AMERICAN UNIVERSITY
WASHINGTON, DC

Statement of
Jennifer Daskal

Associate Professor
American University Washington College of Law

Committee on the Judiciary
Subcommittee on Crime and Terrorism
United States Senate

Hearing on Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights

May 24, 2017

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

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

Committee on the Judiciary
Subcommittee on Crime and Terrorism
United States Senate

Hearing on Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights

May 24, 2017

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

Almost a year ago, the Second Circuit issued its decision in what is known as the *Microsoft Ireland* case, upending longstanding practice, and ruling that search warrants issued under the Electronic Communications Privacy Act (ECPA) only reach data that is physically held within the territory of the United States.[1] It is a decision that is concerning on almost every relevant axis. It impedes the ability of U.S. law enforcement to lawfully access data in the investigation of criminal activity, threatens to undercut privacy in both the short-term and long-term, and makes little practical or normative sense. Just about everyone who has looked at the case—including the judge who wrote the opinion—has urged Congress to amend the statute and better protect the key interests at stake.[2]

Meanwhile, other provisions of ECPA are imposing hard-to-justify barriers on foreign governments' ability to access communications content, such as emails, critical to their own investigations of local crime—also with negative consequences for security, privacy, and the economy.

These results stem from a mismatch between old law and new technology. They rest on an outmoded assumption that law enforcement's jurisdiction over data is and should be tied to the location of sought-after data at a given moment in time—even though the location of the data may have no relevant connection to the crime or targets under investigation and is instead the result of service providers' business decisions based on things like efficiency and speed of delivery, tax rates, and energy costs. Complicating

[1] *In re* Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).
[2] *In re* Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 855 F.3d 53, 55 (2d Cir. 2017)(Carney, J., concurring in denial of rehearing en banc, yet emphasizing that ECPA "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").

matters, the location of sought-after data may not be known; it may be constantly shifting; and it may be distributed over multiple different locations.[3] An update to the law is critically needed to better match our laws with modern technology, to protect law enforcement's ability to engage in legitimate investigations, and to safeguard our security, our privacy, and our economy.

I am deeply encouraged by this Committee's commitment to these issues and decision to hold this hearing today. In what follows, I describe the problems in much more detail and suggest solutions.

Issue #1: Clarifying the Reach of U.S. Warrant Authority – A *Microsoft Ireland* Fix.

In the ten months since the Second Circuit issued its decision in the *Microsoft Ireland* case, the problems with the ruling have become increasingly apparent. U.S. law enforcement is being told by a range of U.S.-based providers, such as Google, Microsoft, and Yahoo, that sought-after data is located outside the territorial boundaries of the United States and thus cannot be turned over. The U.S. government can no longer access that data even with a warrant issued by a neutral magistrate based on a finding of probable cause that the data is evidence of a crime. This is so even if the FBI is investigating a local crime involving U.S. citizen victims, perpetrators, and witnesses. No matter how serious the crime.

Instead, the U.S. government must make a diplomatic request for the data directed at the country where the data is located. But sometimes the U.S. government does not know where the data is located, and thus has no way to know where to direct the request. Google, for example, will tell the U.S. government whether data is located within or outside the United States, but will not specify *where* outside the United States certain data is located. Sometimes the government knows, but there is no workable mutual assistance process in place and thus no mechanism for the United States to access sought-after data. Sometimes there is a mutual legal assistance treaty in place, but the process is so slow that it still takes a year or more for the data to be ultimately accessed and turned over.

