THE CLOUD ACT: CREATING EXECUTIVE BRANCH MONOPOLY OVER CROSS-BORDER DATA ACCESS

Miranda Rutherford†

In 2013, law enforcement officers in New York applied for a warrant under the Stored Communications Act (SCA), ordering Microsoft to disclose information relating to the email account of one of its users, whom the officers suspected of narcotics trafficking.[1] Microsoft complied with the portions of the warrant covering data stored in the United States, but stated that the rest of the data requested was stored in Ireland, which it argued was not covered under the parameters of the warrant.[2] Microsoft then moved to quash the warrant.[3] The magistrate judge and the district court denied the motion to quash.[4] The Second Circuit reversed, reasoning that the language and purpose of the SCA did not extend to overseas data.[5] Rather, the court found that when the SCA was written, "international boundaries were not so routinely crossed as they are today," and the act never could have foreseen a situation in which international data would be demanded.[6] The United States appealed to the Supreme Court, where the case was argued as *U.S. v. Microsoft Corp.*

Microsoft's attempt to quash the search warrant brought to the forefront an issue concerning the SCA that had been percolating in the minds of lawmakers and scholars for years: how the SCA could function in the era of internationalized data storage. Beginning in 2014, Senator Orrin Hatch had repeatedly introduced the Law Enforcement Access to Data Stored Abroad (LEADS) Act, which would have solved the problem in *U.S. v. Microsoft* by extending the SCA to data stored abroad.[7] The Obama administration

DOI: https://doi.org/10.15779/Z387940V34

† J.D. Candidate, 2020, University of California, Berkeley, School of Law.

1. U.S. v. Microsoft Corp., 138 S. Ct. 1186, 1187 (2018).
2. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 200–01 (2d Cir. 2016).
3. *Id.*
4. *Id.* at 201.
5. *Id.*
6. *Id.*
7. S. 2871, 113th Cong. (2014).

proposed similar legislation in 2016.[8] However, none of the variations of the LEADS Act, or its successor, the Clarifying Lawful Overseas Use of Data (CLOUD) Act (introduced in both the House and the Senate in February 2018), gained traction in Congress or even received hearings.

Yet once the *Microsoft* case proceeded to oral arguments at the Supreme Court, whatever brakes had been on the SCA reform train came off. Without much warning, the CLOUD Act was incorporated as the last section in a massive omnibus spending bill signed into law on March 23, 2018.[9] The Act addressed the issue at play in *Microsoft*, amending the SCA so that warrants issued under the SCA could be used to compel disclosure of overseas data held by American companies.[10] The Supreme Court summarily declared the issue in *Microsoft* moot after the CLOUD Act was signed into law.[11]

However, the CLOUD Act does not merely address American warrants for overseas data. It also streamlines the process by which foreign law enforcement can access data stored in the United States, allowing American service providers to disclose information to foreign governments that have an "executive agreement" with the United States.[12] Further, the Act allows for real-time interception of data inside the United States by foreign governments outside of the requirements set by the Wiretap Act.[13] Such international access had previously been administered via Mutual Legal Assistance Treaties (MLATs). MLATs are bilateral treaties between nations wherein governments commit to mutual aid in criminal investigations.[14] The MLAT process ensures that all access demands pass through the legal system of the country where the data is being stored, rather than being served by the foreign government directly on the private entity storing the data.[15] This process can move quite slowly, wasting prosecutors' time in a criminal investigation.[16] Under the CLOUD Act, once an executive agreement is in place, law enforcement authorities in a foreign country can go directly to companies in the United States with their demands, rather than proceeding through executive channels.[17] Since executive agreements are established by the Department of Justice, the executive branch is given significant power to set the constraints

8. Jean Galbraith, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, 112 AM. J. INT'L L. 487, 488 (2018).

9. 115 H.R. 1625, Pub. L. 114-141, 115th Cong. (2018).

10. 18 U.S.C. § 2701.

11. U.S. v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018).

12. 18 U.S.C. § 2511(2)(j).

13. *Id.*

14. *Validity, Construction, and Application of Mutual Legal Assistance Treaties (MLATs)*, 79 A.L.R. FED 2D 375 (2013).

15. *Id.*

16. Galbraith, *supra* note 8, at 487.

17. *Id.*

on extraterritorial data access, which can lead to problems of both due process and conflicts of values.

This paper will first outline the international data storage regime prior to the CLOUD Act, with a particular focus on the problems the CLOUD Act endeavored to solve. It will then explain how the CLOUD Act was composed and passed, and its effects on cross-border data access. Finally, a critique will be offered of the CLOUD Act's impact on due process and creation of conflicts of values, with an examination of the first executive agreement formed under the CLOUD Act's new regime.

