

DIGITAL ACCESS TO SCHOLARSHIP AT HARVARD
DASH.HARVARD.EDU

HARVARD LIBRARY


Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement

Citation

Lin, Tiffany, and Mailyn Fidler. 2017. Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement. A Berklett Cybersecurity publication, Berkman Klein Center for Internet & Society.

Link

http://nrs.harvard.edu/urn-3:HUL.InstRepos:33867385

Terms of use

This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material (LAA), as set forth at
https://harvardwiki.atlassian.net/wiki/external/NGY5NDE4ZjgzNTc5NDQzMGIzZWZhMGFlOWI2M2EwYTg

Accessibility

https://accessibility.huit.harvard.edu/digital-accessibility-policy

Share Your Story

The Harvard community has made this article openly available.
Please share how this access benefits you. Submit a story

September 2017

Cross-Border Data Access Reform

a primer on the proposed US-UK agreement

Tiffany Lin
Mailyn Fidler

a Berklett Cybersecurity publication



Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement

Tiffany Lin and Mailyn Fidler[i] | September 7, 2017
A Berklett Cybersecurity Publication[ii]

Introduction

Cross-border data access reform may be on the legislative agenda in late 2017, with recent House and Senate judiciary committee hearings revisiting the topic.[1] In light of this increasing interest, we thought it would be helpful to provide a brief primer on how cross-border data access requests currently work, options for reform, and major challenges to reform ahead. This document presents a short, high-level background review of the debate as it currently stands, particularly focusing on the DOJ's 2016 proposal for reform.

Governments need evidence to investigate and prosecute crimes, but increasingly that evidence takes the form of data stored on the servers of U.S. tech companies. In July 2016, the U.S. Department of Justice (DOJ) released draft legislation that would address some of the challenges foreign governments face when seeking data related to criminal investigations from U.S. companies.[2] Interest in making such changes continues to grow, with relevant laws, including the Electronic Communications Privacy Act (ECPA), maybe seeing Congressional attention in late 2017, especially as the Foreign Intelligence Surveillance Act (FISA) comes up for renewal.

To access electronic content – including email, social media messages, and more – held by U.S. companies, a foreign country currently relies primarily on the processes set out in agreements called Mutual Legal Assistance Treaties (MLATs), if that country has negotiated one with the U.S.[3] MLATs with the U.S. require countries to meet U.S. legal standards when making requests for electronic content data (see more details below and Diagram 1), with less strict standards for

[i] Tiffany Lin, Research Associate, Berkman Klein Center for Internet & Society at Harvard University. Mailyn Fidler, 2016-2017 Fellow, Berkman Klein Center for Internet & Society at Harvard University; Yale Law School J.D. candidate '20. The authors thank the Berklett Cybersecurity project participants – especially Jane Horvath and Matthew Perault – and Berkman Klein Cyberlaw Clinic Instructor Vivek Krishnamurthy, for their invaluable comments and feedback on earlier drafts. We also thank the Berklett Cybersecurity project team, Jonathan Zittrain, John DeLong, Matt Olsen, David O'Brien, Bruce Schneier, Ben Sobel, and Urs Gasser. This piece would not have been possible without their inspiration, support, feedback, and contributions. We are also indebted to the Berkman Klein staff who support the Berklett Cybersecurity project meetings, including Carey Andersen, Daniel Oyolu, and Ellen Popko.

[ii] This publication is an adaptation of a briefing document originally created to inform discussions in the Berklett Cybersecurity project meetings about the proposed U.S.-U.K. agreement on cross-border data sharing and related issues. Launched in 2015, the Berklett Cybersecurity project is a unique forum for discussing true and important, if not novel, facts, perspectives, and surprising consensus on the enduring questions of cybersecurity, government, foreign intelligence, law enforcement, civil society, and industry. The project aims to achieve a depth of trusted and honest discussion among key stakeholders to significantly advance thoughtful progress on these complex issues, and, when possible, inject the insights and consensus from our discussions into public discourse. More information about the project can be found on the Berkman Klein Center's website: http://cyber.harvard.edu/research/cybersecurity. The Berklett Cybersecurity project is generously supported by the William and Flora Hewlett Foundation. Research efforts that contributed to this publication were also supported by the John D. and Catherine T. MacArthur Foundation and the Ford Foundation.

metadata. Countries have grown frustrated with both the normative implications of the MLAT process and its typical lengthiness.

