THE YALE LAW JOURNAL FORUM
APRIL 1, 2019

Privacy and Security Across Borders

Jennifer Daskal

ABSTRACT. Three recent initiatives—by the United States, European Union, and Australia—are opening salvos in what will likely be an ongoing and critically important debate about law enforcement access to data, the jurisdictional limits to such access, and the rules that apply. Each of these developments addresses a common set of challenges posed by the increased digitalization of information, the rising power of private companies delimiting access to that information, and the cross-border nature of investigations that involve digital evidence. And each has profound implications for privacy, security, and the possibility of meaningful democratic accountability and control.

This Essay analyzes the impetus and results of each these initiatives, highlights their promise and their limits, and offers a way forward. We are in many ways at an inflection point. There is, on the one hand, the risk of governments demanding access to all information anywhere and everywhere, in ways that will almost certainly result in reduced cybersecurity, privacy, and civil liberties for all. But on the other hand, there is a unique opportunity to set baseline standards and clear jurisdictional rules—thereby facilitating law-enforcement access while also protecting, and ideally elevating, speech, privacy, and other rights protections in the process.

INTRODUCTION

In February 2018, the Department of Justice and Microsoft faced off against one another before the Supreme Court in a packed courtroom.[1] The case raised the high-profile question of whether U.S. search warrants reached data in the custody and control of U.S.-based corporations but stored overseas. Dozens of amici weighed in, including several foreign governments and entities, mostly

1. *See* Amy Howe, *Argument Analysis: Justices Divided over Disclosure of Overseas Emails*, SCOTUSBLOG (Feb. 27, 2018, 3:51 PM), http://www.scotusblog.com/2018/02/argument-analysis-justices-divided-disclosure-overseas-emails [https://perma.cc/M6QJ-24S5].

supporting Microsoft's position that the U.S. government's warrant authority only reached data that was territorially stored in the United States.[2]

Less than two months later, the drama fizzled as the Court remanded and vacated the lower court opinion.[3] The case was mooted by Congress's enactment of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, tacked onto the end of a 2,000-plus page omnibus budget bill.[4] The CLOUD Act updated the statute that had been in dispute, effectively siding with the government and specifying that the United States' warrant authority reached data within the custody and control of U.S.-based corporations, regardless of the location of the underlying ones and zeroes. Yet while the Supreme Court battle ended with a sputter, Congress generated a new focal point for debate in passing the CLOUD Act. The rules governing cross-border access to data are a topic of significant, ongoing importance to law enforcement officials, technology companies, privacy groups, and key foreign partners alike.

The United States is currently one of many nations grappling with the law enforcement-related challenges posed by the cross-border nature of data flow, management, and storage. At precisely the same time that the United States was pondering the CLOUD Act, the European Commission (EC) finalized a two-year-long process addressing similar issues. On April 17, 2018, the EC unveiled its long-awaited legislative proposals: the e-Evidence Regulation and e-Evidence Directive.[5] An amended version of the e-Evidence Regulation was adopted by the EC on December 7, 2018.[6] Like the CLOUD Act, these proposals seek to

2. A full list of links to the amicus briefs can be found at *United States v. Microsoft Corp.*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp [https://perma.cc/ZL6D-F59H].

3. United States v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018) (per curiam).

4. Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018).

5. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM (2018) 225 final (Apr. 17, 2018), https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF [https://perma.cc/F4PJ-65X3] [hereinafter *Initial Draft e-Evidence Regulation*]; *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,* COM (2018) 226 final (Apr. 17, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0226&from=EN [https://perma.cc/3AZU-6M82] [hereinafter *Draft e-Evidence Directive*].

6. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, 15010/18 (Nov. 30, 2018), http://data.consilium.europa.eu/doc/document/ST-15020-2018-INIT/en/pdf [https://perma.cc/L8KK-KMLA] [hereinafter *Updated Draft e-Evidence Regulation*]. This is the version that will be used in follow-on discussions with the European Parliament. *Id.* at Intro., ¶ 14.

facilitate law enforcement access to data across borders and lay out a set of baseline rules governing access to data and the resolution of cross-border conflict.

On December 9, 2018, the Australian government enacted comprehensive new legislation designed to facilitate law enforcement access to data.[7] The Australian legislation is different in scope from both the CLOUD Act and e-Evidence proposals in that it primarily responds to perceived concerns related to the increasing use of default encryption.[8] But it, too, grapples in detail with the cross-border nature of investigations involving digital evidence. Among other provisions, the draft Australian legislation specifies in detail the requirements that apply if and when the government directly—and remotely—accesses a computer or data known to be located across borders.[9]

Each of these efforts addresses a common set of challenges posed by the increased digitalization of information and the cross-border nature of investigations involving digital evidence. As governments confront these challenges, they seek new ways to access otherwise inaccessible data, regardless of where the data happens to be stored or where the technology company that manages the data happens to be based. This, in turn, requires a rethinking of jurisdictional boundaries, the setting of baseline standards governing access, and the establishment of mechanisms for resolving disputes.

We are in many ways at an inflection point. There is, on the one hand, the risk of governments demanding access to all information anywhere and everywhere, in ways that will almost certainly result in reduced cybersecurity, privacy, and civil liberties for all. But, on the other hand, there is a unique opportunity for governments, technology companies, and civil society to respond to these cross-border challenges by collectively setting baseline standards and clear jurisdictional rules—and thereby facilitating law enforcement access while also protecting, and ideally elevating, speech, privacy, and other rights protections in the process.

This Essay examines a range of potential—and actual—responses to these challenges. Part I provides background on the mutual legal assistance (MLA) framework and its limitations in light of technological change. Part II examines

---

7. *See* Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth) (Austl.) [hereinafter Austl. Assistance & Access Bill] https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_aspassed/toc_pdf/18204b01.pdf [https://perma.cc/WJ7J-HXJ5].

8. *See* Explanatory Memorandum, Telecommunications and Other Legislation Amendments (Assistance and Access) Bill 2018, (Cth) 2 (Austl.) [hereinafter Explanatory Memo, Austl. Assistance & Access Bill] https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf (highlighting challenges posed by encryption).