Just about everyone, including the judge who wrote the Second Circuit opinion, agrees that this is an unsatisfactory state of affairs and that Congress should weigh in. And now at least four magistrate judges—from the Northern District of California,[4] Eastern District of Pennsylvania,[5] Eastern District of Wisconsin,[6] and Middle District of Florida[7]—have rejected the Second Circuit's approach and concluded that the warrant

[3] For a further discussion of these issues, *see* Jennifer Daskal, *The Un-Territoriality of Data,* 125 YALE L.J. 326, 365-377 (2016).
[4] *See In re* Search of Content that is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, 2017 WL 1487625 (N.D. Cal. Apr. 25 2017).
[5] *See In re* Search Warrant No. 16-960-M-01 to Google, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017).
[6] *See In re* Information associated with one Yahoo Email Address that is stored at premises controlled by Yahoo, No. 17-M-1234, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017).
[7] *See In re* Search of Premises Located at [Redacted]@yahoo.com, 6:17-mj-1236 (M.D. Fla. Apr. 7, 2017).

authority under ECPA reaches all data controlled by U.S.-based providers, regardless of the data's physical location. But in at least some cases the providers are appealing, leaving law enforcement unable to access the sought-after data as the cases proceed. And while an eventual circuit split seems likely, leading to possible Supreme Court review, years of litigation and uncertainty may pass before that happens.

Meanwhile, the claimed privacy benefits that result from the ruling are not only overstated, but also in many cases illusory. As a result of the ruling, the government is, instead of accessing sought-after data pursuant to a warrant based on probable cause, told that it must seek the data from a foreign government, according to the foreign governments' standards and procedures. But foreign government standards and procedures are generally *less* protective of privacy than that imposed by the warrant requirement. Hence, it may yield a *reduction* in applicable privacy protections. In fact, the one way that the ruling is good for privacy is in the way it generally makes it harder for the government to access sought-after data. But this is so even in those situations where the government is investigating a serious and ongoing crime and has demonstrated to an independent judge a legitimate basis for accessing it. This is a "privacy benefit" that is hard to defend.

Conversely, however, a legal framework that says U.S. law enforcement could access any and all data held by a U.S.-based provider, without consideration of any countervailing factors, raises its own set of concerns. Two in particular deserve Congress's attention. First, it fails to take into account the sometimes legitimate foreign government interest in controlling access to its residents' and citizens' data. This is something that the United States should respect—in no small part because the United States presumably wants foreign governments to do the same when accessing U.S. citizen and resident data. Second, by ignoring the importance of perceptions, it puts U.S. business interests at risk. Rightly or wrongly, foreign customers of U.S. tech companies are increasingly concerned about what they perceive as broad surveillance by the U.S. government; our companies need to be able to assure their customers that their interests are being taken into account.

So what should Congress do?

Congress should act, as numerous judges and others have urged. It should do so in a way that ensures legitimate law enforcement access to sought-after communications content, pursuant to a warrant based on probable cause, regardless of where the data happens to be located at any given point in time. And it should do so in a way that also takes into account foreign governments' legitimate interests in safeguarding their own residents' and citizens' data.

Here are three possible ways to do so, and better protect our security, privacy, and economic interests in the process:

(i) Required Comity Analysis

When there is a conflict between what U.S. law and applicable foreign law requires in a given case courts will often engage in what is known as comity analysis—taking into account the interests of the foreign state in deciding whose law to apply. In a range of cases, the executive branch often does the same—working with foreign counterparts to structure its demand for evidence in ways that avoid conflict with foreign legal obligations.

Congress should take what is routinely done as a matter of discretion and make it mandatory. Specifically, it should clarify that the U.S. warrant authority extends to U.S.-controlled data, regardless of location. But it *also* should require that when U.S. efforts to seek the data of a non-citizen or legal permanent resident located outside the United States conflict with foreign law, the reviewing court engage in a comity analysis, taking into account factors such as the location of and nationality of the target, the location of the crime, the seriousness of the crime, the importance of the sought-after data to the investigation, and the possibility of accessing the data via other means (e.g., with the assistance of the foreign government).

This sets up a presumption that the United States can access, via a warrant, sought-after communications content from U.S.-based providers, without regard to the location of the data. But it also ensures that the interests of foreign governments in controlling access to the data of their own residents and nationals located outside the United States are taken into account. This is important for at least three reasons.