After substantial debate, and with many proposed ideas from civil society, industry, and academia, the Department of Justice (DOJ) in July 2016 released draft legislation intended to address these concerns. The proposal moves away from the treaty-based system currently underpinning the mutual legal assistance process. Instead, the new legislation would require "lighter touch" bilateral agreements on this issue between the United States and participating countries. Once countries are approved for these bilateral agreements, the legislation would allow them to submit requests for data, made pursuant to the requesting countries' laws and stipulations in the legislation, directly to U.S. electronic service providers, instead of first going through U.S. courts (see Diagram 2). The U.K. would likely be the first country approved to make requests under this new legislation, but the legislation would also pave the way for agreements with other qualifying countries. This legislation advances a legal solution for cross-border data access that proponents hope is sufficiently appealing to foreign governments to forestall more damaging alternative responses to data access concerns, including country-wide service bans, mandated data localization, or forcing companies to make decisions in the face of a conflict of laws.[4]

How the Current MLAT System Works

The increased use of the Internet as a communications mechanism means electronic evidence is increasingly relevant to criminal investigations. Tech companies headquartered in the U.S. hold a majority of electronic data, meaning U.K. police investigating a crime in London, for example, may need to access emails stored by a U.S.-based provider. The current U.S. legal system requires U.K. police to make use of the U.K.'s Mutual Legal Assistance Treaty with the U.S. to access data stored in the United States. Although MLATs were designed to deal with a range of law enforcement cooperation, they have become the main mechanism for accessing electronic evidence across borders. The current MLAT process for electronic evidence requests works as follows (see Diagram 1):

1. A foreign law enforcement agency or other investigative body desiring access to data held by a U.S. company files a request with their country's designated central processing agency, which reviews the request.
2. Once approved, the foreign country sends the request to the U.S. DOJ's Office of International Affairs (OIA).
3. The OIA works with the foreign country to revise the request's format and content to meet U.S. standards.
4. Once the OIA is satisfied, OIA works with a U.S. Attorney's Office to send the request to a local U.S. magistrate judge for review.
5. The court must find that the request is in keeping with all relevant U.S. law, notably including the Fourth Amendment's probable cause standard, rules of privilege, and the Fifth Amendment. If any of these are not met, the OIA and the requesting country's agency continue to work together until the court is satisfied.
6. Once approved by the court, the request is served on the relevant company.

7. Once the company receives the request, it locates and submits the relevant evidence to the OIA.
8. The OIA reviews the evidence to ensure it meets data minimization and human rights standards.
9. Finally, the evidence is sent back to the foreign government's central processing agency, which then provides it to the original investigating team. The process takes six weeks to ten months on average, often depending on the quality of the request (that is, how much the original filed request followed the required standards and how many iterations of review were required).[5]