9. Austl. Assistance & Access Bill, *supra* note 7, §§ 43A, 43B.

the responses to these challenges by three key players, namely the United States, the European Union, and Australia; highlights the similarities and differences between the three approaches; and identifies the broader implications of these developments for privacy and security. Finally, Part III of this Essay offers suggestions for a way forward—one that aims to enhance both security and privacy.

I. THE SHIFTING FACTS ON THE GROUND

Until relatively recently, most evidence sought in the prosecution of criminal activity was physically located in the investigating and prosecuting jurisdiction's territory. To be sure, there have long been cartels and other criminal actors that operate across multiple states' borders. And globalization and previous developments in technology have facilitated the movement of people and goods across borders. But historically, most investigations were local, as was the relevant evidence. Criminal investigations that required access to evidence or witnesses across territorial borders remained the exception rather than the rule.

The developments of a globally interconnected internet and cloud storage has changed that. Increasingly, users in State A contract with or use email or social media services that are based in State B. Meanwhile, technology companies often store users' data across international borders.[10] A user may have never stepped foot in or have any other connection to the jurisdiction where the service provider is located or the data is stored.

This has created a range of challenges for law enforcement for three key reasons. First, digital evidence is increasingly critical to many, if not most, criminal investigations. Photos, communications, business records, tax payments, and financial transactions—all pieces of evidence important in a range of investigations—are now stored digitally. This is evidence that can both incriminate and exonerate. A recent European Commission report estimates that digital evidence is important in about eighty-five percent of investigations.[11] Indeed, digital evidence will only become more relevant with the global expansion of internet penetration and the advent of the Internet of Things.

---

10. I use the term "technology companies" broadly to refer to email service providers, social media companies, and other entities that manage or hold the digital information of others that is or may be of interest to law enforcement entities.

11. *Commission Staff Working Document, Impact Assessment Accompanying Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and 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*, at 14, SWD (2018) 118 final (Apr. 17,

Second, the digitalization of communications and other information brings an additional, critically important, and often quite powerful player into the mix. Rather than tracking or searching a target and his or her possessions directly, law enforcement increasingly seeks—and arguably needs—information that is held in the hands of third-party technology companies. Through a combination of technological, business, and policy decisions, these private companies control to a significant degree how much evidence is and will be made available to law enforcement. The dispute between the FBI and Apple over access to the iPhone used by the shooter in the 2016 San Bernardino terrorist attack is a high-profile example.[12] But there are also countless other ways—some publicly known and touted, but many invisible—in which technology companies set the contours of possible government access.[13]

Third, data sought by law enforcement is often either held outside the investigating state's territorial border or controlled by service providers located across international borders—and sometimes both. The European Commission report found that over half of all criminal investigations involve a cross-border request for digital evidence.[14]

This third factor in particular—the fact that digital evidence is often held or controlled by providers across territorial borders—creates a number of legal uncertainties and practical difficulties. Under longstanding principles of international law, law enforcement in State *A* is generally prohibited from unilaterally searching and seizing property located in State *B*, absent State *B*'s consent.[15] This makes good sense. After all, most of us would feel uneasy about a law enforcement agent from Moscow showing up on the doorstep of a target in, say, Chicago or London, and asserting the right to search his or her home based on a Russian government-issued order.

2018) [hereinafter *EC Impact Assessment*] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:118:FIN [https://perma.cc/Z9K5-5HF4].

12. *See* Sean Hollister & Connie Guglielmo, *How an iPhone Became the FBI's Public Enemy No. 1 (FAQ)*, CNET (Feb. 25, 2016), https://www.cnet.com/news/apple-versus-the-fbi-why-the-lowest-priced-iphone-has-the-us-in-a-tizzy-faq [https://perma.cc/HL2Z-6CZG].

13. For an excellent discussion of the increasing power of technology companies to determine, via a combination of business, policy, and technological decisions, the amount and scope of information available to the government, see Alan Z. Rozenshtein, *Surveillance Intermediaries,* 70 STAN. L. REV. 99 (2018).

14. *EC Impact Assessment*, *supra* note 11, at 14.

15. *See, e.g.*, RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432 cmt. b (AM. LAW INST. 2018) ("[A] state may not exercise jurisdiction to enforce in the territory of another state without the consent of that other state"); JAMES R. CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 478-79 (8th ed. 2012).

States instead have employed what is known as the mutual legal assistance (MLA) process. The MLA process requires the requesting state to make a diplomatic request for property of interest and to wait for the jurisdiction with control over the evidence to respond.[16] As one might expect, the process is slow and cumbersome. It depends on the recipient (what I call the "assisting") government agreeing with and aiding the requesting government in its investigation. More often than not, this is low on the priority list for the assisting government. Even when the assisting government agrees to help, it often takes months or longer to respond, in part because of the number of steps that such assistance requires.[17] In many cases, collecting overseas data is just not worth the effort, particularly when the evidence is ephemeral, as digital evidence often is. The sought-after information may simply no longer be there by the time the request is actually approved.

Equally important, effective use of the MLA system requires clarity as to which territorial state has jurisdiction over the data of interest, including the rightful authority to control and restrict access.[18] It also requires agreement as to when a state has jurisdiction to unilaterally compel production and when it must work through another state and make a diplomatic request for data of interest. As of now, however, there is no universal agreement on these basic legal principles, as applied to digital evidence. Should jurisdiction to compel production turn on where the underlying data is located, as Microsoft and several amici, including members of the European Parliament, advocated when the *Microsoft*

16. For a description of the mutual legal assistance process, see Gail Kent, *The Mutual Legal Assistance Problem Explained*, STAN. L. SCH.: CTR. FOR INTERNET & SOC'Y (Feb. 23, 2015), http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained [https://perma.cc/5E2V-UDCR].

17. Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SECURITY J. (Jan. 28, 2015, 1:05 PM), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age [https://perma.cc/K2CC-MEVK] (noting that it often takes months if not years for foreign governments to respond to MLAT requests). According to a 2013 study, for example, the U.S. government took an average of ten months to respond to MLA requests. *See Liberty and Security in a Changing World*, PRESIDENT'S REV. GROUP ON INTELLIGENCE & COMM. TECHS. 227 (Dec. 18, 2013, 4:41 PM), https://obamawhitehouse.archives.gov/blog/2013/12/18/liberty-and-security-changing-world [https://perma.cc/Y32N-QUQ7]. Since then, there have been efforts to streamline the process. But the volume of requests continues to increase, likely increasing wait times as a result.

