AMERICAN UNIVERSITY
WASHINGTON, DC

Statement of
Jennifer Daskal

Assistant Professor
American University Washington College of Law

Committee on the Judiciary
United States House of Representatives

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

February 25, 2016

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

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

Committee on the Judiciary
United States House of Representatives

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

February 25, 2016

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

For the past six months, I have been working with a cross-section of companies, civil society groups, and other academics who share common concerns about the rules governing law enforcement access to data across borders — and the potentially negative consequences of these rules for privacy, security, American business, and the future of the Internet. While my testimony draws on those conversations, I speak solely in my personal capacity and not on behalf of anyone else.

Earlier this month, the *Washington Post* reported that the United States and United Kingdom are negotiating an agreement that would begin to address some of these concerns.[1] Specifically, the agreement would, according to press reports, permit U.K. law enforcement officials to directly request the content of stored emails and other data from U.S.-based providers. Such an agreement is needed. If done right, it would be an important step forward — one that can minimize dangerous incentives toward data localization and other less accountable means of accessing sought-after data; promote privacy and related human rights; and protect U.S.-based companies from being increasingly caught between conflicting laws.

But an agreement of this kind cannot be implemented without Congress's authorization. Congress thus has an important opportunity — and in my view responsibility — to empower the executive to enter into such agreements and to set the key parameters as to their details. Such parameters are essential to protecting American interests in both the short and long term, and to setting the stage for a system of access to cross-border data that simultaneously protects privacy, security, and the Internet of the 21st century.

[1] Ellen Nakashima & Andrea Peterson, *The British want to come to America – with wiretap orders and search warrants,* THE WASH. POST, Feb. 4, 2016.

The following testimony describes the problem and offers a suggested way forward. I end with a discussion of several important and related issues, including the need to modernize the Mutual Legal Assistance Treaty (MLAT) system, the absence of rules governing foreign government access to transactional records (such as to/from lines on emails), and the ongoing debate over the reach of the United States' warrant authority under the Stored Communications Act (SCA). As I explain in more detail below, the basic jurisdictional questions should be answered in a reciprocal way for both the United States and foreign governments, and should turn primarily on the location and nationality of the target of the investigation, rather than the location of the data.

The Problem

The SCA, enacted in 1986 before communications were truly global, operates as a blocking statute. Except in very limited circumstances, it prohibits U.S.-based Internet Service Providers (ISPs) from disclosing certain data, including the content of users' communications (such as stored emails), to anyone other than the U.S. government pursuant to a U.S.-judge issued warrant based on a U.S.-based standard of probable cause.[2] While such a warrant requirement is a strong privacy-protective standard — and one that I hope Congress ultimately makes applicable, as a matter of statutory law, to *all* United States government requests for stored content[3] — it poses a combination of normative and practical problems when imposed on other countries. Ironically, the end result, as I explain in what follows, may be a reduction of privacy and related rights-protections for all.

As a result of the SCA's blocking provision, law enforcement seeking the content of stored communications, such as emails, that are held by a U.S.-based ISP cannot directly request the data from the ISP. Rather, they must make government-to-government requests for the data — even when they are seeking data of their own citizens in connection with the investigation of a local crime. This is a time-consuming process, and it is frustrating key foreign partners, particularly as criminal investigations increasingly rely on digital evidence in the hands of U.S.-based ISPs. Why, after all, should the United States insist on American standards and American procedures when the only connection to the United States is that the data happens to be held by a U.S.-based provider?

Consider, for example, U.K. law enforcement officials investigating a London murder. Imagine that the agents think the crime arose from an affair gone bad and seek the emails of the alleged perpetrator to help establish motive. If the target of the investigation uses a U.K.-based ISP, the officials would likely get access to the data within days, if not sooner. If, instead, the data is held by Google or another U.S.-based provider, the U.K. officials will be required to go through what is known as the MLAT process and initiate a formal U.K.-U.S. request for the data.

---

[2] *See* 18 U.S.C. 2702(b); 2703(a) (2012).

[3] I am encouraged by the overwhelming, bipartisan support for the Email Privacy Act, H.R. 699, 114th Cong. (2015), which now has 310 co-sponsors, and I urge the Committee to report the bill favorably and the House leadership to bring it to a vote on the floor.

This is a laborious process. First, the Department of Justice reviews the request. If approved, it is forwarded to the relevant U.S. Attorney's Office. 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 ISP. 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. The process takes an average of ten months.[4]

Foreign governments' frustrations are understandable, 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.[5] 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 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. In fact, current (albeit soon to expire) U.K. law asserts the authority to compel the production of stored content from any company that does business in its jurisdiction, without any limit based on the target's nationality or place of residence;[6]

---

[4] *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 [http://perma .cc/36EE-6J9F] (noting that the United States takes an average of ten months to respond to official requests made through the MLAT process for email records).