I. INTERNATIONAL DATA STORAGE AND THE STORED COMMUNICATIONS ACT

A. THE STORED COMMUNICATIONS ACT AND MUTUAL LEGAL ASSISTANCE TREATIES

Law enforcement demanded Microsoft's data via a warrant under § 2703 of the Stored Communications Act (SCA).[18] The SCA is a section of the Electronic Communications Privacy Act (ECPA), which was passed in 1986 to oversee newly developed electronic communications technology by both penalizing unauthorized wiretapping of the new services and providing measures by which law enforcement could wiretap electronic communications or access electronically-stored data.[19] The SCA "governs data transmitted or held by a third-party service provider," including both providers of electronic communications services (which send or receive communications) and providers of remote computing services (which store data or provide server space or other remote computing resources).[20] Service providers such as Microsoft often play both roles, hosting email messages while also transmitting them.[21] The SCA requires law enforcement to follow specific procedures depending on the type of information demanded, based on how private the drafters of the SCA perceived this information to be.[22] Basic subscriber information merely requires a subpoena.[23] The SCA has more complicated rules for the content of stored email. It has been the practice of the U.S.

18. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 200 (2d Cir. 2016).

19. JAMES P. MARTIN & HARRY CENDROWSKI, CLOUD COMPUTING AND ELECTRONIC DISCOVERY 55 (2014).

20. *Id.* at 57.

21. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1215–16 (2004).

22. MARTIN & CENDROWSKI, *supra* note 19, at 65.

23. *Id.*

Department of Justice for some years to obtain a warrant when seeking stored email, which is how law enforcement proceeded in the *Microsoft* case.[24]

The SCA as passed in 1986 has proved inadequate to handle some of the more complex technological questions that have emerged in the 21st century. This has been most evident with the rise of cloud computing. Major U.S.-based companies store data in servers around the world,[25] whereas smaller companies (and some large ones) make use of global hosting services such as Amazon Web Services.[26] At the same time, the internet has facilitated international crime, enabling criminals to communicate with each other across the globe.[27] As both data and crime have become cross-border, law enforcement agencies have found it necessary to access data stored in other countries. This does not pose a problem when it comes to, for example, Irish law enforcement trying to gain access to Microsoft's data located in Ireland: Irish officials can use local procedures to access that data. However, the SCA does not mention any extraterritorial application of its warrants, leaving it unclear whether or not American law enforcement could gain access to Microsoft's data located in Ireland.[28]

While the SCA was unclear regarding outbound demands for data (from the United States to other countries), it effectively blocked American companies from responding to inbound demands for data (from other countries to the United States).[29] As many of the major technology companies that store data for customers worldwide, including Google, Apple, and Microsoft, are located in the United States, this made it much more difficult for law enforcement officials in other countries to investigate and prosecute crimes using digital evidence.

---

24. *Id.*; *see In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 200 (2d Cir. 2016).

25. *See, e.g.*, *Data Center Locations*, GOOGLE DATA CTRS., https://www.google.com/about/datacenters/inside/locations/index.html [https://perma.cc/S77Q-HL39] (last visited Mar. 20, 2019); *Data Management at Microsoft*, MICROSOFT TRUST CTR., https://www.microsoft.com/en-us/TrustCenter/Privacy/where-your-data-is-located [https://perma.cc/J6JL-ELSL] (last visited Mar. 20, 2019).

26. *See Case Studies & Customer Success*, AMAZON WEB SERVS., https://aws.amazon.com/solutions/case-studies/all/ [https://perma.cc/9CNC-HFBP] (last visited Mar. 20, 2019).

27. *See, e.g.*, MARK LATONERO ET AL., THE RISE OF MOBILE AND THE DIFFUSION OF TECHNOLOGY-FACILITATED TRAFFICKING (2012) (discussing how technology has facilitated human trafficking); Barbara Perry & Patrik Olsson, *Cyberhate: The Globalization of Hate*, 18 INFO. & COMM. TECH. L. 185 (2009) (discussing how technology has facilitated hate crimes); Anita Lavorgna, *Wildlife Trafficking in the Internet Age*, 3 CRIME SCI. 1 (2014) (discussing how technology has facilitated wildlife trafficking).

28. *See* 18 U.S.C. § 2703.

29. *See* 18 U.S.C. § 2702.

To enable both inbound and outbound data access, nations developed the Mutual Legal Assistance Treaties (MLAT) framework. MLATs are treaties established between governments to promise "intergovernmental cooperation in investigating and prosecuting crimes, allow[ing] each of the parties to invoke the legal procedures of the other in aid of criminal investigations and prosecutions."[30] MLATs can cover a "broad range of cooperation measures between the [United States] and foreign countries in criminal matters," which can include identifying witnesses and affected people, serving documents, and collecting fines.[31] However, their data access provisions are most relevant to the discussion of the CLOUD Act. MLATs are based on government-to-government protocols, requiring that when American law enforcement needs access to data stored in another country, it must proceed through the legal procedures of that country rather than seeking the data directly from the entity holding it.[32] Similarly, if a foreign government wants data from a U.S.-based company, its demand must be funneled through the U.S. Department of Justice rather than served directly on the company.[33] International data access was thus treated like all other transnational criminal investigative procedures: by a process of diplomatic cooperation routed through the Department of Justice.