18. For a broader discussion of these issues, see Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018) [hereinafter Daskal, *Borders and Bits*]; Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015) [hereinafter Daskal, *The Un-Territoriality of Data*]; Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328 (2018).

Ireland case was pending before the U.S. Supreme Court?[19] Should it turn on where the company that manages the data is headquartered? Any place the company has a physical presence? Or perhaps any place where the technology company provides services, as the Australian government has suggested, and as is the basis for the European Union asserting jurisdiction under its General Data Protection Regulation?[20] Or maybe the answer should instead turn on the location or nationality of the target of the search? There also is a key question as to who decides—particularly when one government's assertion of jurisdiction clashes with another's claim of exclusive control.

The answers to these questions determine the scope of both security and privacy rights. Those with jurisdiction over the data get to set both the procedural and substantive standards for access and the limits on how collected data is handled and used.

II. KEY INITIATIVES: THE UNITED STATES, EUROPEAN UNION, AND AUSTRALIAN RESPONSES

Each of the three initiatives described at the start of this Essay—the CLOUD Act, the European Union's e-Evidence proposals, and the Australian legislation—seek to respond to key challenges, answer jurisdictional questions, and set baseline rules. I turn to these efforts now.

A. The U.S. Approach: The CLOUD Act

The CLOUD Act has two key conceptual parts.[21] In what I refer to as Part I, Congress made clear that U.S. warrants issued pursuant to the Stored Communications Act (SCA)—the key U.S. statute that governs law-enforcement access to stored electronic communications content[22]—reach all data within the possession, custody, or control of a U.S.-based provider, regardless of the location of

19. *See* Brief for Respondent at 40-44, United States v. Microsoft, 138 S. Ct. 1186 (2018) (No. 17-2), 2018 WL 447349; Brief of Amici Curiae Jan Philipp Albrecht et al. in Support of Respondent Microsoft Corporation at 15-20, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2), 2018 WL 529845.

20. Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1, art. 3(2), art. 48 [hereinafter GDPR].

21. These two parts roughly correspond to sections 103 and 105 of the Act. *See* CLOUD Act §§ 103, 105.

22. Stored Communications Act, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860-68 (1986) (codified as amended at 18 U.S.C. §§ 2701-12 (2018)). For a broader description and analysis of

the underlying data.[23] In so doing, Congress directly answered the question posed before the Supreme Court in the *Microsoft Ireland* case, effectively ruling in favor of the government and repudiating the Second Circuit's ruling to the contrary.[24]

That said, Congress also recognized that the power to compel disclosure of extraterritorially held data may risk conflict with the laws of foreign nations, particularly when U.S. law enforcement seeks the extraterritorially held data of a foreign national located outside the United States. (This part of the Act thus implicitly accepts target location and nationality as grounds for asserting sovereign control, while rejecting data location, in and of itself, as sufficient grounds for delimiting access.) To address this potential conflict, Congress created a new, albeit limited, statutory basis for providers to move to quash based on a conflict with foreign law.[25] If and when this provision applies, reviewing courts are instructed to engage in totality of the circumstances balancing test in deciding whether or not to enforce the warrant. Factors to consider include the location

---

the Stored Communications Act, see Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

23. CLOUD Act § 103(a) (to be codified at 18 U.S.C. § 2713).

24. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.) (*Microsoft Ireland*), 829 F.3d 197, 201 (2d Cir. 2016), *reh'g denied,* Microsoft Corp. v. United States (*In re* Warrant to Search Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 855 F.3d 53, 54 (2d Cir. 2017) (en banc). The Second Circuit opinion was vacated by *United States v. Microsoft Corp.* (*Microsoft Ireland*), 138 S. Ct. 1186, 1188 (2018) (per curiam). Law enforcement struggled with the effect of the Second Circuit ruling, which required agencies to make MLA requests for data held outside the United States, even if the target of the investigation was a U.S. citizen located in the United States and the data could be accessed by a U.S.-based provider. Complicating matters, providers such as Google operate what has been called a "data shard" cloud, pursuant to which data is regularly moved from one location to another, often across territorial borders. As a result, even different parts of a single account may be held in different jurisdictions. For a discussion of the challenges posed, see Daskal, *Borders and Bits*, *supra* note 18, at 189-91, 221-26; Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1694-99 (2018).

25. CLOUD Act § 103(b) (codified at 18 U.S.C. § 2703(h)). The new statutory provision applies in very limited situations where the United States seeks the data of a foreigner located outside the United States and the request generates a conflict with the law of a "qualifying" foreign government. 18 U.S.C. § 2703(h)(2)(i), (ii). Qualifying foreign governments are those that have reached an executive agreement with the United States, *id.* § 2703(h)(i)(A)—currently a null set. Moreover, the whole point of becoming a qualifying government is to minimize legal conflict, meaning that the set of cases in which the statutory comity provisions can and will be invoked are likely to be far and few between.

and nationality of the investigative target whose data is being sought, the importance of the data to the investigation, and the relative interests of the United States and relevant foreign government, among others.[26]

Part I of the Act also explicitly preserves the availability of so-called common law comity claims—pursuant to which providers can move to quash if compliance with the warrant would generate a conflict with foreign law and the new statute-based motion to quash is not available.[27]

What I call Part II of the CLOUD Act[28] tackles provisions in the SCA that prohibit U.S. technology companies from directly disclosing U.S.-held communications content to a foreign government—provisions that have long been a source of frustration for foreign partners.[29] As a result of these disclosure limitations (often referred to as blocking provisions), foreign governments must make a MLA request to the United States for U.S.-held communications content, even if they are seeking their own citizens' data in the pursuit of a domestic criminal investigation.

The blocking provisions have been a source of acute concern for many foreign governments, particularly in light of the fact that so much data is U.S.-held and thus subject to SCA restrictions on disclosure.[30] They create the exact same problem for foreign governments that the Second Circuit's location of data test created for the U.S. government.[31]

The CLOUD Act leaves the blocking provision in place. It thus provides an implicit endorsement of the underlying principle that the United States can and should use its control over U.S.-based providers to dictate the contours of foreign government access to U.S.-controlled communications content. Yet, Part II

---

26. *Id.* § 2703(h)(3).

27. CLOUD Act § 103(c).

28. *Id.* § 105(a) (codified at 18 U.S.C. § 2523).