First, it sets a precedent that we would want and expect with respect to foreign governments' efforts to access the data of U.S. residents and U.S. citizens.

Second, it provides a mechanism for providers to better protect themselves from being caught between two conflicting legal obligations—establishing a way to ensure that courts take their concerns into account.

And *third*, it respects the interests of foreign governments in setting rules governing the access to their citizens' and residents' data, but without creating a foreign government veto over U.S. law enforcement's ability to access critical evidence. This is particularly important in cases in which the U.S. government is investigating state-sponsored or state-facilitated crime; a foreign government veto would grind such investigations to a halt.

(2) Notice Requirement

This would ensure that the United States could use a warrant to compel the production of sought-after communications content from U.S.-based providers, regardless

of where the data is physically held. But it would *also* require the U.S. government to provide notice to a foreign government if it were seeking data of one of its residents or citizens located outside the United States. Such a provision should be coupled with an exception for cases in which notice would reasonably be deemed to undermine the investigation or jeopardize national security, such as, for example, instances in which U.S. law enforcement is investigating state-sponsored criminal activity.

This also has a number of benefits. It respects foreign governments' interest in controlling access to their own residents' and citizens' data, ensuring that the foreign government has notice and thus an opportunity to raise, via diplomatic channels, any concerns with the United States. It thus sets a standard that the United States would presumably want and expect other governments to follow if they sought access to U.S. citizens' and residents' data. Particularly if coupled with a required comity analysis, it helps to ensure that any applicable conflict of laws is identified and considered by an independent court.

(3) Reciprocal Notice/Control

This provision would again set the default presumption that the United States could, via a warrant, access the communications content held by a U.S.-based provider, regardless of the location of the underlying data. At the same time, it would explicitly authorize the executive branch to enter into reciprocal agreements with a foreign government pursuant to which the United States would agree to provide the foreign government notice and an opportunity to block the disclosure if the United States were seeking access to the data of that foreign government's residents or citizens located outside the United States. These agreements would require that the foreign government provide the United States the same kind of notice and opportunity to block disclosure if the foreign government were seeking the data of U.S.-based residents and citizens.

The agreements would be structured so that each government would have a specified time frame to either consent to or object to the requested access. If there is no response at the end of that time period, then the government would be deemed to have consented. This too would need to be coupled with some sort of emergency authorization procedure for particularly serious crimes in which a delay would significantly hinder the investigation or jeopardize national security.

Unlike the notice provision described above, this approach gives foreign governments veto power, but *only* if that foreign government grants the same veto power to U.S. authorities, and *only* pursuant to mutually agreed upon provisions. The executive would have control over which countries, if any, would be eligible for such agreements, thus protecting against the risk of an uncooperative state being given the power to stand in the way of U.S. investigations.

Importantly, such agreements would ultimately lead to an increase in privacy protections for U.S. citizens and residents, providing a check against foreign government surveillance that does not currently exist. They would ensure that the United States learn

of any efforts to obtain U.S. citizen and resident data and provide an opportunity to object to such disclosures when demanded by a government with which such an agreement is in place.

* * *

Each of these provisions respond to the security concerns presented by the inability of law enforcement to access sought-after data pursuant to a warrant based simply on the happenstance of where it is held. They respect privacy interests in that they demand, as a default, a warrant based on probable cause before the government can compel the production of communications content. At the same time, they protect against the risk that the United States will compel—or will be perceived as compelling—production of foreign-held data without regard to the legitimate interests of foreign governments in setting the rules governing access to their own residents' and citizens' data. As a self-interested matter, such provisions help to ensure that foreign governments take into account U.S. interests when they are seeking access to data of U.S. residents and citizens.

Some may nonetheless suggest that because these issues are being litigated in the courts, Congress should step back and let the issues work themselves out there first. That would be a huge mistake. It would mean many more months, if not years, of uncertainty, with costs to our security and privacy in the interim. More importantly, the courts are simply not in a position to adopt the kind of nuanced solution that is needed to appropriately take into account the relevant security, privacy, economic, and diplomatic interests at stake. Only Congress can do so. It both can and should.