[5] *See, e.g.*, Sergei Blagov, *Russia's 2016 Data Localization Audit Released,* BLOOMBERG LAW, Jan. 13, 2016, http://www.bna.com/russias-2016-data-n57982066291/; 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), http://ssrn.com/abstract=2430275 [http://perma.cc/D2FC-F29Y] (describing the rise of data localization movements and analyzing the key motivating factors).

[6] *See, e.g.*, Data Retention and Investigatory Powers Act 2014, c.27, § 4, (Eng.) (expires December 31, 2016). While the legislation specifies that "regard is to be had" to a possible conflict of laws, the legislation does not say whether and in what situations the laws of the nation in which the data is located would trump. *Id.* § 4(4); *see also* INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, REP. ON THE INTELLIGENCE RELATING TO THE MURDER OF FUSILIER LEE RIGBY, 2014, HC 795, at 151 (UK) (describing

- *threats against employees or officers of local subsidiaries* for failing to turn over the sought-after data, even in situations where U.S. law prohibits them from doing so;[7]

- *mandatory anti-encryption regimes* (e.g., mandatory backdoors) that facilitate live interception of the data as it transits through the requesting government's jurisdiction and thereby provide an alternative way to access sought-after communications;[8] and

- *increased use of malware* and other opaque and less accountable means of accessing the data that weaken the security for all users.[9]

These responses threaten the privacy rights of all users of the Internet, including American citizens and residents. They undermine security, harm U.S. business interests, and diminish the productive potential of the Internet over time.

The Solution

The U.S.-U.K. discussions provide a possible response to some of these concerns. If done right, such an agreement could provide a front door alternative to back channel methods of gaining access to the same evidence. It would help to minimize the dangerous incentives in favor of mandatory localization, unilateral assertions of extraterritorial jurisdiction, and mandatory decryption requirements. And it is an opportunity to establish a set of transparent, accountable, and privacy-protective rules — rules that can then become a model for further bilateral and multilateral agreements.[10]

Specifically, the draft agreement, at least as reported by the *Washington Post*, would permit U.K. law enforcement officials to make direct requests to U.S.-based ISPs for stored content, so long as the target of the request resides outside the United States, and is not a U.S. citizen or legal permanent resident. If, however, the U.K. sought emails of U.S. citizens, legal permanent residents, or persons residing in the United States, regardless of their nationality, it would need to employ the MLAT system, and could only

---

a key goal of the legislation as permitting access to otherwise difficult-to-obtain data held by U.S.-based providers).

[7] *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 2014 in Brazil for his company's refusal to produce Skype data belonging to the target of a criminal investigation).

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

[9] *See, e.g.*, Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JUST SECURITY, Feb. 16 , 2014 https://www.justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/ (explaining how malware could be used to subvert otherwise applicable territorial limits on direct access to sought-after data)

[10] *See* Jennifer Daskal, *A New US-UK Data Sharing Agreement: A Tremendous Opportunity, If Done Right*, JUST SECURITY, Feb. 8, 2016, https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/.

obtain the data based on 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. This approach presents a much preferable alternative to the U.K. claim that U.K. law enforcement can unilaterally compel the production of certain communications content from any provider that does business in its jurisdiction, including emails sent and received by U.S. citizens.

These privileges and limits also are reportedly designed to be reciprocal (as they should be), meaning that the U.S. would be permitted to directly compel the production of non-U.K. resident and non-U.K. national data from U.K. providers, but would need to initiate diplomatic processes if it wanted a U.K.-based provider to turn over data on one of its own citizens.

None of this, however, can happen without Congress. For any such bilateral or multilateral agreement to be implemented, Congress first needs to amend the SCA to permit foreign governments to directly request emails and other stored content from U.S.-based providers in certain, specified circumstances.

Specifically, Congress should amend the SCA to authorize the executive branch to enter, on a case-by-case basis, bilateral and multilateral agreements that permit foreign law enforcement to make direct requests to U.S.-based ISPs for U.S.-held stored content. In doing so, Congress should also *set the key parameters of such agreements* — ensuring among other things that the requesting country meets basic human rights standards, that the particular requests satisfy a baseline set of procedural protections, and that the system is subject to meaningful transparency and accountability mechanisms.

