering legitimate access to data for our foreign law enforcement partners, removing conflicts of laws faced by providers, relieving pressure on data localization, and incentivizing new protections for privacy and civil liberties around the world. The Department appreciates the opportunity to further discuss these complex issues with you, and we look forward to continuing to work with you, industry, and other relevant stakeholders. This concludes my remarks. I would be pleased to answer your questions.

APPENDIX A

U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D. C. 20530

May 24, 2017

The Honorable Paul Ryan
Speaker
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Speaker:

On behalf of the Administration, the Department of Justice is pleased to present for the consideration of the Congress a legislative proposal that would (1) provide for the legitimate needs of law enforcement agencies in the United States to obtain, through lawful process, electronic communications stored abroad that are relevant to U.S. criminal investigations; and (2) help resolve potential conflicting legal obligations that U.S. electronic communications service providers ("service providers") may face when required to disclose electronic data by foreign governments investigating serious crime, including terrorism.

The need for effective, efficient, and lawful access to electronic data in criminal investigations is paramount in the digital age. Obstacles to obtaining such electronic evidence jeopardize investigations into every category of criminal activity. A recent court decision has effectively hamstrung the ability of U.S. law enforcement to obtain data stored by U.S. communications service providers outside the United States. In July 2016, the United States Court of Appeals for the Second Circuit held in *Microsoft Corp. v. United States* that section 2703 of the Electronic Communications Privacy Act ("ECPA") does not authorize our courts to issue and enforce warrants served on U.S. providers to obtain electronic communications stored abroad. If this decision stands, or is extended to other parts of the country, the United States would not have, under section 2703, access to data necessary to advance important U.S. investigations that protect the safety of Americans. The Congress can address the ongoing and substantial damage to public safety caused by the *Microsoft* decision, and it should act swiftly. This legislative proposal is necessary to reinstate the pre-*Microsoft* status quo, when providers routinely complied with section 2703 warrants for data within their custody or control, even when stored outside the United States.

The legislative proposal is also necessary to implement a potential bilateral agreement between the United Kingdom and the United States that would permit U.S. companies to provide electronic data in response to U.K. orders targeting non-U.S.

persons located outside the United States, while affording the United States reciprocal rights regarding electronic data of companies storing data in the United Kingdom.

Foreign governments investigating criminal activities abroad increasingly require access to electronic evidence from U.S. companies that provide electronic communications services to millions of their citizens and residents. Often, such data is stored or accessible only in the United States, where U.S. law, including ECPA, limits the companies' ability to disclose it. Our companies may face conflicting legal obligations when foreign governments require them to disclose electronic data that U.S. law prohibits them from disclosing. This legal conflict can occur even though the request is made pursuant to lawful process in the foreign country, involves communications between foreign nationals abroad, and concerns criminal activities outside the United States with no relationship to this country other than the fact that the service provider stores the data in the United States.

In addition to harming our allies' efforts to investigate terrorism and other serious crimes, this puts our companies in a difficult position. Either they comply with a foreign order, and risk a violation of U.S. law, or they refuse to comply and risk violating foreign law.

The Mutual Legal Assistance Treaty ("MLAT") process, which is an important but often labor-intensive mechanism for facilitating law enforcement cooperation, must contend with the challenges posed by significant increases in the volume and complexity of requests for assistance made to the United States in the Internet age. It typically takes months to process such requests, and foreign governments often struggle to understand and comply with U.S. legal standards for obtaining data, particularly content, for use in their investigations and prosecutions. As the number of requests for electronic data continues to grow as a result of the Internet's globalization of personal communications, governments with legitimate investigative needs face increasingly serious challenges in gaining efficient and effective access to such data. Reforming the MLAT process must remain a priority, but, at the same time, it is critical to find even more streamlined solutions for data held by and transmitted via service providers.