(ii) Issue #2: Foreign Government Access to U.S.-held data

Any fix to the problems created by the *Microsoft Ireland* case should also address the separate, but related, problems faced by foreign law enforcement seeking access to U.S.-held data. This, too, is a growing concern—also with costs to security, privacy, and our economy.

The problems stem from provisions, also in ECPA, that preclude U.S.-based providers from turning over communications content to foreign governments without regard to the relevant equities at stake. This is true even if the foreign government is investigating its own national in connection with a local crime and the *only* U.S. nexus to the data is that it happens to be held by a U.S.-based company in the United States. Instead, the foreign government is required to go through the mutual legal assistance process and initiate a diplomatic request for the data.

Consider, for example, U.K. law enforcement investigating a London murder spree. The U.K. officials seek the data of the alleged perpetrator in order to help establish motive and ascertain if he had any accomplices. If the perpetrator used a U.K -based provider, it could access the data within days if not sooner. But if instead he uses Gmail or any other U.S.-based service provider, the U.K. officials are told that they must make a

request for the data through the U.S. government, employing the mutual legal assistance process.

This, however, is a laborious and time-consuming process. First, the Department of Justice reviews the request. Second, a federal prosecutor must obtain a warrant from a U.S.-based magistrate based on a U.S.-based standard of probable cause to compel production of this data. (Needless to say, processing these foreign requests for data is not often at the top of most U.S. Attorneys' priority lists.) Third, the warrant is served on the service provider. Fourth, the data, once produced, is routed back to the Department of Justice, where it is again reviewed before finally being transferred to the requesting government. It is a process that generally takes multiple months, sometimes years.[8]

Foreign governments are, understandably, concerned. And we should be as well. Their inability to access data needed to investigate serious crime threatens global security. And they are responding in a number of concerning ways—all designed to bypass this cumbersome process. The range of responses include:

- *mandatory data localization requirements*, pursuant to which the content of communications (or a copy of such content) of a country's residents and/or citizens are required to be held in-country.[9] This ensures that the requesting country can access the data pursuant to domestic legal process, without having to make a diplomatic request to the United States. Not only do such localization requirements facilitate domestic surveillance in ways that threaten to undercut user privacy, but they increase the costs of doing business, potentially price small start-ups out of the international market, and undercut the Internet's innovative potential;

- *unilateral assertions of extraterritorial jurisdiction,* in ways that increasingly put U.S. companies in the cross-hairs between conflicting laws, with foreign governments compelling production of data and U.S. law prohibiting it.

- *threats to arrest or imprison employees or officers of local subsidiaries* for failing to turn over sought-after data, even in situations where U.S. law prohibits them from doing so;[10]

---

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

[9] *See, e.g.*, Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677 (2015) (surveying localization laws); Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders*, THE HAGUE INST. FOR GLOBAL JUST. (May 1, 2014) (describing the rise of data localization movements and analyzing the key motivating factors).

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

- *mandatory anti-encryption regimes* that facilitate live interception of the data as it transits through the requesting government's jurisdiction, thereby providing an alternative way to access sought-after communications;[11] and

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

These responses threaten Internet security, weaken privacy, harm U.S. business interests, and diminish the productive potential of the Internet over time.

The United Kingdom has made fixing this problem—and facilitating access to sought-after data in an open and transparent manner—one of its top diplomatic priorities vis-à-vis the United States. In fact, the United States and United Kingdom already have drafted an agreement that would permit U.S. service providers to directly respond to U.K. law enforcement's requests for communication content in certain specified circumstances involving the investigation of serious crime. It would permit U.S.-based service providers to respond directly to U.K. government demands for emails and other communications content of non-U.S. citizens located outside the United States, so long as a range of specific conditions are met. If, however, the U.K. government wanted the data of U.S. citizens and legal permanent residents (so-called "U.S. persons") and others located in the United States, it would still need to make a mutual legal assistance request to obtain the data, which would ultimately require the issuance of a U.S. warrant. Such a demarcation reflects the idea that U.S. standards should continue to govern access to data of U.S. citizens, legal permanent residents, and persons located within the United States—whereas the United States has little justification in imposing these specific standards on foreign government access to data of non-citizens who are located outside the United States, so long as baseline substantive and procedural standards are being met.

