GPPi
GLOBAL PUBLIC POLICY INSTITUTE

# System Upgrade

## Improving Cross-Border Access to Electronic Evidence

By MIRKO HOHMANN, SOPHIE BARNETT

POLICY BRIEF
January 2019

The existing international system of mutual legal assistance (MLA) has become too slow and cumbersome for law enforcement officers to keep up with increasing criminal activity online. The system of cross-border access to electronic evidence needs to be reformed, otherwise states may move ahead with their own national initiatives to access data, such as data localization measures. Building a sustainable regime will require working on two fronts: First, improve, rather than abandon, the existing MLA regime. Second, establish an effective, parallel system – among like-minded nations – that provides authorities in different countries with direct access to a company's data.

## Acknowledgements

This policy brief was produced as part of the Transatlantic Digital Debates (TDD) 2018 program. Microsoft Deutschland GmbH provided financial support for research for this paper as part of their support for the TDD program. The views expressed in the paper are those of the authors.

The authors thank all the TDD fellows for fruitful discussions on this topic during the program; Guido Brinkel for his input; Marc Lendermann for sharing his expertise and providing input to the brief; Thorsten Benner and Jill Toh for their help throughout the process of creating it; and Katharina Nachbar and Stephanie Le Lièvre for editing, proofreading and design.

# Contents

# Executive Summary

Over the past decades, criminals have picked up on new technologies to organize, plan and carry out illegal activity online. Unfortunately, law enforcement officers and the legal frameworks in which they operate have struggled to keep up with these changes. Increasingly, those working in law enforcement find themselves in jurisdictions different to those in which the electronic evidence they need is located, with no effective way to seek cross-border access to the data.

The current system of mutual legal assistance (MLA) – which predates the rise of the Internet – is not built for and thus currently fails to address these challenges, mainly because it is slow, cumbersome and asymmetric. Given that data is increasingly central to 21st century criminal investigations, governments from around the world are growing more and more frustrated with the existing regime. Without MLA reform, states will likely move ahead with their own national initiatives to access user data, including measures like forced data localization or government-sponsored hacking. Such approaches can threaten user rights and hurt businesses.

Recently, both American and European lawmakers have responded to this problem by passing (in the case of the US) or proposing (in the case of Europe) new legislation: the CLOUD Act and the E-Evidence Initiative, respectively. Remarkably, both of the initiatives deviate from the principle of territoriality, the long-standing doctrine that the physical location in which data is stored should determine the jurisdiction over it that has guided cross-border access to information for decades. Instead, they suggest that – in specific cases – law enforcement officers in one jurisdiction should be able to directly access data from a company located in another jurisdiction. Neither of the two initiatives seeks to upend the MLA system, but both propose to add a mechanism for quicker access among a small selection of trusted states.

We argue that these efforts are a positive step in the right direction, but the current MLA system – on which all states will continue to rely – should remain the starting point for reform. To reform the MLA system, it is necessary to:

- Increase the funding available to agents handling MLA requests;
- Educate staff;
- Digitalize the submission process;
- Establish clear guidelines for both the private sector and states issuing requests;
- Improve transparency.

Concurrently, when establishing a system of direct access among trusted states, policymakers in the United States and the European Union (EU) should:

- Ensure high substantive as well as procedural standards;
- Be restrictive regarding the number of trusted states;
- Establish a clear nexus of the crimes that qualify as triggers for direct access;
- Provide companies holding sought-after data with the ability to challenge requests;
- Ensure that high transparency standards are embedded within the system.

# Introduction

Just as the spread of the Internet has changed the way billions of users live and work, it has impacted the way law enforcement operates. Most communication now takes place online or in the "cloud," be it via messenger apps, email or voice-over-IP calls. Like everybody else, criminals have adopted these technologies – including to organize, plan and execute illegal activity. As a result, electronic evidence has become crucial for investigating crimes, identifying suspects and convicting perpetrators – in both operations against cyber criminals and crimes in the physical world like drug trafficking.[1]

Unfortunately, an emerging trend has made some electronic evidence harder to come by: as communication infrastructures have globalized, law enforcement officers increasingly find themselves in jurisdictions different to those of the data they seek (and/or the service providers holding it). While criminals quickly move "across borders" – at least online – investigators do not. Their warrants are often limited in reach, and companies are either (technically and/or legally) unable or unwilling to share the content of messages or files with them. This lack of access to user data across borders has eroded the ability of law enforcement agencies to fight and prevent crime.[2]

Cross-border access to information is not an entirely new concept. However, the need for an effective framework to obtain the necessary information has increased dramatically. The current system of mutual legal assistance (MLA), usually taking the form of bilateral mutual legal assistance treaties (MLATs), pre-dates the Internet revolution and has become inadequate to satisfy the needs of law enforcement officers operating in the 21st century. The process is cumbersome, slow and in dire need of reform. If no international solution can be found, states are likely to move ahead with their own initiatives, including forced data localization or government-sponsored hacking to gain access to data. Such approaches can hurt users and businesses alike.

There is little agreement on the kind of system that should replace the current data sharing regime, but both the United States and the European Union (EU) have recently passed (in the case of the US) or proposed (in the EU) new legislation to help law enforcement access data abroad – namely the Clarifying Lawful Overseas Use of Data (CLOUD) Act in the US[3] and the E-Evidence Initiative in Europe.[4] Both seek to redefine

1 Gail Kent, "Sharing Investigation Specific Data with Law Enforcement - An International Approach," The Center for Internet and Society, 2014, accessed July 18, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413.

2 The spread of encryption technologies has also impacted the ability of law enforcement to access data at rest or in transit. A discussion of that particular challenge goes beyond the scope of this paper. It should be noted, however, that access to user data through international sharing arrangements will only gain in relevance as encryption technologies continue to spread.

3 Congress, "S.2383 - CLOUD Act," 2018, accessed July 18, 2018, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

4 European Commission, "E-Evidence," 2018, accessed July 18, 2018, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

the processes through which law enforcement agencies can access data located outside of their jurisdiction, thus challenging existing assumptions of sovereignty. Given the relevance of the US and EU in terms of market size and the companies incorporated in both regions, these efforts will likely shape international standards and therefore deserve close attention.

The purpose of this policy brief is to highlight the implications of these new efforts and make recommendations for shaping a sustainable regime for cross-border data access. First, we outline the existing system and its shortcomings. We then take a closer look at the CLOUD Act and the E-Evidence Initiative to analyze the implications of both approaches. Finally, we make recommendations for how to shape the system for cross-border data access, including ways to improve the existing MLA regime and how the US and European legislative efforts can be implemented.

# The MLA Regime: A Multi-Jurisdictional Headache

> "MLATs have not been designed [...] to facilitate ongoing investigations on a day to day basis. They never have been, and it would be very difficult to turn them into that."
>
> Charles Farr[5]

> "The MLAT process is needlessly lengthy [...] and it is unpredictable. The police dislike it, privacy advocates dislike it, and so should you."
>
> Andrew K. Woods[6]

Over the last decades, online communication for both legitimate and illegitimate purposes has spread globally. As a result, a majority of criminal investigations now rely on communications data as a key source of information.[7] Given the global nature of today's digital infrastructures, it is unlikely that all information relevant to a particular investigation can be found residing with a domestic service provider and on domestic servers. As a result, law enforcement agencies increasingly need to access digital evidence from service providers in other jurisdictions.

If law enforcement officers in one country, for example in Germany, seek communications data from a service provider in another country, such as the US, there are currently three[8] different methods to request and receive that evidence:[9]

1. **Voluntary disclosure:** The US provider may share certain information about its users without a legal obligation to do so. However, these ad-hoc agreements are limited in scope. Not only are communications providers concerned that

5 UK Parliament, "Draft Communications Data Bill - Draft Communications Data Bill Joint Committee Contents," 2012, accessed July 8, 2018, https://publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7909.htm.

6 Andrew K. Woods, "Why Does Microsoft Want a Global Convention on Government Access to Data?," *Just Security,* February 19, 2014, accessed July 18, 2018, https://www.justsecurity.org/7246/microsoft-global-convention-government-access-data/.

7 Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age," *Harvard Law School National Security Journal*, January 28, 2015, accessed July 18, 2018, http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/.

8 In theory, "letters rogatory" are a fourth option. In these cases, a court in Germany would directly approach a court in the US to request information. The letters have mostly been replaced by MLA procedures. See Drew Mitnick, "The urgent need for MLAT reform," Access Now, September 12, 2014, accessed July 18, 2018, https://www.accessnow.org/the-urgent-needs-for-mlat-reform/.

9 Mitnick, "The urgent need for MLAT reform." See also Kent, "Sharing Investigation Specific Data with Law Enforcement."

their customers may negatively perceive such sharing of data with law enforcement – there are often legal limitations as to what they can share. In the case of US providers, the Electronic Communications Privacy Act of 1986 prohibits the sharing of content data with non-US law enforcement agencies.[10] This blocking statute does not affect subscriber data and metadata (i.e., information about who the subscriber is communicating with), yet clearly limits what a provider may share.[11] In addition, voluntary disclosure leaves the respective company room for interpretation, creating an unsatisfactory situation for all parties involved.