The current situation is unsustainable. Some countries have begun to take enforcement actions against U.S. companies, imposing fines or even arresting company employees. If foreign governments cannot access data they need for legitimate law enforcement, including terrorism investigations, they also may enact laws requiring companies to store data in their territory. Such "data localization" requirements would only exacerbate conflicts of law, make Internet-enabled communications services less efficient, threaten important commercial interests, undermine privacy protections by requiring data storage in jurisdictions with laws less protective than ours, and ultimately impede U.S. Government access to data for its investigations. And, as the global market for Internet-related services expands, the U.S. Government increasingly will need effective and efficient access to electronic information stored or uniquely accessible abroad. Conflicts of law increasingly may pose an obstacle to such access.

The potential bilateral agreement with the United Kingdom and the Administration's legislative proposal not only would resolve legal conflicts for communications service providers located in the United Kingdom and the United States, and promote and protect the global free flow of information, but would establish a framework and standards that could be used to reach similar agreements with other countries whose laws provide robust protection of human rights, privacy, and other fundamental freedoms. It could thereby increase protections for privacy and civil liberties globally, as countries seeking to qualify for such agreements would need to demonstrate that their legal systems met these requirements.

The legislative proposal achieves these priorities by requiring the Attorney General, with the concurrence of the Secretary of State, to determine and certify to the Congress that foreign partners have met obligations and commitments designed to protect privacy and civil liberties. Orders issued by the foreign government must be subject to review or oversight by a court, judge, magistrate, or other independent authority. Significantly, foreign orders covered by this legislation and the agreements it would authorize would not be permitted to target U.S. persons wherever they were located, or persons located in the United States. Procedures and oversight would be required to ensure that this rule was followed. Moreover, the Administration would be required to notify the Congress prior to making the required determinations.

However, in order for the United States to receive reciprocal benefits from such agreements, U.S. law must authorize law enforcement to obtain electronic data located abroad. This requires reinstating the pre-*Microsoft* status quo discussed above, during which providers routinely complied with section 2703 warrants for data within their custody or control, even when stored outside the United States. It does not make sense to enter into agreements if U.S. law enforcement investigators cannot access or do not have authority to access data stored in the U.K. or any other foreign jurisdiction covered by such an agreement.

In sum, the proposed legislation would provide numerous benefits to the United States, including (1) removing barriers and conflicts for U.S. businesses; (2) protecting U.S. interests and citizens, and enhancing public safety; (3) ensuring reciprocal access to data for U.S. investigations; (4) reducing data localization incentives; (5) reducing the mutual legal assistance burden on U.S. government resources; and (6) encouraging improvement of global privacy and civil liberties protections. We urge the Congress to work with the Administration to pass legislation that would allow the United States to enter into and implement bilateral agreements that would achieve these important objectives.

Thank you for the opportunity to present this proposal. The Office of Management and Budget has advised us that enactment of this legislation would be in accord with the Program of the President.

Sincerely,

Samuel R. Ramer
Acting Assistant Attorney General

Enclosures

IDENTICAL LETTER SENT TO THE HONORABLE MICHAEL R. PENCE, PRESIDENT, UNITED STATES SENATE; THE HONORABLE CHARLES E. GRASSLEY, CHAIRMAN, COMMITTEE ON THE JUDICIARY, UNITED STATES SENATE; THE HONORABLE DIANNE FEINSTEIN, RANKING MEMBER, COMMITTEE ON THE JUDICIARY, UNITED STATES SENATE; THE HONORABLE ROBERT W. GOODLATTE, CHAIRMAN, COMMITTEE ON THE JUDICIARY, U.S. HOUSE OF REPRESENTATIVES; AND THE HONORABLE JOHN CONYERS, JR., RANKING MEMBER, COMMITTEE ON THE JUDICIARY, U.S. HOUSE OF REPRESENTATIVES.

Legislation to Permit Secure and Privacy-Protective Access to Cross-border Electronic Data for Law Enforcement to Combat Serious Crime Including Terrorism

Section 1: Short Title.

This Act may be cited as the "___."

Section 2: Congressional Findings and Purpose

The Congress finds the following:

(1) Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism.

(2) Such efforts by the United States government are being impeded by the inability to access the content of data stored outside the United States that is in the custody, control, or possession of communications service providers that are subject to U.S. jurisdiction.

(3) Foreign governments also increasingly seek access to electronic data held by communications-service providers in the United States for the purpose of combatting serious crime.