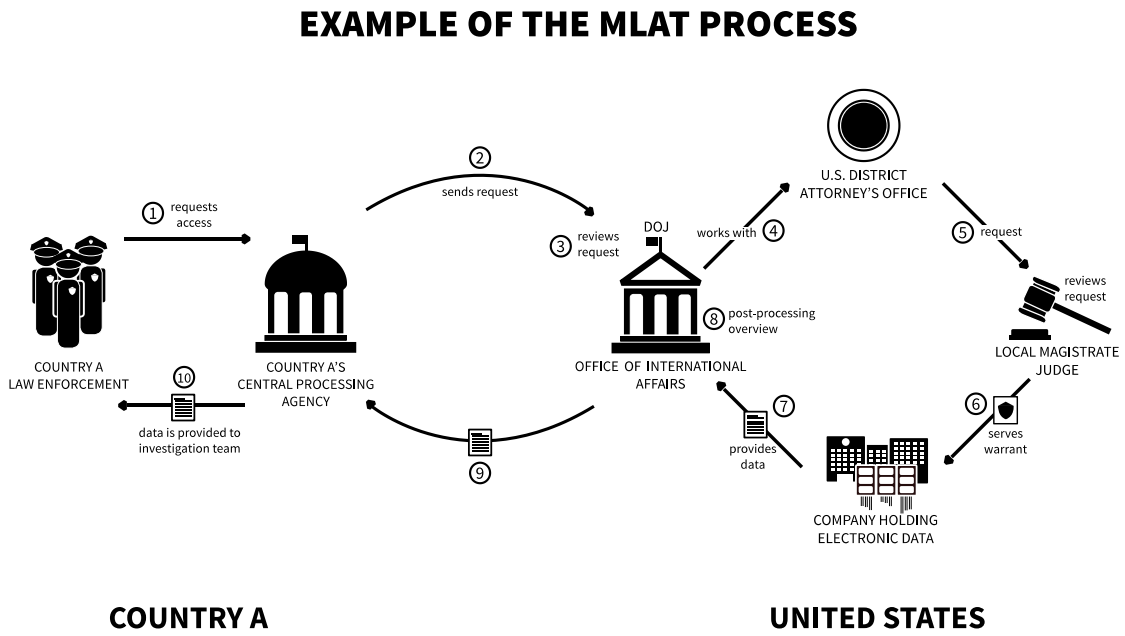


Diagram 1 Example of the U.S. Mutual Legal Assistance Treaty Process for Electronic Evidence

Countries must follow the MLAT process to access data held in the U.S. largely because U.S. law restricts when U.S. companies can disclose information to outside entities. The Electronic Communications Act (ECPA), (specifically, Title II of ECPA, also called the Stored Communications Act) contains blanket restrictions that prohibit U.S. companies from sharing the *content* of stored electronic communications with government entities, other than pursuant to a warrant or consent of the user.[6] Companies are also able to disclose content information voluntarily in the event of an emergency.[7] In terms of *metadata*, the situation is slightly different: companies can disclose metadata to foreign governments more easily than it can to U.S. government agencies, which must obtain a court order.[8] In terms of real-time surveillance, the Wiretap Act prohibits it without a warrant or court order unless certain exceptions have been met.[9] Together, these prohibitions have been interpreted to cover any government entity, including foreign entities.[10] This presumption feeds the reliance on the MLAT process, which generates the legal orders that allow companies to share data.

Problems with the Current System

As the demand for electronic evidence has grown and with an increasing amount of user data being stored remotely on company servers,[11] the number of MLAT requests has burdened the original MLAT architecture, rendering it outdated and inefficient. In their 2015 fiscal year budget request, the Department of Justice stated that "request for assistance from foreign authorities ha[d] increased nearly 60 percent, and the number of requests for computer records has increased ten-fold" over the past decade, slowing processing times.[12] Countries are understandably frustrated with current state of affairs and are looking to other methods for accessing data, such as expanding their own surveillance capabilities, limiting use of encryption,[13] mandating data localization,[14] expanding extraterritorial application of their laws, and exploitation of software vulnerabilities by law enforcement in order to access data,[15] all of which would run counter to an open Internet, which the U.S. has historically championed. More generally, countries are frustrated that U.S. law essentially determines global practices, viewing the globally-applied MLAT legal standards as a limit on state sovereignty.