But the agreement cannot be implemented unless Congress amends the statute first. Legislation introduced by the Department of Justice last spring would do just that, and provides a framework for Congress to build on.[12]

The legislation would amend the relevant provisions of ECPA so that U.S.-based service providers can, in specified and narrow circumstances, directly provide communications content to foreign law enforcement officials, so long as baseline substantive and procedural protections are in place. Notably, this kind of direct access would *only* be available to those countries that entered into executive agreements with the United States; would continue to require use of the mutual legal assistance process if the foreign government were accessing the data of U.S. persons and others located in the United States; and would require reciprocal rights of access to the United States in cases

---

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

[12] *See* Draft Legislation to Permit the Secure ad Privacy –Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism (July 15, 2016), https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html.

in which it is seeking foreign-held data. Moreover, the legislation includes a number of specific criteria that would apply.

First, only those governments that were certified by the executive branch as affording "robust substantive and procedural protections for privacy and civil liberties" could enter into such agreements.

Second, it mandates several layers of protection for the data of U.S. persons and others located in the United States. Foreign governments would still be prohibited from directly accessing the data of a U.S. person or other person located in the United States. Foreign governments would be prohibited from acquiring data with the purpose of obtaining information *about* a U.S. person or other person in the United States. Foreign governments would be prohibited from obtaining data at the behest of or with the objective of passing it back to the United States. And foreign governments would be prohibited from transmitting the content of U.S. person communications to the U.S. government unless the data relates to significant harm or threatened harm to the United States or U.S. persons.

Third, each request made pursuant to these agreements must meet several criteria designed to protect privacy. The requests must be for the purpose of preventing, detecting, investigating or prosecuting serious crime; must be targeted to a specific account, device, address, person, or other specific identifier; must be lawful under the foreign government's domestic authorities; must be reviewed or overseen by a court or other independent authority, and must be based on articulable and credible facts.

Fourth, the foreign government must seal, segregate, or delete non-relevant information.

Fifth, the foreign government must submit to periodic compliance reviews by the United States.

And *sixth,* the agreements sunset after five years unless explicitly renewed.

The draft legislation is not perfect, and there are improvements that can and should be made. Congress should, for example, demand judicial "review" of content requests as opposed to "review or oversight" of such requests; it should strengthen the set of findings that support a certification that a country affords robust protections for privacy and civil liberties; and it should make explicit that companies can and should refer any requests to the Department of Justice if they are unclear whether the specified criteria are met.

But in general it is an approach that makes sense. It respects the important principle that U.S. standards should continue to govern access to data of U.S. citizens, legal permanent residents, and persons located within the United States—whereas the United States has little justification in imposing these specific standards on foreign

government access to data of non-citizens who are located outside the United States, so long as baseline standards and procedures are met.

It also puts in place a set of standards that foreign governments must comply with in order to be able to directly access U.S.-held data. This is essential and justified for at least two reasons. *First,* while the targets of foreign government requests under this system will be foreign nationals that are located outside the United States, communications are inherently intermingled. It is likely—in fact almost certain—that such requests will at times lead to the incidental collection of U.S. person data and data of other persons physically residing in the United States. This reality provides both an opportunity, and arguably an obligation, for Congress to demand a set of baseline standards to protect those persons that fall squarely within its responsibility and authority to protect. *Second,* these types of agreements provide the United States with a unique opportunity to begin to set the contours of global privacy rights—something that is not only the right thing to do, but will also ultimately inure to the benefit of the United States. Countries need to meet the specified standards in order to get expedited access to data in legitimate cases. It thus provides a unique opportunity for the United States to promote the leveling up of protections for all.