(4) Communications-service providers face potential conflicting legal obligations when a foreign government orders production of electronic data that United States law may prohibit providers from disclosing.

(5) Foreign law may create similarly conflicting legal obligations when the United States government orders production of electronic data that foreign law prohibits communications-service providers from disclosing.

(6) International agreements provide a mechanism for resolving these potential conflicting legal obligations where the United States and the relevant foreign government share a common commitment to the rule of law and the protection of privacy and civil liberties.

(7) The purpose of this Act is to –

(a) clarify that U.S. law authorizes law enforcement to obtain electronic data under a provider's custody or control, even if the data is stored abroad;

(b) provide authority to implement international agreements to resolve potential conflicting legal obligations arising from cross-border requests for the production of electronic data where the foreign government targets non-U.S. persons outside the United States in connection with the prevention, detection, investigation, or prosecution of serious crime; and

(c) ensure reciprocal benefits to the United States of such international agreements.

Section 3: Amendments to Current Communications Laws.

(a) Chapter 121 of Title 18, United States Code, is amended by adding a new subsection 2713 as follows:

"A provider of wire or electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside the United States."

(b) Chapter 119 of Title 18, United States Code, is amended by adding:

(1) A new subsection 2511(2)(j) as follows:

"It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX.";

and

(2) Replacing subsection 2520(d)(3) as follows:

"a good faith determination that section 2511(3), 2511(2)(i), or 2511(2)(j) of this title permitted the conduct complained of;"

(c) Chapter 121 of Title 18, United States Code, is amended by adding:

(1) A new subsection 2702(b)(9) as follows:

"to a foreign government pursuant to an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX.";

(2) A new subsection 2702(c)(7) as follows:

"to a foreign government pursuant to an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX.";

and

(3) Replacing subsection 2707(e)(3) as follows:

"a good faith determination that section 2511(3), section 2702(b)(9), or section 2702(c)(7) of this title permitted the conduct complained of;"

(d) Chapter 206 of Title 18, United States Code, is amended by:

(1) Adding to the end of subsection 3121(a) as follows;

"or an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX.";

(2) Replacing subsection 3124(d) as follows:

"**No cause of action against a provider disclosing information under this chapter.**—No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter, request pursuant to section 3125 of this title, or an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX."

and

(3) Replacing subsection 3124(e) as follows:

"**Defense.**—A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, a statutory authorization, or a good faith determination that the conduct complained of was permitted by an order from a foreign government as defined in and subject to an agreement that the Attorney General has determined and certified to Congress satisfies 18 U.S.C. § XXXX, is a complete defense against any civil or criminal action brought under this chapter or any other law."

Section 4: Executive Agreements on Access to Data by Foreign Governments. Chapter ___ of Title 18, United States Code, is amended by adding a new section XXXX as follows:

"(a) An executive agreement governing access by a foreign government to data subject to Chapters 119, 121, and 206 of this Title shall satisfy this section if the Attorney General, with the concurrence of the Secretary of State, determines and certifies to Congress that:

(1) The domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement, provided that such a determination under this section take into account, as appropriate, credible information and expert input, and that the factors to be considered in making such a determination include whether the foreign government:

(i) has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated through accession to the Budapest Convention on Cybercrime, or through domestic laws that are consistent with definitions and the requirements set forth in Chapters I and II of that Convention;

(ii) demonstrates respect for the rule of law and principles of non-discrimination;

(iii) adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights (including but not limited to protection from arbitrary and unlawful interference with privacy; fair trial rights; freedoms of expression, association and peaceful assembly; prohibitions on arbitrary arrest and

detention; and prohibitions against torture and cruel, inhuman, or degrading treatment or punishment);

(iv) has clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective of oversight of these activities;

(v) has sufficient mechanisms to provide accountability and appropriate transparency regarding the government's collection and use of electronic data; and

(vi) demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet.