These government-to-government protocols have meant that MLATs can be time-consuming. The statute of limitations and the Speedy Trial Act have "pause buttons" of three years and one year respectively for MLAT processes, indicating how long an MLAT process can often take.[34] A three-year evidence-gathering process can seriously hamper criminal investigations, particularly if the crime being investigated is of a time-sensitive nature. And of course, the process of negotiating an MLAT can itself be time-consuming.[35]

Unsurprisingly, the slowness of MLAT processes has made them unpopular. The magistrate judge who initially ruled on the SCA warrant's extraterritoriality in *Microsoft* was concerned that obtaining the necessary digital data through the MLAT process would levy a "substantial" burden on the

30. *Validity, Construction, and Application of Mutual Legal Assistance Treaties (MLATs)*, 79 A.L.R. FED 2D 375. Countries without MLATs with the United States can still engage in an even lengthier process to demand data: "letters rogatory." *Id.*

31. Stephen C. Thaman, *Report on USA*, *in* TRANSNATIONAL INQUIRIES AND THE PROTECTION OF FUNDAMENTAL RIGHTS IN CRIMINAL PROCEEDINGS 509, 513 (Stefano Ruggeri ed., 2013).

32. *Validity, Construction, and Application of Mutual Legal Assistance Treaties (MLATs)*, 79 A.L.R. FED 2D 375.

33. *Id.*

34. *Id.*

35. *See id.*

government and would "seriously impede[ ]" law enforcement efforts.[36] The increasing need for electronic data had also severely strapped the Department of Justice's Office of International Affairs (OIA), which reviews MLAT procedures.[37] The Department of Justice reported in 2017 that "[s]ince 2000, the number of foreign requests for assistance to OIA has increased nearly 85% and the number of requests for computer records has increased over 1000%. Staffing and resources at OIA had not kept pace with the growth in its work."[38] The MLAT process had become nearly untenable.

B. ACADEMIC CRITIQUES OF EXTRATERRITORIALITY

The SCA, and ECPA more broadly, have long been the subject of criticism for being unduly cumbersome and outpaced by technology.[39] Critics of the SCA began to focus specifically on international data demands as cloud computing and international data storage became more prevalent. Jennifer Daskal suggested in 2015 that international data storage introduced a never-before-seen element to questions of international data access and international criminal procedure more broadly.[40] Because data can travel so easily, quickly, and arbitrarily across borders, and its storage location may have no relation to where it is being used or managed, Daskal argued that territorial approaches to data were inadequate.[41] As the Fourth Amendment is applied only to citizens and those with substantial contacts with the United States, the mobility of data leaves " 'the people' insufficiently protected by a territorial Fourth Amendment."[42] In Daskal's view, the only way to address this disparity between the Fourth Amendment's reach and the extraterritoriality of data would be to re-think the territoriality of Fourth Amendment principles themselves, not just to amend statutes.[43]

Myra Din echoed these concerns when she argued that the extraterritoriality of data raised new problems that judges seemed to be struggling with, particularly when the battle was animated by differing

36. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 221 (2d Cir. 2016).

37. CRIMINAL DIV., U.S. DEP"T OF JUSTICE, PERFORMANCE BUDGET: FY 2017 PRESIDENT'S BUDGET 23 (2016), http://www.justice.gov/jmd/file/820926/download [https://perma.cc/DF8C-KYYG].

38. *Id.*

39. *See generally* Kerr, *supra* note 21 (presenting critiques of the SCA's structure and outdated nature).

40. Jennifer Daskal, *The Unterritoriality of Data*, 125 YALE L.J. 326, 326 (2015).

41. *Id.*

42. *Id.* at 380.

43. *Id.* at 381.

international conceptions of privacy.[44] Din suggested that to some extent, preserving territorial boundaries in the law is a lost cause.[45] Instead, in assessing inbound and outbound data demands, judges should engage in "active cross-referencing," whereby U.S. judges would "analyze various foreign laws and policies and compare them to U.S. counterparts without presuming that one set is superior to the other."[46] Yet as Peter Swire and DeBrae Kennedy-Mayo noted in an analysis of the European Union's and the United States' approaches to privacy, these jurisprudential and policy disagreements between countries underscore the problems with the MLAT system and would need to be considered in MLAT agreements, rather than on a case-by-case basis by individual judges.[47] As countries have their own approaches to privacy and criminal procedure, each MLAT treaty would need to be reformed based on the priorities and values of the two parties in order to address these policy concerns.[48]

Whereas scholars such as Daskal argued that data by its nature cannot be territorial and others emphasized the vast differences among international values and priorities, Andrew Woods countered these approaches by drawing a comparison between data and other intangibles that are nonetheless considered like physical property, such as money or debt.[49] As these "older" intangibles have also been accompanied by jurisdictional debates which courts have successfully resolved, Woods argued that data's territorial debates could be resolved just as easily, and by using similar mechanisms.[50] Woods suggested amending ECPA by removing the sections of the SCA which blocked inbound data demands, so that these demands would not have to proceed through the MLAT process to reach companies.[51] Woods also advised courts to focus on case-by-case comity analysis, which would more equitably and clearly resolve conflict of laws issues.[52] Woods expressed suspicion that—given the different conflicts that could arise with data demands—overarching diplomatic treaties could resolve such conflicts, and proposed using the same types of balancing tests that courts currently use to decide international conflicts of laws.[53]

---

44. Myra F. Din, *Data Without Borders: Resolving Extraterritorial Data Disputes*, 26 J. TRANSNAT'L L. & POL'Y 1, 4 (2016).