29. Specifically, the SCA prohibits providers from turning over the content of communications except in a limited number of situations. *See* 18 U.S.C. §§ 2702, 2703(a). While a "governmental entity" may compel such production pursuant to a lawfully issued warrant, a governmental entity is defined as "a department or agency of the United States or any State or political subdivision thereof." 18 U.S.C. § 2711(4). Thus, foreign governments do not qualify.

30. *See Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights Before the Subcomm. on Crime & Terrorism of the Senate Judiciary Comm.*, 115th Cong. (2017) (statement of Paddy McGuinness, Deputy National Security Adviser, United Kingdom), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20McGuinness%20Testimony.pdf [https://perma.cc/T532-4Q26].

31. These blocking provisions have yielded increasing conflicts of laws, with a foreign government demanding a company to turn over the very data that U.S. law says cannot be disclosed. *See* Brad Smith, *In the Cloud We Trust*, MICROSOFT NEWS (2015), https://news.microsoft.com/stories/inthecloudwetrust [https://perma.cc/F6UW-E3MT].

of the CLOUD Act also provides a mechanism for these restrictions to be lifted on a country-by-country basis, for renewable periods of up to five years, pursuant to an executive agreement between a partner government and the United States.[32]

These agreements are limited by a number of parameters. Specifically, the CLOUD Act lays out a number of conditions that not only limit which foreign governments are eligible for such agreements, but also whose data can be obtained, and how the data can be both requested and used by the foreign government.[33] Importantly, partner foreign governments must be certified as meeting baseline human rights and rule of law standards. Each request made pursuant to such an agreement is subject to a number of conditions as well, including the requirements that it be particularized, based on "articulable and credible facts," and subject to review or oversight by a court, judge, or magistrate or other independent authority.[34] Requests must be made in conjunction with the investigation of "serious crime."[35]

The agreements also include a number of requirements as to the use of collected data. The data must be stored on a "secure system" accessible only to those "trained in applicable procedures."[36] The foreign government is required to segregate, seal, or delete non-relevant information.[37] In addition, the foreign government must agree to periodic reviews by the U.S. government to ensure that the provisions of the executive agreement are being followed.[38] Notably, these use-based requirements include added protections compared to the status quo in many circumstances. Under the otherwise applicable mutual legal assistance process, the U.S. government often has limited say as to how data is handled or stored, and it does not have any formal mechanism for reviewing foreign government use of data that has been disclosed.[39]

---

32. CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523); 18 U.S.C. § 2523(e) (establishing that agreements must be reviewed and affirmatively renewed every five years).

33. CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523(b)).

34. *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(D)).

35. *Id.* § 105 (codified at 18 U.S.C. § 2523 (b)(4)(D)(1)).

36. *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(F)).

37. *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(G)).

38. *Id.* (codified at 18 U.S.C. § 2523 (b)(4)(J)).

39. The E.U.-U.S. Umbrella Agreement is an exception; it lays out a series of limitations on the onward transfer, use, and retention of data shared between U.S. and E.U. law enforcement officials. *See* Agreement between the United States and EU on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, 2016 O.J. (L 336) (entry into force on Feb. 1, 2017), https://eur-lex.europa.eu/legal

The agreements are also subject to limits on scope. They only permit foreign government direct access to data of foreigners who are located outside the territorial borders of the United States. Even with an executive agreement in place, the partner governments cannot directly compel the production of the communications content of U.S. persons (defined to include U.S. citizens and legal permanent residents)[40] or the communications content of others physically located in the United States; those requests still need to go through the MLA system.[41]

These provisions reflect a shift from location of data to location and nationality of the target as a determinant of access. Partner foreign governments can directly compel production of foreigners' data, so long as they comply with the baseline requirements in doing so. But if they want access to a U.S. person's data, they still need to go through the mutual legal assistance process and ultimately get a U.S. official to support the request, followed by U.S. court approval based on the U.S. standard of probable cause.

In sum, the CLOUD Act relies on the United States' position as the home of many major technology companies to both ensure access (Part I) and set baseline rules for others' access, even in situations in which foreign governments seek data of their own citizens and residents pursuant to their own legal authorities (Part II). The Act continues to insist on the application of U.S. laws and procedures when foreign governments seek access to the U.S.-held communications content of U.S. citizens and residents.

B. The E.U. Approach: The Draft e-Evidence Regulation

Similar to the data sharing provisions included in Part II of the CLOUD Act, the E.U.'s draft e-Evidence Regulation sets up a mechanism for authorities in one E.U. member state to compel the production of stored data held by a service provider established or represented in another member state. The draft Regulation is coupled with a draft e-Evidence Directive that requires service providers offering services in the European Union to locate a representative in at least one

-content/EN/TXT/HTML/?uri=CELEX:22016A1210(01)&from=EN [https://perma.cc/4ATQ-4N98].

40. CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523 (a)(2)).

41. *Id.* For a further elaboration of these protections, see Jennifer Daskal, Microsoft Ireland, *the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9, 13-15 (2018), https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0 [https://perma.cc/T763-VX69]; Jennifer Daskal & Peter Swire, *Why the CLOUD Act Is Good for Privacy and Human Rights*, JUST SECURITY (Mar. 14, 2018), https://www.justsecurity.org/53847/cloud-act-good-privacy-human-rights [https://perma.cc/79Z7-NCKV].

member state. This responds to the fact that extraterritorially located technology companies increasingly control, manage, or have access to E.U. citizens' and residents' data; the draft Directive seeks to ensure E.U. jurisdiction over these non-E.U. based providers.[42]

The draft e-Evidence Regulation is similar in many ways to the U.S. CLOUD Act. It shifts the focus away from the location of data as the key determinant of jurisdiction.[43] As with Part II of the CLOUD Act, it enables the requesting government to directly compel production of data from providers located in another member state, and thereby bypass the otherwise applicable requirement that it first gain the assistance and cooperation of the host government in order to access sought-after data.[44]

Similar to the CLOUD Act, the draft Regulation also establishes the baseline requirements that apply, including the requirements that all requests must be necessary and proportionate.[45] All requests for content, as well as a separate category of transactional data (defined to include location data and information

42. *See Updated Draft e-Evidence Regulation*, *supra* note 5; *Draft e-Evidence Directive*, *supra* note 5, at art. 3(1). The Regulation and Directive are the subject of ongoing discussion and debate and are likely to undergo additional revisions before being adopted, if ever. This Essay focuses on the draft provisions as of the time of writing in December 2018.