2. **Law enforcement cooperation:** If law enforcement agencies from different jurisdictions work on a case together, they can share additional information among each other. However, for joint investigations to take place with US law enforcement, there needs to be a clear US dimension to the case.[12] Such a dimension might exist in international investigations like those regarding the distribution of child pornography, but not in, for example, a local murder case. This makes law enforcement cooperation a rare solution to the problem.

3. **Mutual legal assistance:** The most common – and legally robust – mechanism for sharing evidence across borders is through mutual legal assistance, usually based on a treaty (an MLAT) between two countries (or, as in the case of the EU, regional organizations). MLA not only allows for sharing the content of communications, but can also include search and seizure procedures or the confiscation of proceeds of a crime, to name two examples.[13]

10 Kate Westmoreland, "ECPA reform is not just a U.S. issue," The Center for Internet and Society, April 10, 2014, accessed July 18, 2018, http://cyberlaw.stanford.edu/blog/2014/04/ecpa-reform-not-just-us-issue. The ECPA makes an exception on the sharing of content data in cases of "danger of death or serious physical injury to any person." See also Legal Information Institute, "U.S. Code," Cornell Law School, 2018, accessed July 18, 2018, https://www.law.cornell.edu/uscode/text/18/2702.

11 Kent, "Sharing Investigation Specific Data with Law Enforcement."

12 Gail Kent, "The Mutual Legal Assistance Problem Explained," The Center for Internet and Society, February 23, 2015, accessed July 18, 2018, http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained.

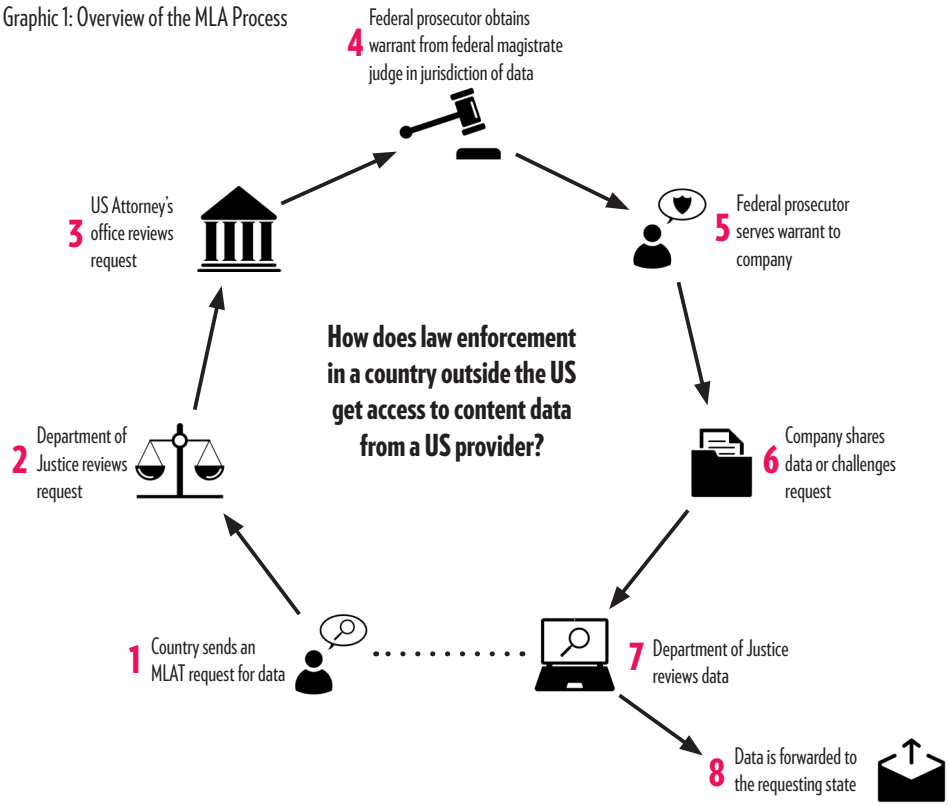
13 Kent, "Sharing Investigation Specific Data with Law Enforcement."

## The Problem With Mutual Legal Assistance

The MLA regime in its current form is slow and cumbersome, and still not universal.

The most pressing problem is the slow process. It takes an average of 10 months for US agencies to process a request, and can take up to several years.[14] Graphic 1 depicts the steps that a non-US law enforcement officer has to go through to access content data from a US provider.[15] In order to start the process, officers need to work with domestic prosecutors and justice agencies – such as the German Federal Office of Justice – to send a letter requesting the relevant data to the Office of International Affairs (OIA) at the US Department of Justice (DOJ). If the DOJ approves the request, it is sent to the respective US Attorney, who in turn approaches the company in question with a subpoena or court order. Once the company has shared the relevant data, the DOJ reviews and, where appropriate, minimizes its contents – removing information that is irrelevant to the purpose of the data request – before forwarding it to the requesting state. Few of these steps occur electronically.

Graphic 1: Overview of the MLA Process




14 Hill, "Problematic Alternatives."

15 Alan McQuinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders," Information Technology and Innovation Foundation, July 2017, 2018, accessed July 2018, https://itif.org/publications/2017/07/24/how-law-enforcement-should-access-data-across-borders. See also Woods, "Why Does Microsoft Want a Global Convention on Government Access to Data?"

The goal of this complex process is to ensure that countries do not approach companies located in other jurisdictions with unlawful requests. However, without the necessary reforms to modernize the MLA system, the realities of digitization and the growing demand for data as evidence in investigations places more and more pressure on the authorities to handle requests in a reasonable time frame. This is especially the case in the US, where most of the major technology companies are based, and where the "number of requests for computer records has increased ten-fold" over the past decade.[16]

In addition to the slow process, there is a strong asymmetry in the demand for and supply of data. As previously mentioned, the US is currently home to most of the key technology companies from which law enforcement officers around the world seek data. In the current system, it would be up to the US to invest in additional resources, such as more staff, in order to speed up the process – but the incentives to do so are low. Concurrently, MLA coverage is not global: the US has signed Mutual Legal Assistance Treaties (MLATs) with just over sixty, mainly Western, states, leaving the remaining countries with only limited options to access data from US service providers.[17]

Another challenge is the difference in legal regimes between states. For a request to be approved by the DOJ, it must meet US legal standards. However, there is often a "lack of legal understanding of the standards and processes in foreign jurisdictions."[18] Without such understandings, requests can be denied after months of review, exhausting already strained resources on both sides.

## Consequences and Implications

For the aforementioned reasons, Andrew Woods at the University of Arizona College of Law has called the current MLA regime "a multi-jurisdictional headache."[19] This headache not only hinders effective investigations, causing victims unnecessary harm, but has broader implications for Internet policymaking: if governments are unable to access the requested data via the existing system, they are likely to work around it by creating alternatives to achieve access. However, such alternatives have the potential to threaten user rights and negatively impact businesses.[20] The most common example is the passage of data localization legislation, which forces businesses to store data within a country's territory to facilitate direct access and avoid the need for international assistance altogether. (Box 1 provides an overview of this challenge.) Furthermore, since encryption is also rendering data inaccessible to law enforcement agencies, it is likely that governments will introduce additional legislation forbidding encryption

16 Hill, "Problematic Alternatives."

17 McQuinn and Castro, "How Law Enforcement Should Access Data Across Borders."

18 Mitnick, "The urgent need for MLAT reform."

19 Woods, "Why Does Microsoft Want a Global Convention on Government Access to Data?"

20 Jennifer Daskal and Andrew K. Woods, "Cross-Border Data Requests: A Proposed Framework," *Just Security,* November 24, 2015, accessed July 18, 2018, https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/.

technologies or forcing companies to provide access.[21] Another path for governments to access data is through hacking directly into either the potential perpetrators' devices or the servers of the companies that are holding the information stored on it. Finally, the lack of clear (international) processes has put technology companies on the spot: not only are they faced with conflicting legal obligations in the different jurisdictions in which they operate (which creates legal uncertainty), they must also make judgements about how to interpret those laws and become the arbiter between governments and users, a role that has traditionally – and for good reasons – been allocated to courts.

It is clear that the current system is untenable. Without a solution to the problems outlined above, countries will assert their authority to obtain data in forms that threaten the security of users and businesses alike.[22] Without coordination at a global level, different national or regional solutions will be developed, threatening the interconnected and integrated nature of the Internet.

21 See for example: Jamie Tabaray, "Australia Government Passes Contentious Encryption Law," New York Times, December 6, 2018, accessed December 21, 2018, https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.