Many actors have called for reform.[16] For instance, the President's Review Group on Intelligence and Communications Technologies in 2013 highlighted some major needed changes, including creating an online submission form, increasing resources to the DOJ's Office of International Affairs (OIA), and streamlining steps and provisions in the process.[17] Additionally, calls for ECPA reform generally have gone on for some time, given its 1980s origins putting it at odds with some of the technological realities of today. Companies have called for changes to the cross-border data access system, given the increasingly difficult positions in which they find themselves. For instance, at times companies are unable to produce data due to conflicting laws between the U.S. and a foreign state, or due to the nature of the company's technical architecture.[18] As a result, companies are joining the call for a more streamlined process, allowing easier lawful access to data in ways that would still ensure privacy and civil liberties protections.[19]

DOJ's Proposed Legislation on Cross-Border Data Access

The DOJ's July 2016 cross-border data access legislative proposal would enable approved foreign governments to conclude executive agreements with the U.S. that would allow them to submit requests for electronic data, both stored and intercepted live, directly to U.S. companies. These requests would bypass the current gatekeeping performed by the U.S. legal system.[20] The draft legislation sets out the standards countries must meet to qualify for an agreement and establishes parameters on what the requests can include. For instance, requests must pertain to a serious crime, including terrorism. This proposal would also afford the U.S. reciprocal rights with respect to the partner country. Although put forward by the DOJ, the proposal took into account previous papers and working group efforts.[21]

The proposed bill would amend parts of ECPA, specifically the Wiretap Act, the Stored Communications Act, and the Pen Register Act. It would insert exceptions to permit companies to 1) intercept and 2) disclose stored electronic communications in response to a foreign order made pursuant to an executive agreement.[22] Again, in this case, the foreign government would have to qualify for and possess a current relevant executive agreement with the U.S. and the

foreign order would have to meet certain specifications. However, orders do not undergo individual inspection by the U.S. government, making the vetting of countries for the executive agreement the single guaranteed point of scrutiny.

Details of the Proposed Legislation

The proposal outlines conditions a foreign government must meet to qualify for an executive agreement with the U.S.[23] The Attorney General, with the concurrence of the Secretary of State, must determine and certify to Congress that the foreign government meets certain standards, including that the foreign government has domestic laws that afford robust substantive and procedural protections for privacy and civil liberties. These conditions require, in part, that the foreign government has:

- substantive and procedural laws on cybercrime and electronic evidence;
- evidence of respect for the rule of law and principles of non-discrimination, and adherence to applicable international human rights obligations;
- mechanisms to provide accountability and transparency for data collection;
- a showing of clear mandates, procedures, and effective oversight of authorities' collection, retention, use, and sharing of data;
- mechanisms for accountability and transparency for the collection and use of data; and
- a commitment to promote and protect the free flow of information and the open Internet (essentially a promise not to pursue actions such as data localization).

Once a country has established an executive agreement, that country is able to send a request to an electronic communications company directly, without first going through U.S. agencies or courts. The request itself:

- cannot infringe freedom of speech;
- must be subject to review or oversight by a court, judge, magistrate, or other independent authority in the issuing country;
- must be based on requirements for a reasonable justification based on articulable and credible facts;
- must be issued in compliance with the *foreign* country's domestic law, and any obligation for a provider to produce data is solely from that law;
- not intentionally *target* a U.S. person (or person located in the U.S.) or target a non-U.S. person with the intention of obtaining information on a U.S. person;
- must pertain to the "prevention, detection, investigation, or prosecution of serious crime, including terrorism" and must use a specific identifier (i.e., name, account, or personal device);
- must be based on articulable and credible facts, particularity, legality, and severity of the conduct under investigation; and
- if the order is for the interception of wire or electronic communications, it must be of fixed, limited duration and can only be issued where that same information could not be reasonable obtained by a less intrusive method.

The executive agreement places further procedural requirements on the foreign government. The foreign government must:

- promptly review all material collected, and segregate, seal or delete (may not disseminate) material not found to be relevant to the request;
- not disseminate content of a U.S. person to a U.S. authority unless it relates to significant harm or threat of the U.S. or U.S. persons including crimes of national security, terrorism, violent crime, child exploitation, or significant financial fraud;
- afford reciprocal rights of data access to the U.S.;
- agree to periodic reviews of compliance, with the U.S. government reserving the right to rescind the agreement; and,
- the company would not be compelled under U.S. law to respond to the request (but companies may, in reality, face other, non-legal pressures to comply).