43. *Initial Draft e-Evidence Regulation*, *supra* note 5, at 13 ("[The draft] Regulation also moves away from data location as a determining connecting factor [for determining jurisdiction], as data storage normally does not result in any control by the state on whose territory data is stored. Such storage is determined in most cases by the provider alone, on the basis of business considerations." (internal citations omitted)).

44. *Initial Draft e-Evidence Regulation*, *supra* note 5, at 1 (emphasizing that "cooperation mechanisms are under increasing pressure from the growing need for timely cross-border access to electronic evidence"); *id* at 2 ("The present proposal targets the specific problem created by the volatile nature of electronic evidence and its international dimension. It seeks to adapt cooperation mechanisms to the digital age, giving the judiciary and law enforcement tools to address the way criminals communicate today and to counter modern forms of criminality."). As with the CLOUD Act, these provisions have been the subject of extensive criticism. *See, e.g.*, Theodore Christakis, *Big Divergence of Opinions on E-evidence in the EU Council: A Proposal in order to Disentangle the Notification Knot*, CROSS-BORDER DATA F. (Oct. 22, 2018), https://www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot [https://perma.cc/A4JQ-G6U9]; *EU "e-evidence" Proposals Turn Service Providers into Judicial Authorities*, EDRi (Apr. 17, 2018), https://edri.org/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities [https://perma.cc/4W9X-AFUS].

45. *Updated Draft e-Evidence Regulation*, *supra* note 5, art. 5(2).

about user contacts),[46] must be issued or validated by a judge, court, or investigating judge.[47] Requests for content and transactional data are, as with the CLOUD Act agreements, permitted only for certain types of crimes, namely those with a maximum custodial sentence of at least three years plus a specified list of additional offenses.[48] Like the CLOUD Act, the draft Regulation includes limits on how the data is used, including limits on the forward transfer of acquired data outside the requesting state.[49] It also lays out specific provisions to deal with conflicting legal obligations that might arise.[50]

But there are also key differences. Importantly, the draft e-Evidence Regulation grants new extraterritorial compulsion authority, authorizing E.U. member states to issue production orders to providers located outside the issuing state's territorial jurisdiction, albeit within the European Union.[51] The CLOUD Act, by comparison, does not grant U.S. officials extraterritorial warrant authority. There is no authority in U.S. law that authorizes U.S. law enforcement to issue disclosure orders on foreign-based providers that lack a physical presence in the United States. True, Part II of the CLOUD Act envisions reciprocal agreements, pursuant to which the United States could, in theory, compel production of certain communications content from providers based in partner foreign countries. But there is not—as of now—any explicit legal authority in U.S. law that would enable issuance of these kind of extraterritorial disclosure orders. The CLOUD Act does not provide any.[52]

The e-Evidence Regulation is much more expansive than the CLOUD Act in other ways as well. Part II of the CLOUD Act merely lifts bars on disclosure, pursuant to executive agreements and subject to a range of specific parameters as to the agreement details. It does not place any affirmative obligation on the providers. And it does not in any way curtail the range of objections that a provider might raise with respect to disclosure.

---

46. *Id.* art. 2(9) (defining "transactional data").

47. *Id.* art 4(2). By contrast, production orders for subscriber and the separate category of "access" data can be issued by a prosecutor as well. *See id.* art. 4(1); *id.* art. 2(8) (defining "access data" to include things like data and time or use).

48. *Id*. art. 5(4).

49. *Id,* arts. 12a, 12b.

50. *Id.* art. 16.

51. *Id.* arts. 1, 4.

52. For a similar discussion of the issues as they apply to the wiretap authority, see Jennifer Daskal, *Setting the Record Straight: The CLOUD Act and the Reach of Wiretapping Authority under US Law,* CROSS-BORDER DATA F. (Oct. 1, 2018), https://www.crossborderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law [https://perma.cc/U4XQ-ECTW].

The draft e-Evidence Regulation, by contrast, both imposes strict time-limits on providers and curtails the grounds for objecting to disclosure orders. Specifically, it requires that providers respond within ten days in general, and within six hours in case of emergency—an obligation that is backed by the threat of hefty fines for noncompliance.[53] The range of approved objections, and thus grounds for noncompliance, are strictly limited. Grounds for objecting are limited to basically three categories only: the order is incomplete, contains "manifest errors," or does not provide sufficient information to execute the order; there is an "impossibility" of compliance; or the order creates a conflict of laws.[54] All such objections must be raised within ten days. Provisions that would have allowed for additional objections based on fundamental rights protections were included in the initial draft proposal,[55] but they were deleted in the amended proposal adopted by the European Commission.[56]

The proposal adopted by the European Commission similarly dropped one of the more innovative features of the initial draft regulation dealing with conflict of laws. The initial draft categorically barred the enforcement of production orders that conflicted with third country laws necessary to protect the fundamental interests of the individuals or country involved. And it set up an explicit mechanism to obtain third-party country input in making this determination.[57] But these provisions were deleted in the version adopted by the European Commission. The European Commission's draft provides for a balancing test for all conflict of law cases, without any of the clear redlines based on protections of fundamental rights or interests.[58]

In exchange, the European Commission added a new notice provision, requiring the issuing state to inform the enforcing state (the state where the production order is served) if and when the issuing state is seeking content data of a person residing outside the issuing state's jurisdiction.[59] The enforcing state

53. *Updated Draft e-Evidence Regulation*, *supra* note 6, art. 9(1), (2); art. 13 (authorizing sanctions up to 2% of the "total worldwide annual turnover of the service provider's preceding financial year").

54. *Id.* art. 9(3); art. 9(4); 16(1).

55. *Initial Draft e-Evidence Regulation*, *supra* note 5, art. 9(5).

56. *Compare Initial Draft e-Evidence Regulation*, *supra* note 5, art. 9(5), ch. 4, *with Updated Draft e-Evidence Regulation*, *supra* note 6, art. 9(5), ch. 4.

57. *Id*. art. 15.