22 Mitnick, "The urgent need for MLAT reform."

## Box 1: Data Localization

At their core, data localization requirements are an instrument to control where and how data is stored as well as by whom. They often take the form of laws and regulations that limit "the storage, movement, and/or processing of data to specific geographies and jurisdictions" as well as "the companies that are legally permitted to manage data based upon the company's country of incorporation or principle situs of operations and management."[23]

Data localization policies are not monolithic. They can be sector-specific, such as the Reserve Bank of India's directive, which requires foreign payment firms to store financial information in India,[24] or much broader, like Indonesia's Government Regulation No. 82 that requires "electronic systems operators for public service" to set up data and disaster recovery centers in Indonesia for the purpose of law enforcement and data protection.[25] The US has long required that sensitive government data be stored on domestic companies' servers.[26]

Data localization is not a new phenomenon,[27] but the push to keep data "at home" gained new momentum following the Snowden disclosures in 2013, which renewed pressure on governments to protect their citizens and businesses from perceived threats to national security and user privacy.[28] Importantly, the relationship

23 Jonah Force Hill and Matthew Noyes, "Rethinking Data, Geography, and Jurisdiction: Towards a Common Framework for Harmonizing Global Data Flow Controls," New America, February 22, 2018, accessed July 18, 2018, https://na-production.s3.amazonaws.com/documents/Rethinking_Data_Geography_Jurisdiction_2.21.pdf.

24 Aditi Shah and Aditya Kalra, "Exclusive: India proposes easing local data storage rules for foreign payment firms - document," *Reuters*, July 11, 2018, accessed July 18, 2018, https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-india-proposes-easing-local-data-storage-rules-for-foreign-payment-firms-document-idUSKBN1K1240.

25 Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel and Bert Verschelde, "The Costs of Data Localization: Friendly Fire on Economic Recovery," European Centre for International Political Economy, 2014, accessed July 18, 2018, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

26 Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," Lawfare Research Paper Series 2, no. 3 (2014): p. 3, accessed July 18, 2018, https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf.

27 *ibid.*

28 Konstantinos Komaitis, "The 'wicked problem' of data localisation," *Journal of Cyber Policy* 2, no. 3 (2017): p. 356.

between major US-based technology firms and the US national security establishment, in which the former were obliged to provide the latter with large-scale access to user data, has led some policymakers to conclude that storing data domestically or prohibiting it from travelling through untrustworthy countries would keep data safe and/or would curtail National Security Agency (NSA) surveillance.[29]

While national security is undoubtedly a key motivation for data localization, economic objectives have also influenced these policies. In particular, they may be rooted in the infant industry argument, meaning the attempt to offer local businesses a chance to gain a competitive advantage in domestic markets historically dominated by US firms. More generally, governments may implement barriers to data flows for the purpose of protecting citizens' jobs and local goods.[30]

Censorship and domestic surveillance are other rationales for localizing data. For authoritarian governments, keeping data at home facilitates not only control of the information that reaches their populations, but also helps monitor citizens' activities and control dissent.[31] China's surveillance apparatus is significantly enabled by the ease with which the Chinese government can access user data, which is usually handled by domestic companies and stored locally. In Russia, in 2014, the Duma approved a draft law requiring foreign Internet companies to store Russian user data inside the country.[32]

Finally, in the absence of meaningful MLA reform, democratic governments may feel compelled to enact data localization regulations to enhance law enforcement access to electronic evidence. If all data on a country's citizens is stored on servers located in the respective country, legal access to such data becomes easier even though foreign companies can still deny access based on their legal interpretation.

---

29 Tim Maurer, Robert Morgus, Isabel Skierka, and Mirko Hohmann, "An Analysis of European Proposals after June 5, 2013," Global Public Policy Institute and New America's Open Technology Institute, November 24, 2014, accessed July 13, 2018, https://www.gppi.net/2014/11/24/technological-sovereignty-missing-the-point.

30 Komaitis, "The 'wicked problem' of data localisation," p. 359.

31 Hill, "The Growth of Data Localization," pp. 26-27.

32 Ewen MacAskill, "Putin calls internet a 'CIA project' renewing fears of web breakup," *The Guardian,* April 24, 2014, accessed July 17, 2018, https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia. See also Hill, "The Growth of Data Localization," p. 16.

# A New Data Access Regime

The key problem of the current MLA regime is its assumption that the physical location of data should dictate who has jurisdiction over that data. This assumption was fair for the time preceding the Internet, and it has guided exchange between law enforcement agencies for decades. Territory-based rules assume that there is an "observable, identifiable, and stable location, either within the territory or without,"[33] and that this location should determine who has jurisdiction over it. However, the global and intangible nature of data challenges these assumptions. Users and their data are rarely in the same jurisdiction, companies can easily move or copy data across borders, and large databases can be split up so that relevant information is stored on different servers in different jurisdictions. The geographical limitations that once guided cross-border law enforcement cooperation are no longer in place, but the legal system governing it remains unchanged.

Recently, this has led to legal disputes, the most well-known being *United States v. Microsoft Corporation*. Although the case was rendered moot after the passage of the CLOUD Act in March 2018, United States v. Microsoft Corp raised the critical issue of whether a US company must comply with a domestic court order to provide emails, even if they are stored abroad. In 2013, US law enforcement agents, as part of a criminal investigation, obtained a warrant for a suspect's emails that was rooted in the 1986 Stored Communications Act (SCA).[34] Microsoft challenged the order because the emails were stored in a facility located in Ireland. The US warrant, the company claimed, lacked extraterritorial reach.[35] Complying with the US warrant order would put Microsoft in the undesirable situation of violating Irish law. Accordingly, they argued, to lawfully obtain access to the requested data, the US government should seek MLA from the Irish government.[36] In contrast, the US government argued that, should Microsoft win, US law enforcement would effectively lose the ability to obtain evidence related to serious crimes, including child pornography and terrorism, and that companies could "shift their data beyond the reach of US authorities by simply moving it out of the country."[37] Ultimately, *United States v. Microsoft Corp* required the US courts to determine whether Congress – in legislation passed in 1986, when the

33 Jennifer Daskal, "The Un-Territoriality of Data," *Yale Law Journal* 125, no. 2 (2015): p. 327.

34 Ellen Nakashima, "Supreme Court to hear Microsoft case: A question of law and borders," *The Washington Post,* February 25, 2018, accessed August 6, 2018, https://www.washingtonpost.com/world/national-security/supreme-court-case-centers-on-law-enforcement-access-to-data-held-overseas/2018/02/25/756f7ce8-1a2f-11e8-b2d9-08e748f892c0_story.html?noredirect=on&utm_term=.790fcef99aa8.

35 Nakashima, "Supreme Court to hear Microsoft case."

36 *ibid.*

37 Louise Matsakis, "Microsoft's Supreme Court Case Has Big Implications for Data," *Wired*, February 27, 2018, accessed August 6, 2018, https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/?mbid=social_twitter_onsiteshare.

very idea of cloud computing was "the stuff of science fiction"[38] – intended the warrant authority to be able to reach data that is stored abroad but controlled by a US company acting domestically.

To address these challenges, stakeholders agree on the need to reform or at least update the MLA regime. However, there is less agreement as to what the reformed system should look like. Ultimately, there are different answers to the question of which factor should determine access to a user's data across borders: it could be the location of the data, the location of the user (her residency and/or nationality), the location of the company (its place of corporation and/or legal presence), or the location of the respective law enforcement agency.[39]

## The US and the EU Lead the Way

Work on a multilateral solution has already begun. In June 2017, the Plenary of the Cybercrime Convention Committee of the Council of Europe started to work on a second additional protocol to the Budapest Convention on Cybercrime that will deal with enhanced international cooperation and access to evidence stored in the cloud.[40] As the Budapest Convention has been ratified by the US, the additional protocol would also be of relevance to US law enforcement authorities. However, it is unlikely that the drafting process will be finished before the end of 2019.

In the meantime, both US and European lawmakers have acted unilaterally by respectively passing and proposing new legislation: the CLOUD Act, which was adopted in the US in early 2018,[41] and the E-Evidence Initiative, which is part of the European Commission's recently proposed new regulation and directive.[42] Box 2 provides an overview of both initiatives.

The CLOUD Act and the E-Evidence Initiative are relevant for two reasons. First, due to the size of the European and American markets, and given that most major technology corporations are based in the US, standards and regulation set there have the potential for broader adoption. Second, both approaches partly deviate from the principle that the physical location in which the data is stored determines jurisdiction. Instead, the CLOUD Act and E-Evidence Initiative suggest that, in specific cases, law enforcement officers should be able to directly access a company's data (if that company is operating in the same jurisdiction) without needing MLA. Neither of the two initiatives seeks to upend the MLA system, but to add an additional process for quicker access between certain nations.

---

38 Jennifer Daskal, "Microsoft Ireland Argument Analysis: Data, Territoriality, and the Best Way Forward," *Harvard Law Review*, February 28, 2018, accessed August 6, 2018, https://blog.harvardlawreview.org/microsoft-ireland-argument-analysis-data-territoriality-and-the-best-way-forward/.

39 Daskal, "The Un-Territoriality of Data," p. 348.

40 Council of Europe, "T-CY Plenaries," 2018, accessed December 21, 2018, https://www.coe.int/en/web/cybercrime/t-cy-plenaries.