The proposed legislation would also contain an "anti-cat's paw" provision, stating that the U.S. cannot use this agreement to ask a foreign government to share information the U.S. would not be able to obtain on its own.[24] This provision protects the privacy of U.S. persons by requiring U.S. government agencies to work through U.S. channels to obtain data, rather than skirting legal requirements by turning to foreign partners with less restrictive practices to obtain the same data. For instance, this provision prohibits U.S. agencies from asking a foreign country to collect information about a U.S. person through a request to a company, instead requiring U.S. agencies to go through the established U.S. warrant process to obtain that information.

These new bilateral agreements would augment, not replace, the current MLAT system. Foreign governments could still use the MLAT process for requests that fall outside the parameters of the executive agreement, or if they lack an executive agreement but have an MLAT.

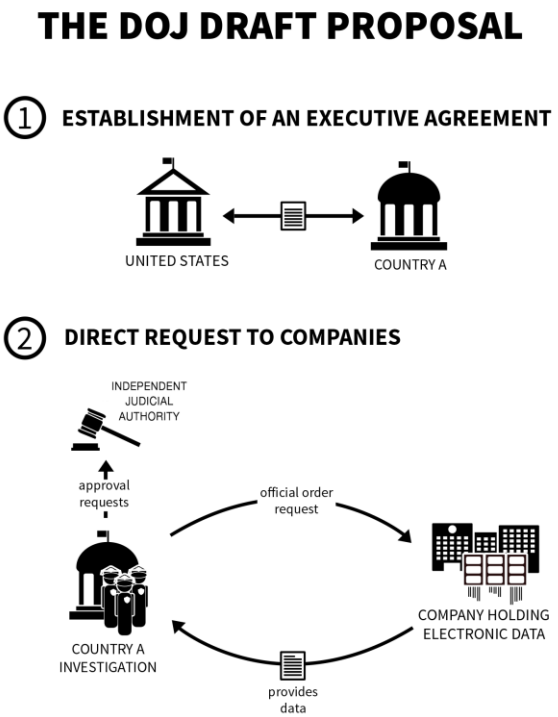


Diagram 2 Diagram of DOJ Cross-Border Data Access Proposal

Stated Benefits of the Draft Proposal

The proposal takes the fairly bold step of providing foreign countries the ability to make requests based on the law of the requesting country rather than U.S. law, and allowing companies the option to respond without penalty under U.S. law. Previous proposals had been much less ambitious, and foreign countries and U.S. companies will likely welcome this significant restructuring of a strained and outdated process. The proposed legislation contains needed limitations on this new process, including restricting requests under this agreement to serious crimes, placing limits on the ability to use this process to obtain information about U.S. persons, requiring a degree of independent oversight of the requests, and prohibiting interception requests with open-ended timelines. For requesting governments, the ability to request both stored and real-time data is an appealing modernization. For responding companies, the proposed legislation does not compel response, it merely removes the legal barriers for responding, still giving companies a high degree of flexibility.

Stated Concerns about the Draft Proposal

Several civil society groups have voiced concerns about the draft proposal. The Center for Democracy & Technology argued the proposal should ultimately be rejected because it lacks adequate civil liberties and privacy protections.[25] Similarly, Human Rights Watch, Amnesty International, and the ACLU released a joint statement urging Congress to reject the proposed legislation.[26] The concerns can be split into three categories: concerns about protections left out of the bill, concerns that the safeguards included in the bill are not strict enough, and concerns regarding the process itself.