58. This is akin to the balancing test adopted in the CLOUD Act for reviewing conflicting legal obligations, although the e-Evidence Draft includes the added, and draconian, requirement that such conflicts be raised within ten days. *Updated Draft e-Evidence Regulation*, *supra* note 6, art. 16(2); CLOUD Act § 103(a) (codified at 18 U.S.C. § 2703(h)(3) (2018)).

59. *Updated Draft e-Evidence Regulation*, *supra* note 6, art. 7a.

can then raise one of a number of specified objections, including that data is protected by privileges and immunities provided for by the enforcing state's laws, or that disclosure affects the state's fundamental interests, such as national security or defense.[60] The issuing state is then required to withdraw or adapt a not-yet-complied-with-order if "necessary" to give effect to the specified ground for objection.[61]

This provision reflects the idea, akin to that of the CLOUD Act, that the location (and residency) of the target matters for purposes of asserting sovereign control. But the provisions are oddly drafted to only partially achieve the implicit goal. The enforcing state—the one that is given notice—may not be the state where the data subject resides. It is possible, after all, that Member State A (the issuing state) seeks data from a provider in Member State B (the enforcing state), but that the target of the investigation (whose data is sought) is in third-party Member State C. Moreover, the obligation on the issuing state to withdraw or adapt the order in response to an objection only applies to pending orders. Given that providers have just ten days to comply, this is a fairly short window for the enforcing state to both identify and raise an objection.

Thus, whereas the e-Evidence Regulation, as initially drafted, created clear guidance—and redlines—in the face of conflicting legal obligations, as well as a meaningful opportunity for third-party countries to intervene, the version adopted by the European Commission abandons these protections. In its place is of a notice provision that provides minimal protections and only partially accounts for the interests of third-party countries in controlling access to their own citizens and residents' data.

C. The Australian Initiative: Draft Assistance and Access Bill

Australia's draft Assistance and Access Bill has a different focus. It primarily responds to perceived problems in accessing data due to the increased use of encryption. But a key motivation underlying the initiative is the same as that of the U.S. Congress and European Commission—a concern about the "volume of communications that cross national borders," the fact that "crucial" data, services, and products are located extraterritorially, and the "eroding" ability of Australian law enforcement to access intelligible data.[62]

---

60. *Id.* arts. 5(7)(b), 7a.

61. *Id.* art. 7a.

62. *See Assistance and Access Bill 2018: Explanatory Document*, AUSTL. DEP'T HOME AFF. 7 (Aug. 2017), https://www.homeaffairs.gov.au/consultations/Documents/explanatory-document.pdf [https://perma.cc/92J6-6W2Y].

In response to these challenges, the draft law authorizes, among other innovations, the issuance of technical assistance notices and technical capability notices that require technology companies to provide "reasonable, proportionate, practicable and technically feasible" assistance in connection with a warrant or other applicable authorization.[63] The technical assistance notices require use of existing capabilities, while the capability notices require building of new capabilities, and must be approved by the Attorney General.[64] Both can be served on any company that provides services or products used by persons in Australia, even if the company does not have a physical presence in Australia.[65] However, they are subject to a number of limitations: they cannot be used to require building of a new decryption capability or the implementation or building of any systemic weakness or vulnerability.[66]

Australia's draft bill also separately authorizes the use of remote search warrants for digital devices.[67] This is different from the compelled disclosure orders that are the subject of the CLOUD Act and draft e-Evidence Regulation, which are issued on third-party providers. The Australian bill, by contrast, provides a mechanism to law enforcement to directly access sought-after data, thereby bypassing the service provider altogether.[68]

Here, too, the law addresses questions of extraterritorial access. If a device or data is known to be located in a foreign government's jurisdiction, the warrant

---

63. See Explanatory Memo, Austl. Assistance & Access Bill, *supra* note 8, at 11-12; *see also* Austl. Assistance & Access Bill, *supra* note 7, at sch. 1, §§ 317L, 317P, 317T, 317V. For critiques of these provisions, see Jamie Smyth, *US Tech Companies Hit Out at Australian Data Bill*, FIN. TIMES (Sept. 10, 2018), https://www.ft.com/content/2797d3ec-b4d2-11e8-bbc3-ccd7de085ffe [https://perma.cc/AR5W-VUBQ]; Rianna Pfefferkorn, *Comments on the Australian Assistance and Access Bill*, STAN. L. SCH.: CTR. FOR INTERNET & SOC'Y (Sept. 9, 2018), http://cyberlaw.stanford.edu/files/publication/files/2018-09-09%20Pfefferkorn%20Comments%20to%20Australian%20Govt%20on%20Assistance%20%26%20Access%20Bill.pdf [https://perma.cc/GK49-ATN6].

64. Austl. Assistance & Access Bill, *supra* note 7, § 317T.

65. Austl. Assistance & Access Bill, *supra* note 7, at sch. 1, §§ 317C, 317L; *Austl. Assistance & Access Bill Explanatory Document*, *supra* note 62, at 9.

66. *Id.* § 317ZG. That said, both technical assistance orders and technical capability orders can be relied on to require the use of or building of a "capability that is able to be deployed selectively to weaken the electronic protection of a *particular* service, device or item of software." Explanatory Memo, Austl. Assistance & Access Bill, *supra* note 8, at 13 (emphasis added).

67. Austl. Assistance & Access Bill, *supra* note 7, at sch. 2, §§ 27A-H.

68. *Id.* Remote access is often colloquially referred to as "lawful hacking." For a related discussion of the contours of permissible government hacking under U.S. law, see generally Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 590 (2018).

cannot issue without the consent of a competent authority in the foreign government.[69] Evidence obtained in violation of this requirement cannot be introduced in court.[70] If, however, the location of the device or data is unknown, then the warrant can be issued despite the absence of foreign-government consent.[71] Once the location is determined, however, then the obligation to notify and obtain consent is triggered.

Together, these provisions provide an interesting jurisdictional approach—one that highlights a marked contrast in the treatment of direct access (when the government is searching directly) and indirect access (when the government compels a third-party provider to disclose). When it comes to indirect access, the legislation grounds jurisdiction over technology companies on the fact that they serve Australians, even if they lack a physical presence in Australia—a far-reaching assertion of jurisdiction that is akin to what is provided for in the e-Evidence Regulation. But when it comes to direct searches of devices, the jurisdictional ambit is much more limited. The legislation requires affirmative consent by the foreign government where the device or data is located. If and when an objection is made, then the search cannot be carried out. Instead, law enforcement officials are required to work through the mutual legal assistance system or forgo access altogether.