41 Congress, "S.2383 - CLOUD Act."

42 European Commission, "Proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final," April 17, 2018, accessed December 21, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN. See also European Commission, "Proposal for a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final," April 17, 2018, accessed December 21, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX-:52018PC0226&from=EN.

## Box 2: The CLOUD Act and the E-Evidence Initiative

### The CLOUD Act

The CLOUD Act was signed into US law on March 23, 2018. It provides legal clarity for law enforcement authorities seeking access data stored abroad.[43] Among other things, it amends the 1986 Stored Communications Act (SCA) to remove a blocking statute, i.e., to allow service providers located in the US to disclose communications content directly to foreign law enforcement authorities in certain circumstances.[44]

In the past, a foreign government investigating a local crime involving its own citizens had to go through the mutual legal assistance (MLA) process to obtain electronic evidence even if the only connection to the US was the place of incorporation of the communications platform used in committing the crime. The reverse was true for the US. To increase the efficiency with which foreign and US governments can lawfully obtain data, the CLOUD Act makes three important changes. First, it expands the jurisdiction of US warrants made under the SCA so they have extraterritorial reach. If the data being sought concerns US "persons" – US citizens and non-citizens residing in the US – and is controlled by an US service provider (but not necessarily stored on an American server), US law enforcement can request data directly from the company in question rather than going through the MLA process.[45]

Second, the CLOUD Act allows the US president to enter into bilateral executive agreements with "qualifying" foreign governments. These agreements are based on reciprocity and pre-authorize other governments to make law enforcement requests directly to service providers incorporated in the US, as long as the data pertains to "serious crimes, including terrorism" and does not concern a US citizen or resident.[46] Executive agreements are intended to reduce the administrative burden of processing foreign MLA requests for data held by US companies, which mainly rests on the Department of Justice (DOJ). To qualify for such agreements, a foreign country must be certified as human rights-compliant by the US Attorney General.[47] Congress then has 180 days to review the agreement. If approved, the foreign government is safe-listed for five years.[48]

Third, the CLOUD Act clarifies the rights of US service providers to challenge law enforcement requests for data. It distinguishes between requests by countries that have an executive agreement with the US versus those that do not. If there is an executive agreement, the company confronted with a request has 14 days to challenge the order in court if it "reasonably believes" that the person whose data is concerned is not a US citizen and does not reside in the US or that disclosure would create a conflict of laws.[49] If there is no executive agreement, the CLOUD Act simply upholds the right of the company to challenge the warrant under common law comity analysis, a fundamental principle of the law of conflicts.[50] In such instances, the court weighs various factors including the importance of the information being requested, the request's level of specificity, whether the information originated in the US, alternative mechanisms to obtain the information, and the US and foreign national interests at stake.[51]

---

43 Stephen P. Mulligan, "Cross-Border Data Sharing under the CLOUD Act," Congressional Research Service, April 23, 2018, accessed December 21, 2018, https://fas.org/sgp/crs/misc/R45173.pdf. See also David Ruiz, "Responsibility Deflected, the CLOUD Act Passes," Electronic Frontier Foundation, March 22, 2018, accessed July 13, 2018, https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes.

44 Robert Loeb, Brian P. Goldman, and Emily S. Tabatabai, "The CLOUD Act, Explained," Orrick, April 6, 2018, accessed July 13, 2018, https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained.

45 *ibid.*

46 Neema Singh Guliani and Naureen Shah, "The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them," *Lawfare*, March 16, 2018, accessed July 13, 2018, https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them#.

47 Guliani and Shah, "The CLOUD Act."

48 Loeb et al., "The CLOUD Act."

49 Camille Fischer, "The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data," Electronic Frontier Foundation, February 8, 2018, accessed July 13, 2018, https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data.

50 Brad Smith, "The CLOUD Act is an important step forward, but now more steps need to follow," Microsoft, April 3, 2018, accessed July 13, 2018, https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/.

51 Loeb et al., "The CLOUD Act."

## The E-Evidence Initiative

On April 17, 2018, the European Commission released the E-Evidence Initiative, a set of proposed rules for obtaining electronic evidence in criminal proceedings.[52] Aimed at alleviating the legal uncertainty generated by differences in EU member state approaches regarding law enforcement access to data in other EU or non-EU countries, the initiative attempts to create a common EU framework.[53] It has two elements: a Directive and a Regulation.[54] The Directive aims to create a "level playing field for all companies offering the same types of services in the EU, regardless of where they are established."[55] It obliges companies that offer services in a member state to establish a legal representation in the EU to "facilitate the receipt of, [and] compliance with enforcement orders to gather electronic evidence on behalf of these service providers"[56] – even if the company's headquarters are located in a third, non-EU country.

The proposed Regulation further expands the reach of member states' enforcement orders by replacing data storage as the determinant for jurisdiction with requirements that the requested data will both be needed for a criminal proceeding and related to the services of a provider operating in the EU.[57] Under the new framework, judicial authorities in one member state would be authorized to issue so-called European Production and Preservation Orders to directly compel a service provider to disclose or preserve electronic evidence for any crime for which the maximum jail sentence is a minimum of three years, "irrespective of the place of data storage."[58] These Production and Preservation Orders would apply to non-content (i.e., subscriber, access or transactional data) as well as content data.[59]

While the Directive clarifies that the proposed legislation will not affect companies' freedom to choose where to store data, the Regulation stipulates that "a service provider who stores data relating to its European users outside of the EU ... will thus have to provide data to European authorities ... unless there is a conflict with a [non-EU] third-country law."[60] In cases where a service provider faces such conflicting obligations, the E-Evidence Initiative includes mechanisms to challenge the request.[61] Importantly, the provider may argue that the disclosure violates a third-country law protecting fundamental rights, national security or other interests.[62]

---

52 European Commission, "Joint Declaration on the EU's legislative priorities for 2018-19," 2017, accessed July 13, 2018, https://ec.europa.eu/commission/publications/joint-declaration-eus-legislative-priorities-2018_en.

53 Eleni Kyriakides, "Digital Free For All Part Deux: European Commission Proposal on E-Evidence," *Just Security*, May 17, 2018, accessed July 13, 2018, https://www.justsecurity.org/56408/digital-free-part-deux-european-commission-proposal-e-evidence/.

54 European Commission, "Proposal for a regulation on European Production and Preservation Orders." See also European Commission, "Proposal for a directive laying down harmonised rules on the appointment of legal representatives."

55 European Commission, "Frequently Asked Questions: New EU rules to obtain electronic evidence," 2018, accessed July 13, 2018, http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm. See also Article 7 of European Commission, "Proposal for a directive laying down harmonised rules on the appointment of legal representatives."

56 Consideration 3 of European Commission, "Proposal for a directive laying down harmonised rules on the appointment of legal representatives."

57 European Commission, "Frequently Asked Questions."

58 European Commission, "Frequently Asked Questions."

59 European Commission, "Frequently Asked Questions."

60 European Commission, "Frequently Asked Questions."

61 Article 15 of European Commission, "Proposal for a regulation on European Production and Preservation Orders." See also Lauren Moxley, "EU Releases e-Evidence Proposal for Cross-Border Data Access," Inside Privacy, May 8, 2018, accessed July 13, 2018, https://www.insideprivacy.com/uncategorized/eu-releases-e-evidence-proposal-for-cross-border-data-access/.

62 Moxley, "EU Releases e-Evidence Proposal."

## Comparison and Implications

The US was facing two problems that it sought to address through the CLOUD Act. First, lawmakers wanted to solve the problems highlighted by the Microsoft case and ensure that US law enforcement can access data on US citizens or residents stored abroad by US companies. Second, they sought to decrease the MLA-induced burden on the DOJ. The CLOUD Act addresses both these challenges, although the latter is closely linked to the US entering into executive agreements with other countries, which it has yet to do.

For the EU, the motivation behind the E-Evidence Initiative was slightly different and related in part to concerns of harmonization within the Union.[63] Currently, there is a hodgepodge of laws governing cross-border data access, both at the supranational level and between EU member states. In fact, the majority of members' national legislation does not allow for law enforcement in one member state to access data from a service provider in another country, and only Spain and France allow domestic service providers to respond directly to foreign law enforcement requests.[64] Additionally, unlike the US, the EU has comparatively few major technology companies incorporated within its borders. Therefore, it demands access more broadly, including from "all providers that offer services in the European Union," whether or not the companies are incorporated there.[65] This broad framing marks a key difference between the E-Evidence Initiative and the CLOUD Act because the SCA, which the CLOUD Act reforms, only applies to service providers incorporated in the US and not those incorporated in other countries that are providing their services in the US. The E-Evidence Initiative goes beyond this in so far as non-European companies would be obligated to comply with EU rules if they offer their services on the European market.