(2) The foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement; and

(3) The agreement requires the following with respect to orders subject to the agreement:

(i) The foreign government may not intentionally target a United States person or a person located in the United States, and must adopt targeting procedures designed to meet this requirement;

(ii) The foreign government may not target a non–United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States;

(iii) The foreign government may not issue an order at the requests of or to obtain information to provide to the United States government or a third-party government, nor shall the foreign government be required to share any information produced with the United States government or a third-party government;

(iv) Orders issued by the foreign government must be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

(v) Orders issued by the foreign government must identify a specific person, account, address, or personal device, or any other specific identifier as the object of the Order;

(vi) Orders issued by the foreign government must be in compliance with the domestic law of that country, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law;

(vii) Orders issued by the foreign government must be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;

(viii) Orders issued by the foreign government must be subject to review or oversight by a court, judge, magistrate, or other independent authority;

(ix) Orders issued by the foreign government for the interception of wire or electronic communications, and any extensions thereof, must be for a fixed, limited duration; interception may last no longer than is reasonably necessary to accomplish the approved purposes of the order; and orders may only be issued where that same information could not reasonably be obtained by another less intrusive method.

(x) Orders issued by the foreign government may not be used to infringe freedom of speech;

(xi) The foreign government must promptly review all material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those trained in applicable procedures;

(xii) The foreign government must segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious

crime, including terrorism, or necessary to protect against a threat of death or seriously bodily harm to any person;

(xiii) The foreign government may not disseminate the content of a communication of a U.S. person to U.S. authorities unless the communication (a) may be disseminated pursuant to Section 4(a)(3)(xii) and (b) relates to significant harm, or the threat thereof, to the United States or U.S. persons, including but not limited to crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud.

(xiv) The foreign government must afford reciprocal rights of data access, to include, where applicable, removing restrictions on communications service providers and thereby allow them to respond when the United States government orders production of electronic data that foreign law would otherwise prohibit communications-service providers from disclosing;

(xv) The foreign government must agree to periodic review of its compliance with the terms of the agreement by the United States government; and

(xvi) The United States government must reserve the right to render the agreement inapplicable as to any order for which it concludes the agreement may not properly be invoked.

(b) A determination or certification made by the Attorney General under subsection (a) shall not be subject to judicial or administrative review.

(c) The Attorney General shall provide notice to the Judiciary Committees of the Senate and the House, and the Foreign Relations Committee of the Senate, and the Foreign Affairs Committee of the House 60 days prior to making a determination under subsection (a) of his intent to do so. Any determination or certification under subsection (a) regarding an executive agreement under this section and any termination of such an agreement, shall be published in the Federal Register as soon as is reasonably practicable.

(d) The Attorney General, with the concurrence of the Secretary of State, shall renew a determination under subsection (a) every five years. In the absence of such a renewal, the agreement will no longer satisfy this section.

(e) As used in this section, "United States person" means a citizen or national of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence; or a corporation that is incorporated in the United States."

Section 5: Rule of Construction.

Nothing in this Act shall be construed to preclude any foreign authority from obtaining assistance in a criminal investigation or prosecution pursuant to Section 3512 of Title 18, United States Code, Section 1782 of Title 28, United States Code, or as otherwise provided by law.

Section-by-Section Analysis of Legislation to Permit Secure and Privacy-Protective Access to Cross-border Electronic Data for Law Enforcement to Combat Serious Crime Including Terrorism