In addition to requiring foreign governments to rely on the MLAT system (including the requirement of a warrant based on probable cause) to get the data of U.S. residents, as well as U.S. citizens and legal permanent residents wherever located, Congress should specify that any agreement include the following elements:

(i) *General Human Rights Protections*: The executive branch should be required to certify that the partner government meets basic human rights norms prior to entering into such an agreement. This is critical to guard against sought-after data being used to torture, abuse, or otherwise violate the target's (or others') human rights;

(ii) *Request-Level Protections:* The legislation should specify a set of baseline requirements that the requests made under this system should meet. These should include, at a minimum, a requirement that the requests be made by an independent and impartial adjudicator; be targeted to a particular person, account, or device; be narrowly tailored as to duration; and be subject to robust minimization requirements to protect against the retention and dissemination of non-relevant information;

(iii) *Transparency and Accountability Measures*: The legislation should mandate that the partner government publish reports regarding the number, type, and temporal scope of the data requests they issue under this framework. (The United States would similarly need to agree to do the same with respect to requests made of foreign-based providers.) The partner government should also be required to comply with regular assessments designed to evaluate compliance with these requirements; and

(iv) *Sunset Provision*: The legislation should specify that any such agreement sunset after a set period of years, absent an assessment that the requisite procedural and substantive requirements have been met.[11]

These requirements are both essential and justified for at least two key 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. citizen 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 minimal 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 and at the same time promote Internet security. The United States is often in the position, via its annual State Department Human Rights reporting and a myriad other diplomatic channels, of exhorting other countries to improve human rights standards and protect free expression. The United States now has a rare opportunity to couple such exhortations with an attractive carrot. Countries need only meet the specified standards in order to get access to data in legitimate cases. It thus provides an opportunity for the leveling up, rather than the leveling down, of protections for all.

Additional Issues

Mutual Legal Assistance Reform. At least initially, only a handful of countries may be in a position to meet the specified requirements. And even those that do still will need to employ the mutual legal assistance system if they seek data of U.S.-located persons, as well as U.S. citizens and legal permanent residents, wherever located.

There is thus an ongoing need to update and streamline the mutual legal assistance system, and I applaud the efforts of many members of this Committee who have advocated for reforms such as the creation of an online system for tracking foreign government requests. Additional resources are needed to facilitate more efficient and

[11] For a further elaboration of these principles, *see* Jennifer Daskal & Andrew K. Woods, *Cross-Border Data Requests: A Proposed Framework*, JUST SECURITY, Nov. 24, 2015, https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/.

expeditious handling of such foreign government requests — requests that will only increase over time as more and more evidence becomes digitalized.[12]

Wiretap Authority. The U.K. also wants the authority to compel U.S. provider assistance with live intercepts of data transiting through the United States and/or controlled by U.S.-based providers. And in fact, the draft U.S.-U.K. agreement, as reported, covers both stored communications and live intercepts. If enacted, U.K. law enforcement would be permitted to directly compel U.S.-based providers to assist with live intercepts. But this, too, would require Congressional action, in the form of an amendment to the Wiretap Act.

In considering this possibility, it is worth clarifying a few points. The *Washington Post* characterizes this possibility as the Brits "com[ing] to America,"[13] but this is not an accurate description of what the U.K. seeks. The agreement would, at least according to the publicly available information (and according to anything that Congress would reasonably authorize), be limited to U.K. wiretap orders for foreign national targets located outside the United States. It would allow, for example, the U.K. to compel a U.S.-based provider to assist with the real-time monitoring of a live chat between two U.K. nationals who are located in London and are suspected of plotting a terrorist attack on Big Ben. It would *not* permit the U.K. to wiretap persons located in the United States, or U.S. citizens or U.S. legal permanent residents wherever located. Nor should it.

It would, however, operate as a *new* authority. Currently, foreign governments can get access to U.S.-held stored content; they just have to use the laborious and inefficient MLAT system. No such mechanism exists for foreign law enforcement to directly compel the production of live intercepts from U.S.-based providers. And while U.S. agents may assist the U.K. — or other foreign governments — in certain circumstances (such as in the course of a joint venture), wiretap applications under U.S. law are subject to much more rigorous court review and minimization requirements than the requests for stored communications.

These historical facts are important, and suggest the need for caution — or at least further inquiry and the possible implementation of additional protections — prior to amending the Wiretap Act. That said, the history should not be decisive. The line between live and stored communications is increasingly blurred. And depending on the details, prospective time-limited intercepts can be much less intrusive than the acquisition of stored content over a much longer time frame. More information about the full range of communications and types of orders that might be subject to such an agreement is needed.

---

[12] *See, e.g.*, Andrew K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, GLOBAL NETWORK INITIATIVE (2015), http://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf [http://perma.cc/PA6M-XVLZ] (suggesting a range of useful improvements to the mutual legal assistance system); *supra* note 3, THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES at 226-29 (Dec. 12, 2013) (suggesting ways to improve the mutual legal assistance treaty process).

[13] *See, supra*, note 1.