Another difference is that the CLOUD Act lifts the blockade placed by the Electronic Communications Privacy Act in cases of an existing executive agreement and thereby allows companies to voluntarily provide information, while the proposed E-Evidence Initiative considers so-called binding production orders.[66] However, a key similarity between the two approaches is their focus on the locations of the user and the company – rather than that of the data – as the determinant of jurisdiction. Both legislative efforts aim to oblige companies to transfer data, irrespective of the place of storage. As such, they have the potential to infringe on the long-standing principle of territoriality. According to this principle, the jurisdiction to which the data and thus the company holding the data is subject is determined by the data's physical location. This prevents states from enforcing their laws extraterritorially and enabling the infringement of another country's sovereign territory.[67] Instead, both approaches

63 This is made clear in the explanatory memorandum contained in the proposals, for instance the considerations in the draft directive: "In addition, a harmonised approach creates a level playing field for all companies [...]."

64 European Commission, "Questionnaire on improving criminal justice in cyberspace - Summary of Responses," 2016, accessed July 18, 2018, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf.

65 European Commission, "Frequently Asked Questions."

66 Bertrand de la Chappelle, "IGF 2018 - Day 2 - Salle VI - WS #393 CLOUD Act & e-Evidence: implications for the Global South," Internet Governance Forum, 2018, accessed December 21, 2018, https://www.intgovforum.org/multilingual/content/igf-2018-day-2-salle-vi-ws-393-cloud-act-e-evidence-implications-for-the-global-south.

67 Daskal, "The Un-Territoriality of Data," p. 34.

focus on whether a company is active in the market ("law of the place of performance"), whether it is incorporated there, or whether the data is that of a citizen or resident.[68]

The potential consequences of this turn away from a bi- or multilateral system based on territoriality should not be underestimated. After all, the doctrine has long and successfully created trust among the actors involved. Although there are certainly problems with the territoriality doctrine, as shown above, US and European legislators alike should consider thoroughly whether a fundamental shift in the system is beneficial for criminal investigations overall.[69]

An important implication of the unilateral enforcement of laws is the heightened potential for conflicts between the laws of different countries. Any company holding relevant data could face a dilemma in which it can comply either with the production order from the requesting state or with the laws of the state where the data is stored, forbidding compliance with the order.[70] In the case of US-EU relations, the E-Evidence Initiative could require US companies to provide access to data, while the SCA forbids the provision of such access unless there is an executive agreement with the US.[71] At the same time, when US authorities request data stored in the EU, companies may risk breaching the EU General Data Protection Regulation (GDPR).[72] Under Article 48 of the GDPR, any judgment or decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable if it is based on an international agreement, such as an MLAT. Article 46 of the GDPR therefore acts as a "blocking statute" on the European side.

Consequently, companies might be compelled to break one country's laws in complying with those of another. This is not a new phenomenon and both efforts take this challenge into account in that they provide options for judicial review in cases in which a provider believes that a request would undermine fundamental rights or breach a third country's laws.[73]

Another relevant implication of both initiatives is the growing relevance and role, along with responsibilities, of private companies and Internet service providers. This is a somewhat natural trend given that data is increasingly stored with companies, and

---

68 Christoph Burchard, "Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1," *Zeitschrift für Internationale Strafrechtsdogmatik* no. 6 (2018): p. 193, accessed July 18, 2018, http://www.zis-online.com/dat/artikel/2018_6_1206.pdf.

69 Christoph Burchard, "Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2," *Zeitschrift für Internationale Strafrechtsdogmatik*, no. 7-8 (2018): p. 253, accessed July 18, 2018, http://www.zis-online.com/dat/artikel/2018_7-8_1213.pdf.

70 Daskal, "The Un-Territoriality of Data," p. 34.

71 It remains unclear whether the EU as a whole is even able to enter into executive agreements with the US as part of the CLOUD Act, potentially forcing all EU member states to enter into such agreements bilterally. See Jennifer Daskal and Peter Swire, "A Possible US-EU Agreement on Law Enforcement Access to Data?," *Just Security,* May 21, 2018, accessed December 21, 2018, https://www.justsecurity.org/56527/eu-agreement-law-enforcement-access-data/.

72 Tina Gausling,"Offenlegung von Daten auf Basis des CLOUD Act - CLOUD Act und DS-GVO im Spannungsverhältnis", MultiMedia und Recht 2018, accessed December 22, 2018, https://www.beck-shop.de/mmr-multimedia-recht/productview.aspx?product=1584. See also Michael Rath and Axel Spies, "CLOUD Act: Selbst für die Wolken gibt es Grenzen," Corporate Compliance Zeitschrift no. 5 (2018): p. 229, https://www.luther-lawfirm.com/fileadmin/user_upload/PDF/Veroeffentlichungen/2018_CCZ_05_Rath_Spiess_CLOUD_Act.pdf.

73 § 2703 (h) (2) U.S.C. allows for a "motion to quash or modify." Similarly, chapter 4 of the proposal for the EU E-Evidence Regulation foresees a review procedure.

law enforcement officers seek such data more regularly as part of their investigations. Yet while the private sector receives requests for data in traditional MLA procedures through domestic authorities, it would need to vet the requests from foreign authorities around the world under an effective regime as envisioned in the CLOUD Act. There is a risk in privatizing legal assistance, because companies will follow their own guidance and establish their own mechanisms for evaluating such requests, which are neither wholly transparent nor determined in democratic processes.[74]

A final implication is that the approaches will lead to the creation of a system of clubs between countries that is likely to be even smaller than that between the current MLA countries. As mentioned above, the US currently works with approximately sixty nations through the MLA regime, already excluding two-thirds of the world's states from access to data that is held with US companies – unless those countries pass domestic legislation, such as data localization laws, to force companies to share data, thus putting them in the position to comply with either the US' or third country's laws. Since the bilateral agreements as envisioned through the CLOUD Act provide increased access, the signatories will be selected more rigorously and such agreements are likely to only come into effect with a handful of democratic nations. As such, their exclusivity is unlikely to ease the tensions outside this small club of states that have mutually agreed to provide access to the data that is stored with their companies.

74 Burchard, "Teil 2," p. 259.

# Shaping the Data Access System

Two things are clear: first, the current MLA regime is ineffective and in need of fixing; and second, a new, parallel system of data access that is not based on the principle of territoriality is emerging among like-minded nations. Building a sustainable access regime will require working on both of these aspects. First, it is necessary to improve – rather than abandon – the existing MLA regime. This system follows traditional legal practices and will remain the primary way to access data for the majority of countries. Second, however, all actors must ensure that the parallel system providing authorities in different countries with direct access to a company's data is effective and sustainable in the long term. The next section suggests next steps for both of these aspects.

## The Necessary Starting Point: MLA Reform

A reform of the MLA regime is a necessary starting point to relieve some of the pressure that has built up in the existing system. It is also the only way to address problems affecting more than just a small handful of countries.

A number of key principles serve as guidelines for several, more specific recommendations outlined below. Based on conversations with stakeholders from all sectors, Andrew Woods proposes five principles for MLA reform:[75]

- A country's MLA request must be justified and the level of assistance the country enjoys should be proportional to the country's interest in the data;
- Reforms must encourage respect for human rights (protecting user privacy, narrowly tailoring how much data is requested/transmitted, etc.);
- Reforms must increase the transparency of the existing MLAT regime;
- Reforms must significantly increase the efficiency of the existing MLAT regime;
- Reforms must be scalable in order to manage increasing government requests.

Several specific recommendations flow from implementing these principles.[76] These are outlined in the subsequent section.

75 Andrew K. Woods, "Data Beyond Borders: Mutual Legal Assistance in the Internet Era," Global Network Initiative, 2015, accessed July 18, 2018, https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1517&context=law_facpub.

76 Hill, "Problematic Alternatives."

## Increase Funding and Educate Staff

When looking at the slow MLA process, particular attention must be paid to problems with both the country requesting the data as well as the one receiving the request. In the current system, there is a disproportionate burden placed on the US for increasing the efficiency of the MLAT process via increased funding and more staff. The reality remains that "insufficient resources are [the] key cause of MLAT backlogs"[77] and the US should therefore consider investing in additional staff to process such requests.[78] At the same time, requesting states should also consider action in two areas. First, they should provide financial support to the US for staff increases. This would, in turn, increase the incentives to invest more in the OIA and take positive steps to speed up the MLA process on the American end. Without such cooperation, there will be few incentives for the US to dedicate valuable resources solely to help other countries. Second, these other states should invest more heavily in educating their own law enforcement officers on how to properly engage with the MLA system, especially to better understand the particular standards and requirements of the US legal system (which often has a higher legal standard for producing data than the requesting state).[79] This involves building the national capacity to craft appropriate requests for data that can actually be lawfully accessed.[80] As a result, requests could be reviewed more quickly and perhaps rejected less often.

## Digitalize the MLA Process

While most of the resources involved in the MLA process are spent on producing digital evidence, the current system does not capitalize on the efficiency that digital solutions offer. Instead of submitting requests via paper, fax, or email, governments should establish an online system that allows countries to make such requests and holds all the relevant information for requesting authorities in one place.[81] Such a system would not only streamline the process of submitting and responding to requests; it can also serve to keep an overview on the status of requests. And it does not need to be a global solution, but could first be used by individual states as a way to save their own officers time and effort.