This seeming dichotomy reflects the long-standing international principle that states cannot unilaterally search and seize property in another state's jurisdiction without that jurisdiction's consent. The rule makes sense for extraterritorially located devices, given the long-standing, and well-reasoned, wariness about foreign law enforcement unilaterally and surreptitiously crossing borders to search and seize personal property. But the Australian government adopts this rule even if the *device* is territorially located. So long as the *data* being accessed is known to be located outside Australia, even if accessed from a device within Australia, the legislation requires affirmative foreign government consent. Such an approach appears to reify the notion of data sovereignty tied to location of data—and does so in a way that makes little normative sense. After all, data location may simply be the result of third-party business decisions for reasons such as tax rates and energy costs, and have little-to-no connection to the relevant players or equities in the case.[72]

---

69. Austl. Assistance & Access Bill, *supra* note 7, at sch. 2, § 43A.

70. *Id.* § 43B.

71. *Id.* § 43A(4)(b).

72. *See* Daskal, *The Un-Territoriality of Data*, *supra* note 18, at 365-75.

Yet, when asking a third-party provider to access the data, the jurisdictional limits based on data location no longer apply—and Australia asserts the authority to compel assistance of any provider offering services to end-users in Australia, regardless of the location of the provider or the data being sought.

III. EXTRATERRITORIAL STANDARD SETTING

Each of these efforts reflects an attempt to grapple with three intersecting features of today's digital landscape. First, the increasing digitalization of information, and hence the increasing digitalization of evidence critical to law enforcement investigations. Second, the rising role and power of multinational, private companies that control and store so much of individual users' data, making them the gateway for governmental access to that data. And third, the increasing cross-border nature of criminal investigations, given the possibility—and, for smaller countries, the high likelihood—that digital evidence sought in criminal investigations is held or controlled by companies located across territorial borders.

To some critics, these efforts are jurisdictional power grabs that erode otherwise applicable and often more protective limits on governmental access to data. Part II of the CLOUD Act, for example, has been subject to vociferous criticism on the grounds that it allows foreign governments to bypass the otherwise applicable, and privacy-protective, requirement of a warrant based on probable cause that applies when foreign governments employ the mutual legal assistance process to access sought-after communications content held in the United States.[73] Similarly, the draft e-Evidence proposals have been criticized for allowing requesting governments to bypass protections and additional checks that otherwise apply when they have to work with partner governments to access sought-after data, rather than directly issuing disclosure orders on the private parties that hold the data.[74]

But whereas many of the critiques appropriately highlight the need for additional protections, the outright opposition to these kinds of new jurisdictional approaches misses the forest (as well as the wind direction) for the trees.[75] Put simply, governments, whether one likes it or not, are not going to give up on

73. *See, e.g.*, Neema Singh Guilani & Naureen Shah, *The CLOUD Act Doesn't Help Human Rights: It Hurts Them,* LAWFARE (Mar. 16, 2018, 1:08 PM), https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them [https://perma.cc/ZH76-S8DW].

74. *See, e.g.*, Martin Böse, *An Assessment of the Commission's Proposals on Electronic Evidence*, POL'Y DEP'T FOR CITIZENS' RTS. & CONST. AFF., EUR. PARLIAMENT 6-7 (Sept. 2018), http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf [https://perma.cc/HGM9-CKUF].

75. *See, e.g.*, Daskal, *Borders and Bits*, *supra* note 18, at 180-86; Daskal & Swire; *supra* note 41.

their quest for timely access to digital evidence. Absent workable, transparent mechanisms to access data across borders, governments will seek access by other means, whether via data localization mandates or other, more surreptitious means.

This is not just a hypothetical concern. Several countries already have passed or are actively considering data localization laws, motivated, at least in part, by an interest in facilitating law enforcement access (and fueled by the view, as reflected in the Australian legislation, that there is a sovereign interest in data held in one's own territory).[76] Once these laws are in place, governments can demand disclosure without regard to foreign rules or standards. Not only is there no need to obtain something like a warrant based on probable cause, but the United States and other countries have *zero* say in the substantive and procedural standards that apply.

In other situations, governments seek to surreptitiously access data held across borders that they have difficulty obtaining through other lawful, transparent means. The Australian law authorizing remote accessing of devices is a reflection of this interest: it authorizes the direct, and remote, accessing of devices to account in part for those situations in which access via a third party is not possible or does not yield sufficient or timely information. Whatever one thinks of the merits, at least Australia's provisions are transparent, coupled with the explicit requirement of foreign government consent if the device is located across territorial borders. One could imagine other attempts at remote, cross-border access carried out in secrecy, without any regard for the laws and norms applicable in the jurisdiction where the device is located, and without any transparency—and thus opportunity for discussion and debate—about the substantive and procedural rules that apply.

If these predictions are correct (and they are already borne out with respect to growing data localization requirements),[77] then the efforts at facilitating cross-border access have the potential to enhance privacy over the status quo. They provide a unique opportunity for countries like the United States, as the

---

76. *See, e.g.*, Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* INFO. TECH. & INNOVATION FOUND. 20-31 (May 2017), https://www2.itif.org/2017-cross-border-data-flows.pdf [https://perma.cc/W933-E55H] (listing data localization laws); Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders,* 2 LAWFARE RES. PAPER SERIES 3, 24-26 (July 21, 2014), https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf [https://perma.cc/H232-N8D5] (same).

77. *See Data Localization Snapshot*, INFO. TECH. INDUSTRY COUNCIL, https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf [https://perma.cc/W7JE-GRLM] (current as of Jan. 19, 2017).

home to a disproportionate share of technology companies, and others to both establish a more effective, lawful, and transparent system of cross-border access and set the procedural and substantive standards that apply.

On the other hand, the critiques raise valid concerns. Broad assertions of jurisdiction, in the absence of baseline procedural and substantive protections, threaten to undercut key protections in ways that leave users insufficiently protected.[78] The risk is a cure that is no better, and potentially worse, than the risks of inaction. In response to both the reality and the risks, I offer four broad observations, drawing on the analysis of the three approaches above.