The need for effective, efficient, and lawful access to electronic data in criminal investigations is paramount in the digital age. Obstacles to obtaining such electronic evidence jeopardize investigations into every category of criminal activity. A recent decision of the United States Court of Appeals for the Second Circuit, *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016), has effectively hamstrung the ability of U.S. law enforcement to obtain data stored by U.S. communications service providers outside the United States. The United States is not alone in seeking to obtain electronic evidence stored outside its territory. Countries around the world rely on data held by U.S. communications service providers to protect their legitimate law enforcement and public safety interests. However, U.S. electronic communications service providers face potentially conflicting legal obligations when a foreign government serves them with legal process requiring the production of electronic data that U.S. law may prohibit them from acquiring or disclosing. The proposed legislation seeks targeted amendments to Title III of the Omnibus Crime Control and Safe Streets Act (the Wiretap Act), the Stored Communications Act ("SCA"), and Chapter 206 of Title 18 (the Pen/Trap Statute) to (1) provide for the legitimate needs of law enforcement agencies in the United States to obtain, through lawful process, electronic communications stored abroad that are relevant to U.S. criminal investigations; and (2) reduce the chance that providers will be caught in conflicting obligations between U.S. and foreign laws by allowing service providers to intercept, access, and disclose communications content and metadata in response to an order from a foreign government, if that order falls within the scope of an executive agreement that the Attorney General, with the concurrence of the Secretary of State, has determined, and certified to Congress, meets several statutory conditions. Among those conditions is the requirement that the foreign order not target any U.S. person or any person located in the United States. In addition, the Attorney General must certify that the law of the foreign government provides robust protections for privacy and civil liberties. The legislation also provides a complete bar to civil and criminal liability for violations of the statutes if the providers acted in good faith reliance on such foreign orders, in parallel to existing provisions of law establishing such liability protection for good faith reliance on U.S. orders. The proposed legislation also ensures that U.S. law enforcement will be able to obtain reciprocal benefits of such executive agreements by clarifying that U.S. law authorizes law enforcement to obtain electronic data located abroad.

Section 2 sets forth congressional findings and the purpose of the proposed legislation — in particular, to clarify that U.S. law authorizes law enforcement to obtain electronic data under a provider's custody or control, even if the data is stored abroad, and to provide authority to implement executive agreements that resolve potential conflicting legal obligations arising from cross-border requests for the production of electronic data where a foreign government targets non-U.S. persons outside the United States in connection with the prevention, detection, investigation, or prosecution of serious crime, if that foreign government and the United States share a common commitment to the rule of law and the protection of privacy and civil liberties.

Subsection 3(a) amends the Stored Communications Act by clarifying that U.S. communications providers' obligations to preserve, backup, or disclose the contents of data extend to all data within the providers' possession, custody, or control, even if such data is located outside the United States. This provision clarifies that U.S. law authorizes U.S. law enforcement to obtain electronic data under a provider's custody or control, even if the data is stored abroad, which ensures timely access to electronic data in criminal investigations for U.S. law enforcement when that data is held by a U.S. provider, and also ensures that U.S. law enforcement can gain the reciprocal benefits of executive agreements authorized under Section 4.

Subsection 3(b)(1) amends the Wiretap Act by adding an additional exception to the general prohibition on accessing real-time wire or electronic communications. The exception permits interception and disclosure to respond to a foreign order made pursuant to an executive agreement that the Attorney General has determined and certified to Congress satisfies a separate statutory provision (section 4). Subsection 3(b)(2) amends the Wiretap Act to establish that good faith reliance on such an order is a complete defense against any civil or criminal action.

Subsections 3(c)(1) and (2) similarly add additional exceptions to the SCA's general prohibition on accessing and disclosing stored communications and customer data (18 U.S.C. §§ 2702(b) and 2702(c), respectively) to respond to a foreign order pursuant to an executive agreement that meets the requirements of section 4. Subsection 3(c)(3) similarly amends the SCA to establish that good faith reliance on such an order is a complete defense against any civil or criminal action.

Subsection 3(d)(1) amends the Pen/Trap Statute to permit the installation of a pen register or a trap-and-trace device to respond to a foreign order pursuant to an executive agreement that meets the requirements of section 4. Subsections

3(d)(2) and 3(d)(3) amend the Pen/Trap Statute to bar criminal and civil causes of actions under the Pen/Trap Statute that stem from good-faith compliance with such a foreign order.

Section 4 creates a new section in Title 18 setting forth requirements for executive agreements such that foreign government orders covered by them would fall within the exceptions laid out in section 3. Subsection 4(a) establishes that an executive agreement will satisfy the statutory requirements of the new section if three conditions are met.