77 Hill, "Problematic Alternatives."

78 Woods, "Data Beyond Borders."

79 Access Now, "Discussion Paper - What are Solutions to the "MLAT Problem"?," n.d., accessed July 18, 2018, https://www.mlat.info/policy-analysis-docs/discussion-paper-what-are-the-solutions-to-the-mlat-problem.

80 Woods, "Data Beyond Borders."

81 Hill, "Problematic Alternatives." See also: Access Now, "Discussion Paper."

### Establish Clear Guidelines for the Private Sector

Given the growing relevance of the private sector in passing cloud data about customers on to government officials – potentially directly to officials from another country – there is a need for greater clarity on how companies should handle such requests. To begin with, companies should clearly outline what kind of data they hold and through which processes that data can be accessed. To help government officials access data from different companies, the technology industry could further develop a consensus on how to interpret requests "and the way in which they exercise their discretion as to when, how, and under what conditions user information is provided."[82] To improve cooperation with foreign governments, it is helpful to establish clear points of contact so that law enforcement officers know whom to approach with their requests. Some technology companies have already started working on portals that law enforcement officers can then use to submit and track requests. Such solutions can help make the overall process more efficient.[83]

### Improve Transparency

A final point is transparency. To begin with, the industry-wide policies mentioned above should be published in a way that allows the public to understand how decisions on law enforcement access to user data are made. Additionally, companies should continue to expand their transparency reports regarding the number and type of data requests they receive from (foreign) governments, and how many and which kind they approve. For companies that have reached a certain size or number of users, governments should make such reports mandatory. Similarly, governments should regularly publish the number of requests they have made and the responses they have received from the private sector.

## Making the CLOUD Act and the E-Evidence Initiative Work

As mentioned above, both the US CLOUD Act and the EU's E-Evidence Initiative deviate from the long-held doctrine of territoriality as the main principle guiding the exchange of information between governments and companies in different countries. The decision to abandon such a long-standing principle should not be taken lightly since it can affect the trust between stakeholders and carry unexpected ramifications. Most importantly, if the EU moves forward in demanding access from all companies that provide services in its territory, more and more states – democratic or not – will demand such access, too. In doing so, they will likely point to EU law as a basis (and they might not include the paragraph that third countries' laws should not be breached through such demands). There is still a consensus among relevant scholars and stakeholders

82 Access Now, "Discussion Paper."

83 Ali Breland, "Apple to create portal for law enforcement data requests," *The Hill,* November 9, 2018, accessed December 21, 2018, https://thehill.com/policy/technology/406045-apple-to-create-law-enforcement-portal-for-data-requests.

that a new system is necessary,[84] but the quest for perfection should not be "the enemy of the good."[85] As such, the goal should be to make the CLOUD Act and the E-Evidence Initiative work, and to render them as compatible as possible. The following ideas can help do so.

## The CLOUD Act

Several experts have created extensive lists of recommendations regarding the implementation of the CLOUD Act,[86] which we do not seek to reproduce here. Instead, we highlight four points that seem the most relevant to us. To do so, it make sense to first take a closer look at the kind of system that the CLOUD Act is trying to establish, namely a framework:

- "[...W]ith high substantive and procedural standards,
- Allowing relevant authorities from specific countries,
- In investigations regarding certain types of crimes with clear nexus with the requesting country,
- To directly submit structured and due process-respecting requests,
- To private companies in another country to obtain the voluntary disclosures
- Of user data, irrespective of where such data is stored." [87]

Apart from the fact that data requests under this framework would not be voluntary from the perspective of private companies, these criteria appear to fit the current system well (assuming that bilateral executive agreements come into place), and they can therefore help to better understand where to pay close attention.

84 Greg Nojeim, "MLAT Reform: A Straw Man Proposal," Center for Democracy and Technology, September 3, 2015, accessed July 18, 2018, https://cdt.org/insight/mlat-reform-a-straw-man-proposal/. See also Daskal and Woods, "Cross-Border Data Requests;" Google, "Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era," 2017, accessed July 18, 2018, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf; Smith, "The CLOUD Act;" and Vivek Krishnamurthy, "Cloudy with a Conflict of Laws," Berkman Klein Center for Internet & Society, 2016, accessed July 18, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733350.

85 Jennifer Daskal and Peter Swire, "Why the CLOUD Act is Good for Privacy and Human Rights," *Lawfare*, March 14, 2018, accessed July 18, 2018, https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

86 Peter Swire and Justin Hemmings, "Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act," *Lawfare*, September 13, 2018, accessed July 18, 2018, https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act. See also Daskal and Woods, "Cross-Border Data Requests" and Jennifer Daskal and Peter Swire, "Suggestions for Implementing the Cloud Act," *Lawfare*, April 30, 2018, accessed July 18, 2018, https://www.lawfareblog.com/suggestions-implementing-cloud-act.

87 Global Internet and Jurisdiction Conference, "Cross-border Access To User Data," Internet and Jurisdiction Policy Network, November 2017, accessed August 20, 2018, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Policy-Options-Document.pdf.

## High Substantive as well as Procedural Standards and A Limitation on Club Members

Given the extensive access that law enforcement in participating countries will have to data that is stored with companies that are located in other participating countries, it is clear that the "club" of members should be small and only include those that meet high human rights and due process standards. Put differently, it is necessary to have high procedural and substantive standards in place, and few countries will be able to meet those. One important element of these high standards include minimization procedures defining which type of data can be held for how long, and ensuring that only the minimum needed data is even provided. Data minimization procedures are human – specifically, privacy – rights-respecting as they ensure that only the user data necessary to the legitimate law enforcement aim is provided. They thus further help to prevent an abuse of process by the state. Such procedures are mentioned in the Act and should be defined more clearly so as to make them part of a regular compliance review in which the club members' compliance with the stated human rights and due process standards is re-assessed.

## Clearly Defined Crimes for Inclusion

The CLOUD Act allows for the exchange of data in cases of "serious crime, including terrorism." Given that different countries will define "serious crime" differently, there is a need to more clearly delineate, in each executive agreement, which crimes will be included and potentially spell out which ones are not relevant.

## Ability to Challenge Requests

The executive agreements should better spell out how companies, when faced with a request from another country, can challenge such requests. The comity analysis remains a vague process and it remains unclear which exact factors will enter into the analysis.[88] Companies should know in which circumstances they can reject requests, or otherwise at least be granted permission to ask the Department of Justice for guidance without having to pass on the data.[89]

## Transparency

Transparency will be key to building trust among involved actors – including public and civil society organizations – and to ensure accountability. Three key measures should be taken in this regard. First, the agreements should be published in full or at least all aspects that are not required to be held secret for operational reasons.

88 Derek B. Johnson, "Implementation plans for a new cross-border data law remain cloudy," FCW, April 27, 2018, accessed December 21, 2018, https://fcw.com/articles/2018/04/27/cloud-act-implement.aspx.

89 Daskal and Swire, "Suggestions for Implementing the Cloud Act."

The public needs to understand the underlying standards and broader structures of the agreements.[90] Once the agreements are in place, both requesting countries and the receiving companies should, on a regular basis, publish transparency reports detailing the amount of requests sent or received, respectively (including the number of requests that were declined). Finally, there is a need for regular reviews and audits to check whether governments as well as companies are complying with the relevant mechanisms, and such reviews will only be effective if they include a catalogue of sanctions.[91]

These recommendations would help to increase the effectiveness and sustainability of the CLOUD Act and the regime that it establishes. They would also help to build trust among civil society and human rights groups, representatives of which have already spoken out against the CLOUD Act.[92] Another step to take their concerns into account would be for the DOJ to establish an expert and stakeholder input process for non-governmental stakeholders.[93] After all, public buy-in will be key for the widespread adoption and implementation of the CLOUD Act.

## The E-Evidence Initiative

As for the EU's E-Evidence Initiative, most of the points made above also hold, albeit with a slightly different focus given that there is more of a focus on gaining access to data rather than granting such access to countries outside the EU.[94]

With regard to the criterion of high substantive as well as procedural standards, there are two additional reasons for the EU to ensure high standards. First, the European Court of Justice is known for arguing for strong privacy protections and can be expected take a close look at the E-Evidence Regulation and Directive. Second, if the EU as a single actor is interested in entering into executive agreements with the US (as opposed to through its individual member states) all EU member states must meet the standards laid out in the CLOUD Act.

The arguments for transparency are the same as those raised in the context of the CLOUD Act: it will be key to ensure regular review and accountability. With regard to the clear definitions of the included crimes, the current proposal already contains the specification that data may only be issued for "criminal offenses punishable in the

90 Daskal and Swire, "Suggestions for Implementing the Cloud Act."

91 Daskal and Woods, "Cross-Border Data Requests: A Proposed Framework."

92 Ruiz, "Responsibility Deflected." See also Guliani and Naureen Shah, "The CLOUD Act Doesn't Help Privacy and Human Rights."