It is an approach that Congress should endorse—and adopt.

An Additional Issue: Broader ECPA Reform

I would be remiss if I failed to take this opportunity to encourage the Senate to also take up broader ECPA reform. In February, the House of Representatives passed the Email Privacy Act by voice vote; a similar bill passed the House last year 419-0. The bill, which has been referred to this Committee, should be taken up and passed by the Senate. It addresses the following two issues:

(i) *Warrant for Content.* This is something that is required by the Sixth Circuit under its decision in *United States v. Warshak*;[13] is the current practice of the U.S. government in its criminal investigations; is demanded by every major U.S. service provider; and reflects the basic premise that law enforcement should not be able to read our emails and other private communications without a warrant. Codification of this requirement would not yield any change in current practice. It would instead ensure that the practices do not change in the future—and that our emails and other private communications are protected in the same way as a letter sent through the mail.

(ii) Notice Requirements. When the government accesses emails from a service provider via a warrant, it need not notify the target of its investigation that it has done so. In other situations, the government is required to give notice, but can delay notice based on a finding that it would have an "adverse result."[14] The government also can obtain an order prohibiting the service provider from disclosing the fact of the search—what is colloquially known as a "gag order." There are of course often good reasons for these

[13] 631 F.3d 266 (6th Cir. 2010).
[14] *See* 18 U.S.C. § 2705(a).

provisions, such as the risk that disclosure will tip off a target and lead to the destruction of evidence.

That said, at some point the investigation comes to an end and the ongoing secrecy is no longer justified. Yet the government is seeking and obtaining gag orders of indefinite duration—precluding the provider from *ever* telling its customer that his or her data has been obtained. Microsoft, for example, reports that between September 2014 and May 2016, it received more than 3,250 secrecy orders, more than 2,000 of which *indefinitely* barred Microsoft from disclosing the law enforcement requests to their customers.[15] Microsoft is not alone. In the first seven months of 2016, Yahoo has received over 700 federal search warrants for user data, and well over half—about 60%—were accompanied by gag orders of indefinite duration. Google reports a similar percentage—about 60% of requests for user data accompanied by gag orders of indefinite duration.[16]

This kind of secrecy cannot be justified. While secrecy is sometimes essential to ensuring the integrity of an investigation, indefinite secrecy is not. The Email Privacy Act responds to these concerns by setting an outer, yet renewable, limit of 180 days for such gag orders. The Senate should require the same.

***

The laws governing law enforcement access to data across borders are in critical need of updating. Due to the Second Circuit decision in *Microsoft Ireland*, the United States is prevented from accessing data in legitimate investigations based simply on where the data happens to be held. This is the case even when U.S. law enforcement has obtained a warrant based on probable case that the data is evidence of a crime, and even though the data is controlled by a U.S.-based service provider. Provisions of ECPA impose the same kinds of difficult-to-justify limits on foreign governments—precluding their ability to directly access the data of their own citizens and residents in the investigation of local crime, based simply on the fact that the data is U.S.-held.

Congress now has both an opportunity—and in my view a responsibility—to update our laws so that law enforcement can lawfully access the data needed to detect and prosecute crime. It should do so in a way that promotes privacy, protects the future growth of an open and connected Internet, and shields U.S. companies from being caught between impossible to resolve competing legal obligations with one nation compelling the production of data and another prohibiting it. These reforms are needed to resolve the mismatch between old laws and new technology, and thereby protect our security, our privacy, and our economy.

---

[15] *See* First Amended Compl., Microsoft Corp. v. United States, 2:16-cv-538, ¶ 2, 16 (W.D. Wash. June 16, 2016).

[16] *See* Br. of Amici Curiae Amazon.com et al, Microsoft Corp. v. United States, 2:16-cv-538, at 8 (W.D. Wash. Sept. 23, 2016).

Thank you.