First, certain governmental interests are more justified than others. Specifically, and as reflected in the CLOUD Act, governments have a legitimate interest, grounded in part in principles of democratic accountability, to set limits and procedures regarding foreign government access to their own citizens' and residents' data. They have much less justification (if any at all) in requiring adherence with their *specific* rules and procedures with respect to the accessing of data of foreigners located outside their jurisdiction.

Nonetheless, governments do have an interest and arguably an obligation to insist on certain minimum baseline protections, even with respect to foreign government access to foreigners' data. This is so both for normative and self-interested reasons. After all, data is inherently intermingled. Foreign government access is likely, in fact almost certain, to yield broad incidental collection; thus, even as a means of protecting one's own citizens and residents, governments ought to care, and demand baseline protections, whenever any government seeks access to digital communications.

Second, and relatedly, the baseline substantive and procedural rules matter. The possibility of setting, and thus helping to entrench, meaningful baseline protections is, in fact, the hidden promise of these initiatives. In this vein, the CLOUD Act is innovative. If every country around the globe adopted the provisions on judicial review; targeted collection; speech protections; limitations on use, dissemination, and retention; and the accountability mechanism, the result would be a net gain in privacy and civil liberties. It also should be emphasized that the requirements in the CLOUD Act merely create a *floor* as to the procedural and substantive requirements to be included in any cross-border access agreements. The specific agreements can, and in key areas should, adopt additional measures that go above and beyond the baseline requirements laid out by the U.S. Congress.

---

78. *See* Brief for Respondent at 1, United States v. Microsoft., 138 S. Ct. 1186 (2018) (No. 17-2), 2018 WL 447349 (warning that a rule in which the United States could access data without regard to its location would "instigate a global free-for-all, inviting foreign governments to reciprocate by unilaterally seizing U.S. citizens' private correspondence from computers in the United States").

Conversely, the kind of strict time limits on response times, coupled with the very limited grounds and time for objection, included in the draft e-Evidence Regulation raise significant concerns. There is both an absence of sufficient checks and balances, and a significant risk that providers will be pushed to comply, even in those situations in which the requests raise significant privacy or other civil liberties concerns.

Third, there is an important opportunity to expand the discussion beyond rules governing access to one that also considers how acquired data is used. Under the current MLA system, as is the case in most domestic legal systems, such review is largely on the front end. But there is a critical need—and a corresponding opportunity—to also set rules on how disclosed evidence is ultimately stored, accessed, disseminated, and otherwise used. In this regard, the executive agreements contemplated by the CLOUD Act provide a good starting point. Among other provisions, the CLOUD Act requires secure storage, mandates destruction of nonrelevant data, and sets limits on the dissemination of acquired data. The CLOUD Act also creates a system of audits, pursuant to which the U.S. government would verify compliance with these and other requirements.[79]

Follow-on efforts also should focus on enforcing and strengthening these and any additional use restrictions. The executive agreements drafted under the CLOUD Act should include detailed auditing procedures that ensure meaningful accountability. The draft e-Evidence Regulation would benefit from additional provisions for ensuring compliance. The Australian legislation would benefit from additional limits as to how acquired data is ultimately used. Further efforts also should also account for the need for more transparency, consistent with security requirements. Transparency can help ensure effective compliance. At a minimum, providers should be permitted, and in fact encouraged, to report data about the number and nature of cross-border requests they receive, consistent with the obligation to protect user privacy and the integrity of ongoing investigations.

Fourth, the initiatives should take seriously and provide explicit guidance regarding the risk of legal conflict. In this regard, the clarity provided by the initial draft e-Evidence Directive, which explicitly prohibited transfer of data that would conflict with the fundamental rights protections imposed by another state, provided a good model. This provided a critical protection against a race to the bottom, allowing third-party states to set limits on access in an effort to protect privacy, speech, or other key rights of their residents and citizens. These protections should be added back into any final regulation.

---

79. CLOUD Act §105 (to be codified at 18 U.S.C. § 2523 (2018)).

While the CLOUD Act does not explicitly require consultation with third-party governments, U.S. courts can and should encourage such third-party input. Courts can and should adopt the perspective of the initial e-Evidence drafters and grant motions to quash if the disclosure order will violate fundamental rights protections provided by foreign law. This may limit access in certain situations, but it will also create standards that will ultimately inure to the benefit of everyone. After all, the systems and approaches promulgated in the United States will almost certainly be looked to and likely employed by others; they should be designed with an understanding and assessment of the reciprocal effects.

With respect to remote access of devices, the Australian law goes even further — prohibiting direct access to extraterritorially located devices or data if there is a foreign government objection, no matter the reason. But this may go too far. Even if an appropriate rule for devices, it is not entirely clear that governments should be able to unilaterally prohibit access to data, simply because it is territorially located, without regard to other factors like the nationality and location of the user and the interests of the requesting state in the information.

CONCLUSION

These three recent initiatives — that of the United States, European Union, and Australia — are opening salvos in what will likely be an ongoing and critically important debate about law enforcement access to data, the jurisdictional limits to such access, and the rules that apply. Governments are, after all, increasingly in the position of working through third-party companies to access the data that they want — and often either the company or the data, or perhaps both, are outside the requesting government's territorial boundaries. This creates challenges and opportunities — challenges for the requesting governments to retrieve the data they need, but also opportunities to set normatively sound jurisdictional boundaries and baseline rules of access. If done right, there is an opportunity to protect both privacy and security. If done wrong, there is a risk of a global free-for-all, with nations seeking access to any and all data everywhere, in ways that facilitate law enforcement access but undercut both privacy and the possibility of democratic accountability and control.

Governments should seize this moment. They should establish more flexible systems of accessing data across borders, akin to some of the provisions in the CLOUD Act and draft e-Evidence proposals, but with additional protections built in. At the same time, they should continue to use the leverage of territorial control to demand the kinds of baseline protections that adhere to everyone's ultimate benefit. If these principles are adopted, states can build a system that

promotes both security and privacy and preserves the possibility of accountability and control.

Jennifer Daskal is an Associate Professor at American University Washington College of Law. Special thanks to Peter Swire and Robert Litt for their thoughtful comments, as well as additional input and ideas from members of the Cross-Border Data Forum. The piece also was significantly strengthened by the excellent editing and input from the staff at the Yale Law Journal, *in particular Miranda Li.*