93 Daskal and Swire, "Suggestions for Implementing the Cloud Act."

94 Further recommendations have been laid out elsewhere. See: European Data Protection Board, "Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)," 2018, accessed December 21, 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf. See also: Alex Roure, "Law Enforcement Access to Electronic Evidence: Will Europe Get It Right?," Disruptive Competition Project, April 16, 2018, accessed December 21, 2018, http://www.project-disco.org/european-union/041618-law-enforcement-access-to-electronic-evidence-will-europe-get-it-right/#.W0725tIzbcs and Center for Democracy and Technology, "CDT Recommendations for Improving the European Commission's E-Evidence Proposals," August 2018, accessed December 21, 2018, https://cdt.org/files/2018/08/2018-08-27-CDT-European-E-Evidence-Paper-FINAL.pdf.

issuing State by a custodial sentence of a maximum of at least 3 years,"[95] or if they belong to a specific list of crimes, including terrorism and child pornography.[96]

Given the broad access to data that the EU seeks from companies that are not incorporated in the EU, it is likely that many of them will be put into situations in which they face conflicts of laws. It is thus all the more necessary to ensure that appropriate processes are in place to give private actors the ability to challenge requests and make their case for why they are not willing or able to share certain data.

In general, the EU should be aware that the scope of the change to the system of international data access it proposes with the Regulation and the respective production orders is quite dramatic. If it gives its member states access to data stored by companies that are not incorporated in the EU, other states, including authoritarian ones, are going to seek the same kind of access. This does not mean that one should not establish such a system, but it is necessary to be aware of the consequences.

The EU should also consider the implications of its own "blocking statute," namely Article 48 of the GDPR, which requires an international agreement for data to be shared with law enforcement officers in non-EU nations. After all, the EU is demanding broad access to data stored abroad, but prohibiting access to data at home for others. European policymakers should keep this conflict in mind when finalizing the E-Evidence Initiative and, for example, include a provision that executive agreements would also lift these prohibitions for the partner country.

The Directive is much less contentious since it focuses on the appointment of a legal representative "for the purpose of gathering evidence in criminal proceedings."[97] Such a measure has already been implemented in Germany through its 2017 Network Enforcement Law and it makes sense to establish such a mechanism on the EU level. After all, if relevant agencies have the authority to serve a company with an order to produce evidence (independently from how broad such authorities are), there needs to be a point of contact for them to serve it to.

---

95 Swire and Hemmings, "Recommendations."

96 *ibid.*

97 European Commission, "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings," 2018, accessed December 21, 2018, https://ec.europa.eu/info/sites/info/files/placeholder_0.pdf.

## Box 3: A Clearinghouse to Address Potential Conflicts of Laws

As mentioned above, the requests for access to data under the CLOUD Act and the EU's proposed E-Evidence Initiative may cause situations in which different laws are in conflict with each other. Both the CLOUD Act and the E-Evidence Initiative foresee review procedures for cases in which a company facing a request for data would be required to breach the law of the country where the data is stored. In this sense, both initiatives take a big step in the right direction by balancing the interests between the jurisdiction issuing the request and potentially contradictory foreign law.

Within the foreseen review procedures, a judge or a tribunal from the country that is issuing the request will be responsible for reviewing the situation and decide on whether or not the company is prevented from providing the data by a foreign law. However, there is a risk that these judges will be biased in favor of the law enforcement

authorities of their own country. A possible solution to this would be a clearinghouse tasked with managing requests for access to data across jurisdictions.[1] There are different ways in which such a clearinghouse can be set up; importantly, it could manage all requests or only those in which there is a dispute or conflict. Establishing a third-party intermediary would certainly come with legal challenges, but just like in international arbitration, where the diverging interests of countries are equally at stake, the clearinghouse could serve as a neutral and legitimate arbitrator. The concerns raised about a clearinghouse, such as those concerning due process and transparency,[2] can be addressed by defining clear rules and operating guidelines. Further, the fear that a clearinghouse might become a target for surveillance or cyber attacks, while legitimate, is not a general obstacle to implementation since judicial authorities face the same challenges. As such, it is an idea worth pursuing to address one of the key challenges in granting law enforcement agencies from different countries access to user data. Importantly, for such an idea to work, all participating states would need to lift their respective blocking statutes in order to allow the clearinghouse to get access to user data.

1 Woods, "Data Beyond Borders," p. 16.

2 Woods, "Data Beyond Borders," p. 17.

# Conclusion

As this paper has made clear, the MLA system is in need of reform and the status quo is untenable. While there is plenty of (well-argued) criticism about the ongoing initiatives, we should not let "the perfect be the enemy of the good."[98] The US CLOUD Act has already been passed and most of the recommendations made above are aimed at getting the executive agreements right. However, these will not be implemented with a broad set of countries, leaving the question of how to engage with states that are not like-minded unanswered. The projected path will likely intensify cooperation between a handful of countries, leaving many outside the club. This makes MLA reform all the more urgent, since states will otherwise revert back to tools that are actually at their disposal, such as data localization efforts. Assessing the implications of their proposed measures should also be at top priority for policymakers in the EU, which is currently planning to turn the long-established system of mutual legal assistance upside down by moving away from the territoriality principle.

98 Daskal and Swire, "Why the CLOUD Act is Good for Privacy and Human Rights."

# References


Access Now, "Discussion Paper - What are Solutions to the "MLAT Problem"?," accessed July 18, 2018, https://www.mlat.info/policy-analysis-docs/discussion-paper-what-are-the-solutions-to-the-mlat-problem.

Aditi Shah and Aditya Kalra, "Exclusive: India proposes easing local data storage rules for foreign payment firms - document," *Reuters*, July 11, 2018, accessed July 18, 2018, https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-india-proposes-easing-local-data-storage-rules-for-foreign-payment-firms-document-idUSKBN1K1240.

Alan McQuinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders," Information Technology and Innovation Foundation, 2017, accessed July 18, 2018, https://itif.org/publications/2017/07/24/how-law-enforcement-should-access-data-across-borders.

Alex Roure, "Law Enforcement Access to Electronic Evidence: Will Europe Get It Right?," Disruptive Competition Project, April 16, 2018, accessed December 21, 2018, http://www.project-disco.org/european-union/041618-law-enforcement-access-to-electronic-evidence-will-europe-get-it-right/#.W0725tIzbcs.

Ali Breland, "Apple to create portal for law enforcement data requests," *The Hill*, November 9, 2018, accessed December 21, 2018, https://thehill.com/policy/technology/406045-apple-to-create-law-enforcement-portal-for-data-requests.

Andrew K. Woods, "Data Beyond Borders: Mutual Legal Assistance in the Internet Era," Global Network Initiative, 2015, accessed July 18, 2018, https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1517&context=law_facpub.

Andrew K. Woods, "Why Does Microsoft Want a Global Convention on Government Access to Data?," *Just Security*, February 19, 2014, accessed July 18, 2018. https://www.justsecurity.org/7246/microsoft-global-convention-government-access-data/.

Bertrand de la Chappelle, "IGF 2018 - Day 2 - Salle VI - WS #393 CLOUD Act & e-Evidence: implications for the Global South," Internet Governance Forum, 2018, accessed December 21, 2018, https://www.intgovforum.org/multilingual/content/igf-2018-day-2-salle-vi-ws-393-cloud-act-e-evidence-implications-for-the-global-south.

Brad Smith, "The CLOUD Act is an important step forward, but now more steps need to follow," Microsoft, April 3, 2018, accessed July 13, 2018. https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/.

Camille Fischer, "The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data," Electronic Frontier Foundation, February 8, 2018, accessed July 13, 2018, https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data.

Center for Democracy and Technology, "CDT Recommendations for Improving the European Commission's E-Evidence Proposals," August 2018, accessed December 21, 2018, https://cdt.org/files/2018/08/2018-08-27-CDT-European-E-Evidence-Paper-FINAL.pdf.

Christoph Burchard, "Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1," *Zeitschrift für Internationale Strafrechtsdogmatik*, no. 6 (2018): pp. 190-203, accessed July 18, 2018, http://www.zis-online.com/dat/artikel/2018_6_1206.pdf.

Christoph Burchard, "Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2," *Zeitschrift für Internationale Strafrechtsdogmatik*, no. 7-8 (2018): pp. 249-267, accessed July 18, 2018, http://www.zis-online.com/dat/artikel/2018_7-8_1213.pdf.

Congress, "S.2383 - CLOUD Act," 2018, accessed July 18, 2018, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

Council of Europe, "T-CY Plenaries," 2018, accessed December 21, 2018, https://www.coe.int/en/web/cybercrime/t-cy-plenaries.

David Ruiz, "Responsibility Deflected, the CLOUD Act Passes," Electronic Frontier Foundation, March 22, 2018, accessed July 13, 2018, https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes.

Derek B. Johnson, "Implementation plans for a new cross-border data law remain cloudy," *FCW*, April 27, 2018, accessed December 21, 2018, https://fcw.com/articles/2018/04/27/cloud-act-implement.aspx.