Stated Concerns Regarding Missing Protections

- The bill does not provide specific protections for metadata, which concerns actors who consider metadata just as useful to law enforcement and as privacy-invasive as content. Some argue that a court order should be required for the most-sensitive metadata.[27] It also remains to be seen how much companies will be able to push back on bad requests and what procedures of recourse would look like.
- The bill does not mention encryption and whether providers could be subject to compelled assistance that goes beyond U.S. law when dealing with foreign requests. As pro-encryption advocates point out, this bill also does not currently predicate access to data stored by U.S. companies on the requesting country's pro-encryption policy, such as prohibiting partner countries from passing anti-encryption legislation.[28]
- The bill does not require dual criminality. In contrast, the current MLAT process requires dual criminality: a foreign government can only submit a request for data relating to a crime that is illegal both in their country and in the U.S. Some advocates argue that the dual criminality piece is a critical feature, as it creates higher standards for civil liberties globally. Others, argue other countries should not be forced to follow standards that are not their own (provided they have met the requirements of the bilateral treaty).

- The bill lacks structured, explicit oversight over the request and response process. No standard mechanism for companies to challenge requests is included in the draft bill. This lack concerns civil society actors are concerned that requests and responses may push the boundaries of acceptability, given they are not individually subject to scrutiny.
- When striking agreements with other countries, the bill gives the ability to grant agreements solely with the executive branch, unlike the MLAT system, which requires Senate approval for each MLAT, increasing the risk of politicizing the approval process.

Stated Concerns Regarding Reduced Standards

- Regarding evidentiary standards, the bill substitutes the current "probable cause" standard that applies to U.S. MLATs with "reasonable justification based on articulable and credible facts."[29] Some argue that this change could mark a "dramatic elimination of a key civil liberties protection in U.S. law,"[30] as foreign states would no longer be required to meet U.S. evidentiary standards, which are generally considered the highest in the world, to request data.
- The bill does not enumerate specific requirements for qualifying for an executive agreement, but rather "factors" or "conditions" to be considered (e.g., meeting international human rights obligations, respect for rule of law). Civil society would prefer defined requirements that restrict the U.S. government's ability to grant agreements based on politics.
- The bill allows foreign governments to submit requests for real-time surveillance, a change from the current MLAT system, which focuses on stored communications.

Other Stated Concerns and Looking Ahead

Key tensions exist in the proposed legislation. As the U.S. looks to include more countries in the program, how will it handle potential political retaliation from countries who fall short of the program's criteria? Countries that are not even close to qualifying under the terms of the proposed legislation will also likely continue to deal with frustrating cross-border data access issues and may continue to push back. So, troubling practices such as data localization may continue in certain regions, despite major efforts to solve the problem.[31] More reform – and more creativity – regarding the MLAT process may be required to address the concerns and possible retaliations of countries who will miss out on the new agreements. Such changes could include modernization of the current process, such as building an electronic submission system, and improved funding of the existing process. A second-tier agreement allowing more restricted access to countries that do not meet all of the proposed standards may also be worth considering.[32]

However, even with the concerns noted above, the proposed legislation could be a huge step forward in updating an outdated system that was not designed for the today's technological paradigm and was not built for such a high volume of requests. Academics who have worked on the bill, including Jennifer Daskal and Andrew Woods, have also recognized many of these concerns, but they call for revision and iteration, not rejection, of the draft proposal.[33] Indeed, without any changes to the current system, countries will likely feel pushed to implement more troubling means of accessing the data they seek. Cross-border data access reform provides a

potential opportunity: by creating a system that both relieves the burdens on foreign law enforcement and U.S. companies and simultaneously act as a standard-raising mechanism for due process in other countries, the reform effort has the distinct possibility of making forward progress along all fronts.

---

[1] Jennifer Daskal, "Preview: Senate Judiciary Committee Hearing (5/24) on Cross-Border Access to Data," *Just Security*, May 23, 2017, https://www.justsecurity.org/41311/preview-sen-judiciary-committee-hearing-524-cross-border-access-data/.

[2] U.S. Department of Justice, "Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism," July 15, 2016 [hereafter "Proposed Legislation"], https://www.documentcloud.org/documents/2994379-2016-7-15-US-UK-Biden-With-Enclosures.html#document/p1.