45. *Id.* at 6.

46. *Id.* at 7.

47. Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the U.S. are Stricter than Each Other for the Privacy of Government Requests for Information*, 66 EMORY L.J. 617, 618 (2017).

48. *See* Peter Swire et al., *A Mutual Legal Assistance Case Study: The United States and France*, 34 WIS. INT'L L.J. 323, 359 (2016).

49. Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 729 (2016).

50. *Id.*

51. *Id.* at 781.

52. *Id.*

53. *Id.*

C. STEPS TOWARDS THE CLOUD ACT

1. The LEADS Act

In this context of governmental dissatisfaction with the delays in the MLAT process and scholarly critiques of the theory underlying the status quo, legislative solutions were proposed to update the MLAT process and modernize cross-border access to data. In September 2014, Senator Orrin Hatch introduced the Law Enforcement Access to Data Stored Abroad (LEADS) Act, which aimed "to safeguard data stored abroad from improper government access."[54] It proposed to amend the ECPA so that search warrants issued under ECPA would require the disclosure of communications regardless of where they were stored if the account holder was a "United States person."[55] However, the LEADS Act never emerged beyond the Committee on the Judiciary during the 113th Congress. Senator Hatch reintroduced it in 2015 during the 114th Congress, but the LEADS Act again never left the Committee on the Judiciary.

2. Recommendations from the Obama Administration

The Obama administration also attempted to spur action on cross-border data access, but with no greater success. In a response to the slowness and difficulty of MLAT data access, particularly for the United States' closest allies such as the United Kingdom, the administration began to discuss establishing a special treaty with the United Kingdom—and eventually with other countries—that would allow such countries to directly serve American companies with demands for digital data.[56] As part of this effort, the administration sent to Congress a legislative proposal in 2016 that would implement a UK-US bilateral data exchange agreement, which Assistant Attorney General (AAG) Kadzik explained was spurred by the Second Circuit's decision in the *Microsoft* case.[57] Although AAG Kadzik focused on the potential UK-US treaty, he acknowledged that the MLAT process had grown untenable, and that crafting a legislative solution would not only benefit UK-US relations, but also relations with the other sixty-some countries that had MLAT agreements with the United States.[58] While AAG Kadzik's proposal was never officially taken up by Congress, it was similar in content to

54. S. 2871, 113th Cong.

55. S. 2871 § 5(2).

56. Letter from Peter J. Kadzik, Assistant Attorney General, to The Honorable Joseph R. Biden, Vice President of the United States of America (July 15, 2016).

57. *Id.*

58. *Id.*

Congress's next attempt at solving the international data problem: the CLOUD Act.[59]

D. *U.S. V. MICROSOFT*

In 2013, a magistrate judge in the Southern District of New York issued a search warrant under the SCA ordering Microsoft to disclose the contents of an MSN email account, including contents of the emails, contact lists, and any information about the owner of the account.[60] Some information about the account owner was stored on servers in the United States, which Microsoft disclosed, but the contents of the account's emails were stored on a server in Dublin.[61] Microsoft moved to quash the portions of the search warrant that applied to the Dublin records.[62] Microsoft argued that warrants under the SCA functioned just as traditional warrants do, and thus it would be outside the magistrate judge's jurisdiction to serve a warrant on the Irish data center.[63] However, the magistrate judge viewed the SCA differently: its warrants were "more akin to a subpoena," and thus by serving Microsoft's office in the United States with a warrant, law enforcement officials were entitled to obtain access to any data "owned, maintained, controlled, or operated by Microsoft Corporation."[64] Accordingly, the magistrate judge denied Microsoft's motion to quash.[65] The Southern District affirmed the magistrate judge's ruling.[66]

Upon appeal, the Second Circuit reversed the District Court's ruling, in a decision that focused primarily on the text of the SCA; in particular, its use of the term "warrant" as opposed to "subpoena."[67] In reaching this decision, the Second Circuit studiously avoided any broader policy considerations about extraterritorial data and barely touched upon how the SCA's meaning might have evolved since the 1980s.[68] The court also did not discuss what could happen when a foreign government wishes to gain access to data held within the United States. Subsequently, the Supreme Court granted certiorari. After oral arguments, Congress took action, and brought the CLOUD Act to the floor.

---

59. David Callaway & Lothar Determann, *The New US Cloud Act—History, Rules, and Effects*, 35 COMPUTER & INTERNET L. 1, 3 (2018).

60. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 203 (2d Cir. 2016).

61. *Id.* at 204.

62. *Id.*

63. *Id.* at 209.