Transactional Records. Notably, the SCA's blocking provision applies only to content. Transactional records (or what the international community calls "traffic data"),[14] including to/from lines in emails and location data, and other non-content data can be provided directly to foreign governments. Transparency reporting suggests that non-content data is in fact turned over to foreign governments in large numbers.[15]

But whereas there is a range of non-content data that U.S. officials can only obtain through a court order, based on a finding of "specific and articulable facts showing that there are reasonable grounds to believe that the [data] sought, are relevant and material to an ongoing criminal investigation,"[16] no such analogous standard applies to foreign government requests — even when seeking data of U.S. citizens and persons located in the United States. This suggests a need to limit foreign government access to such data, particularly in instances when foreign governments are seeking information about U.S. citizens, legal permanent residents, and others located within in the United States.

The Microsoft Case and the LEADS Act. The precise converse of the issues I have described above (with respect to foreign governments seeking access to U.S. held data) are playing out in the pending *Microsoft* case now before the Second Circuit. In that case, the U.S. government is seeking data held outside the United States. Specifically, the government is seeking to compel the production of emails controlled by Microsoft, but stored in Dublin, Ireland. Microsoft objects on the grounds that the U.S. government's warrant authority does not have extraterritorial reach, and that the United States should make a direct request to Ireland for the data, via the MLAT in place between the United States and Ireland.

As I have argued elsewhere, both positions are flawed.[17] The United States is asserting a very broad theory of its jurisdictional reach over data; so long as it has jurisdiction over the provider it can compel production of data, wherever located, and without regard to the nationality or location of the target. This is the exact converse of the authority claimed by the U.K. — an authority that the United States rightly rejects.

Microsoft, in contrast, is unduly focused on data location as the key criterion for establishing warrant jurisdiction. According to Microsoft, the government can only

---

[14] *See, e.g.*, Council of Europe Convention on Cybercrime art. 1(d), opened for signature Nov. 23, 2001, S. TREATY DOC. NO. 108-11 (2006), E.T.S. No. 185 (entered into force July 1, 2004).

[15] *See, e.g., Microsoft Transparency Hub, Law Enforcement Requests Report Jan-June 2015*, https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/lerr/ (indicating that Microsoft received approximately 30,000 foreign government requests for data between January and June 2015 and disclosed non-content data in response to about 10,000 such requests); Yahoo! *Transparency Report: Government Data Requests*, https://transparency.yahoo.com/government-data-requests/index.htm, (indicating that Yahoo! received approximately 10,000 foreign government requests for data between January and June 2015 and disclosed non-content data in response to about 4,500 such requests).

[16] 18 U.S.C. § 2703(d) (2012).

[17] *See* Jennifer Daskal, *The Un-Territoriality of Data,* 125 YALE L.J. 326 (2015); Jennifer Daskal, *The Microsoft Warrant Case: The Policy Issues,* JUST SECURITY, Sep. 8, 2015, https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues/.

compel production if the *data* is located within the United States. But this position both fails to account for the unique attributes of data and further incentivizes concerning data localization requirements. Data is, after all, highly mobile, potentially divisible, and, thanks to the cloud, often held in locations disconnected from — and perhaps not even known to – the data user, the person with the primary privacy interest in the data.[18] It thus makes little normative and practical sense for law enforcement jurisdiction to turn on where data happens to be located at any given time.

As a result, Congressional action is needed regardless of who wins the case — as the Second Circuit urged and many members of the committee have already recognized. The pending Law Enforcement Access to Data Stored Abroad Act (the LEADS Act),[19] which was introduced by Representative Tom Marino and is co-sponsored by several members of this Committee, offers one possible attempt to do so and is definitely a step in the right direction. It is very encouraging to see so many members engaging on this important issue.

That said, I worry that the LEADS Act as currently drafted, retains too heavy an emphasis on the location of data, as opposed to other — and in my view preferable — criteria for establishing the scope of warrant jurisdiction. An emphasis on data location runs the risk of entrenching data localization movements and also creates a set of odd anomalies (whereby the ability of the United States to access the data of a foreign national residing in and engaging in criminal activity within the United States would turn on the place where the data is stored).

Consistent with the above-stated approach to the U.S.-U.K. agreement (or any other equivalent agreements that are subsequently negotiated), it would be preferable for warrant jurisdiction to turn on the location and nationality of the target — rather than the location of data. Among many other benefits, such a standard sets the stage for exactly the kind of international agreements that Congress should be encouraging.

***

To sum up, the system for responding to law enforcement's interest in data across borders is broken. The United States has both an opportunity — and in my view a responsibility — to build a future system that simultaneously tracks American values, protects American businesses, safeguards Americans' privacy, and promotes the growth of an open and secure Internet. The fact that the United States and U.K. are talking is a positive step forward. It is now up to Congress to authorize the executive branch to enter into such agreements, but also to ensure that they are done right.

Thank you for the opportunity to testify. I look forward to your questions.

[18] *See, supra*, note 13, *The-Unterritoriality of Data*, 125 YALE L.J. at 365-378.
[19] The Law Enforcement Access to Data Stored Abroad (LEADS) Act, H.R. 1174. 114th (2015).