First, per subsection 4(a)(1), and taking into account, as appropriate, credible information and expert input, the Attorney General, with the concurrence of the Secretary of State, must determine and certify to Congress that the foreign government's domestic law, in light of the data collection and activities subject to the executive agreement, affords robust substantive and procedural protections for privacy and civil liberties, including by

(i) having adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated through accession to the Budapest Convention on Cybercrime, or through domestic laws that are consistent with definitions and the requirements set forth in Chapters I and II of that Convention;

(ii) demonstrating respect for the rule of law and principles of non-discrimination;

(iii) adhering to applicable international human rights obligations and commitments or demonstrating respect for international universal human rights (including but not limited to protection from arbitrary and unlawful interference with privacy; fair trial rights; freedoms of expression, association and peaceful assembly; prohibitions on arbitrary arrest and detention; and prohibitions against torture and cruel, inhuman, or degrading treatment or punishment);

(iv) including clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective of oversight of these activities;

(v) having sufficient mechanisms to provide accountability and appropriate transparency regarding the government's collection and use of electronic data; and

(vi) demonstrating a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet.

Second, per subsection 4(a)(2), the Attorney General, with the concurrence of the Secretary of State, must determine and certify to Congress that the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of any information concerning U.S. persons obtained through the executive agreement. Specific procedures will be agreed upon and adopted as part of each executive agreement.

Third, per subsection 4(a)(3), the Attorney General, with the concurrence of the Secretary of State, must determine and certify to Congress that, with respect to orders issued pursuant to the executive agreement, the executive agreement requires that

(i) the foreign government may not intentionally target a U.S. person or person located in the United States, and must adopt targeting procedures to ensure such targeting does not occur;

(ii) the foreign government may not target a non-U.S. person located outside the United States if the purpose is to obtain information concerning a U.S. person or a person located in the United States;

(iii) the foreign government may not issue an order at the request of or to obtain information to provide to the United States government or a third-party government, and the foreign government cannot be required to share information with the United States government or a third-party government;

(iv) the foreign government orders must be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

(v) foreign government orders must target a specific person, account, address, or personal device or any other specific identifier (*i.e.*, may not engage in bulk collection);

(vi) foreign government orders must be issued in compliance with the foreign country's domestic law, and any obligation for a provider to produce data derives solely from that foreign government's law;

(vii) foreign government orders must be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;

(viii) foreign government orders must be subject to review or oversight by a court, judge, magistrate, or other independent authority;

(ix) foreign government orders for the interception of wire or electronic communications, and any extensions thereof, must be for a fixed, limited duration; interception may last no longer than is reasonably necessary to accomplish the approved purposes of the order; and orders may only be issued where that same information could not reasonably be obtained by another less intrusive method;

(x) foreign government orders may not be used to infringe freedom of speech;

(xi) the foreign government must promptly review all material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those trained in applicable procedures;

(xii) the foreign government must segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or seriously bodily harm to any person;

(xiii) the foreign government may not disseminate the content of a communication of a U.S. person to U.S. authorities unless the communication (a) may be disseminated pursuant to Section 4(a)(3)(xii) and (b) relates to significant harm, or the threat thereof, to the United States or U.S. persons, including but not limited to crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud.

(xiv) the foreign government must afford reciprocal rights of data access to the United States government;

(xv) the foreign government must agree to periodic review of its compliance with the terms of the executive agreement by the U.S. government; and

(xvi) the U.S. government must reserve the right to render the executive agreement inapplicable as to any order for which it concludes the executive agreement may not properly be invoked.

Subsection 4(b) provides that a determination or certification made by the Attorney General under subsection 4(a) shall not be subject to judicial or administrative review.

Subsection 4(c) requires the Attorney General to give 60 days' notice to the Senate and House judiciary and foreign affairs committees prior to making a subsection 4(a) determination or certification. The Attorney General must also publish any such determination or any termination of an executive agreement satisfying section 4 in the Federal Register as soon as is reasonably practicable.

Subsection 4(d) requires that the Attorney General, with the concurrence of the Secretary of State, renew a country's determination of eligibility for an executive agreement satisfying section 4 every five years. Absent such a renewal, the executive agreement will no longer satisfy Section 4.

Subsection 4(e) provides a definition of "United States person" for use in the new Title 18 section.

Section 5 establishes that nothing in the legislation precludes any foreign government from obtaining assistance in a criminal investigation or prosecution through other previously existing processes, such as mutual legal assistance requests.