64. *Id.*

65. *Id.* at 204.

66. *Id.* at 205.

67. *Id.* at 221.

68. *Id.* at 205–06.

II. THE CLARIFYING LAWFUL OVERSEAS USE OF DATA ACT

A. LEGISLATIVE HISTORY

During the 115th session of Congress, while the *Microsoft* case was pending in the Supreme Court, Senator Orin Hatch was finally successful in passing a bill tackling international demands for data. In February 2018, he introduced a new version of the CLOUD Act. Senator Hatch's bill contained a section amending the SCA to cover data stored overseas by American companies as well as a section authorizing the use of "executive agreements" by which foreign governments could demand data stored within the United States.[69] Throughout February and March, the CLOUD Act gained ten co-sponsors, five Democrats and five Republicans, but no hearings were held. Simultaneously, Representative Doug Collins introduced an identical version of the CLOUD Act in the House of Representatives. Again, no hearings were held.

Meanwhile, Congress had been drafting the Consolidated Appropriations Act for the fiscal year that was already well underway. Congress began debate on the Consolidated Appropriations Act on March 22, 2018. Its very last section, page 2116 of a 2148-page bill, incorporated the Senate/House versions of the CLOUD Act nearly word-for-word. On March 23, the Consolidated Appropriations Act unanimously passed both the Senate and the House, with the CLOUD Act tucked in amidst agricultural programs, defense spending, and other agency budget items. There was no discussion in either body of the CLOUD Act.

B. OUTBOUND DEMANDS

The CLOUD Act has two major sections. The first, and shorter, section attempts to solve the problem raised by *Microsoft*: amending the SCA to apply to data held by United States companies overseas (outbound demands). Specifically, the Act adds a new section to ECPA, 18 U.S.C. § 2713, which states:

> A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, *regardless of whether such communication, record, or other information is located within or outside of the United States*.[70]

69. 115 H.R. 1625.

70. 18 U.S.C. § 2713 (emphasis added).

This allows U.S. law enforcement agencies to avoid the *Microsoft* problem when demanding data from companies that hold data overseas; a U.S.-issued warrant served on a U.S. company (or any company otherwise subject to a U.S.-issued warrant) would mandate disclosure of data no matter where it is held.

The CLOUD Act does include a process by which companies can object to outbound demands. However, the grounds upon which a company can object are fairly narrow. When served with an outbound warrant, a company can move to quash or modify the warrant only if the company can show "(i) that the customer or subscriber is not a United States person and does not reside in the United States; and (ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government."[71] "Qualifying foreign governments" are only those governments with which the United States has established an executive agreement (as described below). This implies that if, for example, Microsoft received a warrant for data stored on behalf of an American customer in Ireland, and the United States has not established an executive agreement with Ireland, Microsoft would not be able to move to quash the warrant even if there is a material risk that disclosing the data would violate Ireland's laws. Even if a company is able to meet these two requirements, the court can grant the motion to quash or modify the warrant only if it finds that

> (i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government; (ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and (iii) the customer or subscriber is not a United States person and does not reside in the United States.[72]

In considering the second of these factors, the court must conduct a "comity analysis," taking into account, "as appropriate," the following factors:

> (A) [T]he interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;
>
> (B) the interests of the qualifying foreign government in preventing any prohibited disclosure;
>
> (C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

71. 18 U.S.C. § 2703(h)(2)(A).
72. 18 U.S.C. § 2713(h)(2)(B).

> (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;
>
> (E) the nature and extent of the provider's ties to and presence in the United States;
>
> (F) the importance to the investigation of the information required to be disclosed;
>
> (G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and
>
> (H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.[73]

In short, a court must weigh the costs and benefits of disclosing the data given the interests of the domestic entity seeking disclosure, the importance of disclosure, and the interests of the provider storing the data. The section of the Act concerning outbound demands also contains provisions allowing a company to preserve but not produce data while challenging an outbound demand, and allowing a company to inform its foreign entities of any legal challenges to the outbound demand.[74]

C. INBOUND DEMANDS

The remainder of the Act tackles a problem that *Microsoft* did not raise, but which has been broached by many scholars in the field: how to handle demands from foreign governments for data stored in the United States ("inbound demands"). The CLOUD Act adds a new section to ECPA that allows companies to comply with demands served directly upon them by pre-approved foreign governments (either for release of stored data or for real-time surveillance) without going through the Department of Justice, as required under MLATs. This preapproval process is called an "executive agreement."[75] The Act specifies detailed standards for such agreements, which must be described in a written certification drafted by the Attorney General, with the approval of the Secretary of State, and submitted to Congress for

73. 18 U.S.C. § 2713(h)(3).

74. 18 U.S.C. § 2713(h)(4).