[3] If a country lacks an MLAT with the U.S. – or if the MLAT is not used for other reasons – pursuing evidence using Letters Rogatory is the typical alternative.

[4] Proposed Legislation, *supra* n. 2.

[5] "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," Dec. 12, 2013, https://perma.cc/C4RA-NYL8.

[6] Electronic Communications Protections Act, 18 U.S.C. §§ 2701 et seq.

[7] 18 U.S.C. § 2702(d). In 2015, Microsoft responded to requests for contents of email 45 minutes after the Charlie Hebdo attacks. It did so similarly after the November 2015 Paris attacks. Dina Bass, "Microsoft Got 14 Data Requests on Paris Suspects, Smith Says," *Bloomberg*, March 1, 2016, https://www.bloomberg.com/news/articles/2016-03-01/microsoft-got-14-data-requests-on-paris-terrorists-smith-says.

[8] 18 U.S.C. §§ 2702(c)(6), 2711(4). *See also* David Kris, "Preliminary Thoughts on Cross-Border Data Access," *Lawfare*, September 28, 2015, https://www.lawfareblog.com/preliminary-thoughts-cross-border-data-requests#_edn59.

[9] 18 U.S.C. § 2511.

[10] The 1986 House Judiciary Committee Report states that provisions "regarding access to stored wire and electronic communications are intended to apply only to access in the territorial U.S." H.R. Rep. No. 99-647, at 32-33 (1986).

[11] *See* Vivek Krishnamurthy, "Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters," *Berkman Klein Center Research Publication No. 2016-3* (February 18, 2016), https://ssrn.com/abstract=2733350; Urs Gasser, "Cloud Innovation and the Law: Issues, Approaches, and Interplay," *Berkman Center Research Publication No. 2014-7* (March 17, 2014), https://ssrn.com/abstract=2410271.

[12] U.S. Department of Justice, "FY 2015 Budget Facts Sheet," 2015, https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

[13] *See e.g.*, Jenny Gross and Alexis Flynn, "U.K. Proposal Would Expand Government's Power of Surveillance," *The Wall Street Journal*, November 4, 2015, http://www.wsj.com/articles/u-k-announces-overhaul-to-laws-governing-surveillance-powers-1446649497; Rachel Pick, "A Look at France's New Surveillance Laws in Wake of the Paris Attacks," *Vice – Motherboard*, November 15, 2015, http://motherboard.vice.com/read/a-look-at-frances-new-surveillance-laws-in-the-wake-of-the-paris-attacks.

[14] *See* Stephen Dockery, "Data Localization Takes Off as Regulation Uncertainty Continues," *The Wall Street Journal*, June 6, 2016, http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off- as-regulation- uncertainty-continues/.

[15] *See* Jennifer Daskal, "Statement to the 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, https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Daskal%20Testimony.pdf.

[16] *See e.g.*, "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," Dec. 12, 2013, https://perma.cc/C4RA-NYL8; Vivek Krishnamurthy, "Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal

Assistance Treaty System and Why It Matters," *Berkman Klein Center Research Publication No. 2016-3* (February 18, 2016), https://ssrn.com/abstract=2733350; Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age," *Harvard National Security Journal Online* (Jan. 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age; Global Network Initiative, "Data Beyond Borders: Mutual Legal Assistance in the Internet Age," Jan. 29, 2015, http://globalnetworkinitiative.org/content/data-beyond-borders-mutual-legal-assistance-internet-age.

[17] "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies," Dec. 12, 2013, https://perma.cc/C4RA-NYL8.