Drew Mitnick, "The urgent need for MLAT reform," Access Now, September 12, 2014, accessed July 18, 2018, https://www.accessnow.org/the-urgent-needs-for-mlat-reform/.

Eleni Kyriakides, "Digital Free For All Part Deux: European Commission Proposal on E-Evidence," *Just Security*, May 17, 2018, accessed July 13, 2018, https://www.justsecurity.org/56408/digital-free-part-deux-european-commission-proposal-e-evidence/.

Ellen Nakashima, "Supreme Court to hear Microsoft case: A question of law and borders," *The Washington Post*, February 25, 2018, accessed August 6, 2018, https://www.washingtonpost.com/world/national-security/supreme-court-case-centers-on-law-enforcement-access-to-data-held-overseas/2018/02/25/756f7ce8-1a2f-11e8-b2d9-08e748f892c0_story.html?noredirect=on&utm_term=.790fcef99aa8.

European Commission, "E-Evidence," 2018, accessed July 18, 2018, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

European Commission, "Frequently Asked Questions: New EU rules to obtain electronic evidence," 2018, accessed July 13, 2018, http://europa.eu/rapid/press-release_MEMO-18-3345_en.htm.

European Commission, "Joint Declaration on the EU's legislative priorities for 2018-19," 2017, accessed July 13, 2018, https://ec.europa.eu/commission/publications/joint-declaration-eus-legislative-priorities-2018_en.

European Commission, "Proposal for a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final," April 17, 2018, accessed December 21, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN.

European Commission, "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings," 2018, accessed December 21, 2018, https://ec.europa.eu/info/sites/info/files/placeholder_0.pdf.

European Commission, "Proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final," April 17, 2018, accessed December 21, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN.

European Commission, "Questionnaire on improving criminal justice in cyberspace - Summary of Responses," 2016, accessed July 18, 2018, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf.

European Data Protection Board, "Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)," 2018, accessed December 21, 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf.

Ewen MacAskill, "Putin calls internet a 'CIA project' renewing fears of web breakup," *The Guardian*, April 24, 2014, accessed July 17, 2018, https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia.

Gail Kent, "The Mutual Legal Assistance Problem Explained," The Center for Internet and Society, February 23, 2015, accessed July 18, 2018, http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained.

Gail Kent, "Sharing Investigation Specific Data with Law Enforcement - An International Approach," The Center for Internet and Society, 2014, accessed July 18, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413.

Greg Nojeim, "MLAT Reform: A Straw Man Proposal," Center for Democracy and Technology, September 3, 2015, accessed July 18, 2018, https://cdt.org/insight/mlat-reform-a-straw-man-proposal/.

Global Internet and Jurisdiction Conference, "Cross-border Access To User Data," Internet and Jurisdiction Policy Network, November 2017, accessed August 20, 2018, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Policy-Options-Document.pdf.

Google, "Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era," 2017, accessed July 18, 2018, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf.

Jamie Tabaray, "Australia Government Passes Contentious Encryption Law," *New York Times*, December 6, 2018, accessed December 21, 2018, https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html.

Jennifer Daskal, "Microsoft Ireland Argument Analysis: Data, Territoriality, and the Best Way Forward," *Harvard Law Review*, February 28, 2018, accessed August 6, 2018, https://blog.harvardlawreview.org/microsoft-ireland-argument-analysis-data-territoriality-and-the-best-way-forward/.

Jennifer Daskal, "The Un-Territoriality of Data," *Yale Law Journal* 125, no. 2 (2015): pp. 326-559.

Jennifer Daskal and Andrew K. Woods, "Cross-Border Data Requests: A Proposed Framework," *Just Security*, November 24, 2015, accessed July 18, 2018. https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework/.

Jennifer Daskal and Peter Swire, "A Possible US-EU Agreement on Law Enforcement Access to Data?," *Just Security*, May 21, 2018, accessed December 21, 2018, https://www.justsecurity.org/56527/eu-agreement-law-enforcement-access-data/.

Jennifer Daskal and Peter Swire, "Suggestions for Implementing the Cloud Act," *Lawfare*, April 30, 2018, accessed July 18, 2018, https://www.lawfareblog.com/suggestions-implementing-cloud-act.

Jennifer Daskal and Peter Swire, "Why the CLOUD Act is Good for Privacy and Human Rights," *Lawfare*, March 14, 2018, accessed July 18, 2018, https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

Jonah Force Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," Lawfare Research Paper Series 2, no. 3 (2014): pp.1-41, accessed July 18, 2018, https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf

Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age." *Harvard Law School National Security Journal*, January 28, 2015, accessed July 18, 2018, http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/.

Jonah Force Hill and Matthew Noyes, "Rethinking Data, Geography, and Jurisdiction: Towards a Common Framework for Harmonizing Global Data Flow Controls," New America, February 22, 2018, accessed July 18, 2018, https://na-production.s3.amazonaws.com/documents/Rethinking_Data_Geography_Jurisdiction_2.21.pdf.

Kate Westmoreland, "ECPA reform is not just a U.S. issue," The Center for Internet and Society, April 10, 2014, accessed July 18, 2018. http://cyberlaw.stanford.edu/blog/2014/04/ecpa-reform-not-just-us-issue.

Konstantinos Komaitis, "The 'wicked problem' of data localisation," *Journal of Cyber Policy* 2, no. 3

(2017): pp. 355-365.

Lauren Moxley, "EU Releases e-Evidence Proposal for Cross-Border Data Access," *Inside Privacy*, May 8, 2018, accessed July 13, 2018, https://www.insideprivacy.com/uncategorized/eu-releases-e-evidence-proposal-for-cross-border-data-access/

Legal Information Institute, "U.S. Code," Cornell Law School, 2018, accessed July 18, 2018, https://www.law.cornell.edu/uscode/text/18/2702.

Louise Matsakis, "Microsoft's Supreme Court Case Has Big Implications for Data," *Wired*, February 27, 2018, accessed August 6, 2018, https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/?mbid=social_twitter_onsiteshare.

Madhulika Srikumar, "Sharing data across borders." *The Hindu*, April 2, 2018, accessed July 18, 2018, https://www.thehindu.com/opinion/op-ed/sharing-data-across-borders/article23417587.ece.

Mailyn Fidler, "MLAT Reform: Some Thoughts from Civil Society," *Lawfare*, September 11, 2015, accessed July 18, 2018, https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society.

Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel and Bert Verschelde, "The Costs of Data Localization: Friendly Fire on Economic Recovery," European Centre for International Political Economy, 2014, accessed July 18, 2018, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

Michael Rath and Axel Spies, "CLOUD Act: Selbst für die Wolken gibt es Grenzen," *Corporate Compliance Zeitschrift* no. 5 (2018): p. 229-230, https://www.luther-lawfirm.com/fileadmin/user_upload/PDF/Veroeffentlichungen/2018_CCZ_05_Rath_Spiess_CLOUD_Act.pdf.

Mirko Hohmann, Tim Maurer, Robert Morgus and Isabel Skierka, "An Analysis of European Proposals after June 5, 2013," Global Public Policy Institute and New America's Open Technology Institute, November 24, 2014, accessed July 13, 2018, https://www.gppi.net/2014/11/24/technological-sovereignty-missing-the-point.

Neema Singh Guliani and Naureen Shah, "The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them," *Lawfare*, March 16, 2018, accessed July 13, 2018, https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them#.

Peter Swire and Desai Deven, "A "Qualified SPOC" Approach for India and Mutual Legal Assistance," *Lawfare*, March 2, 2017, accessed July 18, 2018, https://www.lawfareblog.com/qualified-spoc-approach-india-and-mutual-legal-assistance.

Peter Swire and Justin Hemmings, "Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act," *Lawfare*, September 13, 2018, accessed July 18, 2018, https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act.

Robert Loeb, Brian P. Goldman and Emily S. Tabatabai, "The CLOUD Act, Explained," Orrick, April 6, 2018, accessed July 13, 2018, https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained.

Stephen P. Mulligan, “Cross-Border Data Sharing under the CLOUD Act,” Congressional Research Service, April 23, 2018, accessed December 21, 2018, https://fas.org/sgp/crs/misc/R45173.pdf.

Tina Gausling,“Offenlegung von Daten auf Basis des CLOUD Act - CLOUD Act und DS-GVO im Spannungsverhältnis”, MultiMedia und Recht 2018, accessed December 22, 2018, https://www.beck-shop.de/mmr-multimedia-recht/productview.aspx?product=1584.

UK Parliament, “Draft Communications Data Bill - Draft Communications Data Bill Joint Committee Contents,” 2012, accessed July 8, 2018, https://publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7909.htm.

Vivek Krishnamurthy, “Cloudy with a Conflict of Laws,” Berkman Klein Center for Internet & Society, 2016, accessed July 18, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733350.

**Global Public Policy Institute (GPPi)**
Reinhardtstr. 7, 10117 Berlin, Germany
Phone +49 30 275 959 75-0
Fax +49 30 275 959 75-99
gppi@gppi.net

gppi.net