75. 18 U.S.C. § 2523. The executive agreement process does not abrogate the separate MLAT process; countries without executive agreements can still share data under MLATs.

review.[76] In order to establish an executive agreement with the United States, countries must show that they meet four civil liberties and procedural standards: (1) privacy and civil liberties protections; (2) procedures to minimize information acquisition, retention, and dissemination regarding the American person being surveilled; (3) no obligations on the providers to decrypt data or prevent them from decrypting data; and (4) specific restrictions on the agreement to ensure that any inbound demands are made in good faith (for instance, on what grounds the demand can be made and how the surveillance can be minimized).[77] However, the Act does not specify how to measure compliance with these four standards. The majority of the standards require that "adequate" or "appropriate" means be taken without specifying what "adequate" or "appropriate" entails.[78]

The Attorney General's determination that a country qualifies for an executive agreement cannot be judicially or administratively reviewed.[79] Congress may object to an executive agreement via a joint resolution of disapproval, but otherwise the executive agreement will go into force.[80] The Attorney General and the Secretary of State must renew executive agreements every five years to determine if the country has made any changes to the agreement or to its laws and if there are any problems with or controversies regarding the agreement.[81] The Attorney General must then present a report with these findings to Congress, but the Attorney General makes the final decision of whether or not to renew the agreement.[82] Finally, the Act specifies that executive agreements must be published in the Federal Register and that any surveillance falling under an executive agreement must follow minimization procedures as specified by the Foreign Intelligence Surveillance Act.[83]

III. IMPLEMENTATION OF THE CLOUD ACT

While the CLOUD Act did address the problems inherent in the *Microsoft* case and the delays and inconvenience of the MLAT process, it also created a number of new problems. These problems stem from the way in which the entire data demand process is controlled by the executive branch, with little to no judicial oversight over large portions of the process. In particular, any

76. 18 U.S.C. § 2523(b).
77. 18 U.S.C. § 2523(b).
78. *See* 18 U.S.C. § 2523.
79. 18 U.S.C. § 2523(c).
80. 18 U.S.C. § 2523(d)(2), (5)–(7).
81. 18 U.S.C. § 2523(e).
82. *Id.*
83. 18 U.S.C. § 2523(g)–(h).

executive agreement will face two types of problems: problems relating to due process, and problems relating to conflicts of values.

A. DUE PROCESS

The CLOUD Act's language leaves many gaps in both the process of developing executive agreements and the procedures for handling individual data demands. The executive agreement process is left entirely within the control of the Department of Justice, meaning that executive agreements can be formed without any transparency or input from outside stakeholders or judicial oversight. Once an executive agreement is established, countries can demand data following their own national procedures, which may not adhere to U.S. standards. This Section will first discuss the due process issues inherent in developing executive agreements, and then examine the issues with individual data demands.

1. Process of Making Executive Agreements

The CLOUD Act does not require a clear, transparent process for forming executive agreements. Instead, it establishes a wholly internal process within the Department of Justice, which is not required to consult with any external stakeholders nor with the judicial branch. Its executive agreements are only reviewed for rejection (but not amendment) by Congress.[84] The Department of Justice's full control over the process gives the executive branch significant power to dictate not only the countries with which the United States enters into executive agreements, but also the terms of those agreements.

First, there is no requirement that the text of the executive agreement be made public before approval by Congress. This aspect of the executive agreement process has been strongly criticized by the American Civil Liberties Union (ACLU) and other privacy and civil liberties groups.[85] Corporate responses have echoed some of the same concerns; Dropbox and Microsoft have both advocated for transparency in forming executive agreements, with Dropbox in particular supporting "public notice of [the Department of Justice's] intent to negotiate an agreement with a country and engage widely and openly with stakeholders during negotiations."[86] Microsoft has suggested

84. 18 U.S.C. § 2523(d)(5)–(7).

85. American Civil Liberties Union, *The Cloud Act Is a Sinister Piece of Legislation*, MEDIUM (March 13, 2018, 4:15 PM), https://medium.com/aclu/the-cloud-act-is-a-sinister-piece-of-legislation-816f7e1fdac4 [https://perma.cc/BT84-WSHN].

86. *The CLOUD Act Passed: What's Next*, DROPBOX (Apr. 12, 2018), https://www.dropbox.com/news/company/the-cloud-act-passed--what-s-next [https://perma.cc/V54R-65PA]; *see* Brad Smith, *A Call for Principle-Based International Agreements to Govern Law Enforcement Access to Data*, MICROSOFT (Sept. 11, 2018),

that "at minimum, governments must be required to publish the text of the proposed agreement prior to its adoption to allow for meaningful public input."[87] Dropbox has also suggested making the text of executive agreements public in order for companies like Dropbox—as well as, presumably, civil liberties groups and other stakeholders—to make the most of the Congressional review period the CLOUD Act provides and to lobby Congress accordingly.[88] This may be strategically difficult, given the extent to which executive agreements depend on diplomatic compromise; the executive branch and other governments may not want to put all of their cards on the table. Revealing the text of the agreements could also reveal law enforcement investigative techniques or country-specific national security concerns. However, these sensitive sections could be redacted, which would at least allow technologists and lawyers, as well as the general public, to comment on agreements and raise issues the Department of Justice may have overlooked.