[18] *See* Mike Masnick, "Brazil Arrests Facebook Exec Because Company Refuses to Reveal Info On Whatsapp Users," *Techdirt*, March 16, 2016, https://www.techdirt.com/articles/20160301/11324333773/brazil-arrests-facebook-exec-because-company-refuses-to- reveal-info-whatsapp-users.shtml. Questions about the territoriality of data also play a role here. Should territoriality be decided upon where the data is stored, the principle place of business of the company, or the nationality of the individual whose data is being considered? In the recent Microsoft v. United States case, the Second Circuit ruled that the Stored Communications Act does not authorize the U.S. government to compel Microsoft, a U.S. company, to produce data stored only on servers in Ireland. In June 2017, the DOJ petitioned the U.S. Supreme Court for writ of certiorari, which as of this writing remains pending. *See* Joe Uchill, "DOJ applies to take Microsoft data warrant case to Supreme Court," The Hill, June 23, 2017, http://thehill.com/policy/cybersecurity/339281-doj-applies-to-take-microsoft-data-warrant-case-to-supreme-court; Nora Ellingsen, "The Microsoft Ireland Case: A Brief Summary," *Lawfare*, July 15, 2016, https://www.lawfareblog.com/microsoft-ireland-case-brief-summary.

[19] Reform Government Surveillance Group, "RGS Statement on US-UK Data Protection Discussions," July 15, 2016, http://reformgs.tumblr.com/post/147464333157/rgs-statement-on-us-uk-data-protection-discussions.

[20] Proposed Agreement, *supra* n. 2.

[21] *See e.g.*, Jennifer Daskal and Andrew K. Woods, "Cross-Border Data Requests: A Proposed Framework," *Just Security*, November 24, 2015, https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/; Peter Swire and Justin D. Hemmings, "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program," *NYU Annual Survey of American Law*, vol. 71 (2017), pp.687-800, https://annualsurveryofamericanlaw.files.wordpress.com/2017/04/71-4_swirehemmings.pdf; Greg Nojeim, "MLAT Reform: A Straw Man Proposal," *Center for Democracy & Technology*, Sept. 3, 2015, https://cdt.org/insight/mlat-reform-a-straw-man-proposal/.

[22] Proposed Agreement, *supra* n. 2, §§ 3(a)-3(c).

[23] *Ibid*., § 4(a).

[24] *Ibid*., §§ 4(a)(1)(xii), (xiii).

[25] Center for Democracy & Technology, "Cross-Border Law Enforcement Demands: Analysis of the US Department of Justice's Proposed Bill," Aug. 17, 2016, https://cdt.org/files/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf.

[26] ACLU, Amnesty International, and HRW, "RE: Department of Justice Proposal on Cross Border Data Sharing, Amending the Electronic Communications Privacy Act and the Wiretap Act," Aug. 9, 2016, https://www.aclu.org/letter/aclu-amnesty-international-usa-and-hrw-letter-opposing-doj-proposal-cross-border-data-sharing.

[27] *See* Chris Calabrese, Statement to the U.S. House Committee on the Judiciary, *Hearing on Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era* (June 15, 2017), https://judiciary.house.gov/wp-content/uploads/2017/06/Calabrese-Testimony.pdf.

[28] *See* Jennifer Daskal. Statement to the 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), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Daskal%20Testimony.pdf.

[29] Proposed Agreement, *supra* n.2, § 4(a)(3)(vii).

[30] Center for Democracy & Technology, "Cross-Border Law Enforcement Demands: Analysis of the US Department of Justice's Proposed Bill," Aug. 17, 2016, https://cdt.org/files/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf.

[31] *See* Mailyn Fidler, "Africans Want Cross-Border Data Access Reform But They Might Get Left Out," *Net Politics*, October 26, 2016, http://blogs.cfr.org/cyber/2016/10/26/africans-want-cross-border-data-access-reform-but-they-might-get-left-out/.

[32] *See* Peter Swire and Deven Desai, "A 'Qualified SPOC' Approach for India and Mutual Legal Assistance," *Lawfare*, March 2, 2017, https://www.lawfareblog.com/qualified-spoc-approach-india-and-mutual-legal-assistance.
[33] Jennifer Daskal and Andrew K. Woods, "Congress Should Embrace the DOJ's Cross-Border Data Fix," *Just Security*, August 1, 2016, https://www.justsecurity.org/32213/congress-embrace-dojs-cross-border-data-fix/.