Second, the process of forming executive agreements also gives the Department of Justice significant power to determine which countries can qualify for agreements. Because the process is so opaque, this may lead to countries being "safe-listed" by the Department of Justice for entrance into executive agreements, even if those countries have committed human rights abuses or otherwise have poor track records in preserving civil liberties.[89] The Act does require a period of Congressional review, giving the legislative branch the opportunity to disapprove the executive agreement when it is first presented to Congress.[90] Yet the determination of whether a country qualifies for an agreement is explicitly barred from review,[91] and the joint resolution of disapproval requires a veto-proof majority in Congress.[92] Although the CLOUD Act contains minimum standards of civil liberties protections by which a country must abide in order to form an executive agreement, these standards are vague and can easily be interpreted to indicate different levels of civil liberties protections based on the executive branch's own diplomatic

---

https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/ [https://perma.cc/BR4R-72ZF].

87. Smith, *supra* note 86.

88. *The CLOUD Act Passed*, *supra* note 86.

89. Neema Singh Guliani & Naureen Shah, *The CLOUD Act Doesn't Help Privacy and 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/XL5K-QAC5]; *see* American Civil Liberties Union, *supra* note 85.

90. Chris Cook, *Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook*, 29 STAN. L. & POL'Y REV. 205, 228 (2018).

91. 18 U.S.C. § 2523(c).

92. Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1750 (2018).

priorities at the time. Furthermore, as Neema Singh Guliani and Naureen Shah, writing for the ACLU and Amnesty International respectively, observe, "a dizzying array of countries that have ratified major human rights treaties and reflect those obligations in their domestic laws . . . in fact, have arrested, tortured and killed people in retaliation for their activism or due to their identity."[93] The process by which the Department of Justice unilaterally decides which countries are worthy of executive agreements can overlook important concerns that experts or advocates in the field might raise. Their seat at the table is not guaranteed by the CLOUD Act, which only guarantees a seat for the Department of Justice.

Finally, the CLOUD Act does not ensure that real-time developments in countries' politics would be taken into account if laws were to change or new politicians were to take power.[94] Agreements are only reviewed every five years, so in the case of rapid legal and political changes, an agreement may remain in place even if the country no longer complies with the CLOUD Act's civil liberties requirements.[95] As Guliani and Shah note,

> [I]n early 2014, Turkey may have met the CLOUD Act's vague human rights criteria . . . . But since the attempted coup in mid-2016, the Turkish government has arrested more than 50,000 people—including journalists and activists . . . . Under the CLOUD Act, neither Congress nor U.S. courts would be able to prompt a review or a temporary moratorium for a case like Turkey. Users, without notice, would have little practical ability to lodge complaints with the U.S. government or providers. Even if the U.S. government were to take action, the CLOUD Act fails to ensure a sufficiently quick response to protect activists and others whose safety could be threatened.[96]

In contrast, Jennifer Daskal and Peter Swire view the executive agreement process as being a net positive in comparison to the MLAT, as it provides an alternative to the MLAT's lengthy diplomatic processes.[97] However, even as they support the CLOUD Act's foundation,[98] Daskal and Swire acknowledge the opacity issue. They focus on this aspect when suggesting how the CLOUD Act could be implemented. They identify nine different areas in which the CLOUD Act falls short, which they suggest should be addressed in all

93. Guliani & Shah, *supra* note 89.
94. *Id.*
95. *Id.*
96. *Id.*
97. Jennifer Daskal & Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, LAWFARE (Mar. 14, 2018, 12:00 PM), https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights [https://perma.cc/SM5L-QMWP].
98. *Id.*

executive agreements or departmental procedures formed to implement the CLOUD Act.[99] These include input from experts and stakeholders in the field when drafting executive agreements, transparency regarding the terms of the executive agreements, specific procedures for the regular compliance reviews, mechanisms by which to challenge executive agreements, and a point of contact at the Department of Justice for inquiries related to the CLOUD Act.[100] Daskal and Swire also suggest including the Privacy and Civil Liberties Oversight Board in reviewing executive agreements.[101]

These suggestions would go a long way towards ensuring due process in the implementation of executive agreements: input from stakeholders and transparency regarding terms would enable parties other than the executive branch to weigh in on the agreements, and creating mechanisms to review and challenge the executive agreements would provide a means of responding to changes in governments. In addition, the Department of Justice could provide more specific guidelines for the standards countries must meet in order to form executive agreements, as this would give the executive branch less extensive control over the process. Yet none of these suggestions are required by the CLOUD Act. Even if the Department of Justice were to streamline procedures in this way, they would not be required to abide by those procedures.

2. Process of Evaluating Individual Inbound Data Demands

Once an executive agreement is formed, inbound data demands are made under the standards of the demanding country, without U.S. judicial review or notice to users whose data is demanded.[102] This is markedly different from the MLAT process, which requires judicial review of all inbound demands.[103] Instead, under the CLOUD Act, companies must challenge inbound demands through the requesting country's own legal system,[104] which effectively bars U.S. companies who lack the means to engage in international legal processes from objecting to inbound demands.

---

99. Jennifer Daskal & Peter Swire, *Suggestions for Implementing the Cloud Act*, LAWFARE (Apr. 30, 2018, 9:00 AM), https://www.lawfareblog.com/suggestions-implementing-cloud-act [https://perma.cc/7B4R-JG8D].

100. *Id.*

101. Jennifer Daskal & Peter Swire, *Privacy and Civil Liberties Under the CLOUD Act: A Response*, LAWFARE (Mar. 21, 2018, 7:00 AM), https://www.lawfareblog.com/privacy-and-civil-liberties-under-cloud-act-response [https://perma.cc/Z452-7HDT].

102. 18 U.S.C. § 2511(2)(j).

103. *See Validity, Construction, and Application of Mutual Legal Assistance Treaties (MLATs)*, 79 A.L.R. FED 2D 375.

104. *See* 18 U.S.C. § 2511(2)(j) (failing to provide any cause of action for a company to take in a U.S. court).

A coalition of civil liberties groups, including the Electronic Frontier Foundation, the Center for Democracy & Technology, and the National Association for Criminal Defense Lawyers, has identified serious concerns with the CLOUD Act's process for inbound demands, given that they would not be reviewed by the Department of Justice or any U.S. judge.[105] This process could allow countries to obtain data in circumstances where U.S. law enforcement would be prohibited from doing so. For instance, countries could obtain real-time intercepts under standards lower than those applicable to U.S. law enforcement agencies under the Wiretap Act—arguably one of the most concerning portions of the CLOUD Act.[106] Also, foreign governments could access stored data under standards lower than the Fourth Amendment search and seizure standards and could then share that information with U.S. law enforcement, circumventing the Fourth Amendment.[107] Even if U.S. citizens' data is not demanded under the CLOUD Act, U.S. civil liberties groups see intrinsic importance in U.S. privacy and civil liberties protections, and U.S. companies and non-U.S. users of those companies' services value those protections, even if other countries do not meet those standards.

This issue has specifically been raised by the ACLU, which has noted that "foreign governments would be able to get emails and other electronic information without any additional scrutiny by a U.S. judge or official."[108] Guliani and Shah also emphasize this, stating that "the bill would not even require notifying the U.S. government or a user regarding a[n inbound data] request."[109] The Electronic Frontier Foundation has objected to the CLOUD Act, arguing that "U.S. laws will be bypassed on U.S. soil."[110] Dropbox and Microsoft have both identified the lack of U.S. judicial review as an area to improve upon when implementing the CLOUD Act, and both have openly supported U.S. judicial review of inbound demands for data as well as a clearer

105. Letter from Access Now, Advocacy for Principled Action in Government, American Civil Liberties Union, Amnesty International USA, Asian American Legal Defense and Education Fund, Campaign for Liberty, Center for Democracy & Technology, CenterLink: The Community of LGBT Centers, Constitutional Alliance, Defending Rights & Dissent, Demand Progress Action, Electronic Frontier Foundation, Equality California, Free Press Action Fund, Government Accountability Project, Government Information Watch, Human Rights Watch, Liberty Coalition, National Association of Criminal Defense Lawyers, National Black Justice Coalition, New America's Open Technology Institute, Open Media, People For the American Way, and Restore The Fourth, to the United States Congress (Mar. 12, 2018) [hereinafter Coalition Letter].

106. *See* Coalition Letter, *supra* note 105; David Ruiz, *Responsibility Deflected, the CLOUD Act Passes*, ELECTRONIC FRONTIER FOUND. (Mar. 22, 2018), https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes [https://perma.cc/DG9X-2QYB].

107. Coalition Letter, *supra* note 105.

108. American Civil Liberties Union, *supra* note 85.

109. Guliani & Shah, *supra* note 89.

110. Ruiz, *supra* note 106.

legal process overall.[111] Dropbox has found that requiring independent judicial review would allow the CLOUD Act's requirements to be treated "as a floor—and not a ceiling" for privacy protections.[112]

Yet judicial review would likely clash with other countries' concerns regarding the time-sensitive nature of investigations. U.K. Deputy National Security Advisor Paddy McGuinness explains that the United Kingdom's support of the CLOUD Act was based at least in part on the rapidity with which investigations could occur when law enforcement was not hampered by an MLAT.[113] Given the need to streamline data collection during time-sensitive situations and before a crime has actually been committed (such as during investigations of potential terrorist cells), countries may be unwilling to impose further delays.[114]

Even if the demands are reviewed by the demanding country's law enforcement or judicial branch, this puts a great deal of faith in the due processes of countries where "courts greenlight, rather than check, police and intelligence services to go after human rights activists . . . ."[115] Further, when the demanding country establishes an executive agreement with the United States, it can set its own standards as to how data demands are issued. A country could include a nondisclosure requirement such that companies cannot tell users that their data is being demanded or get advice from outside counsel.[116] Microsoft's statement seems to demonstrate particular concern with the burden the CLOUD Act places on companies to act as gatekeepers for data demands, viewing independent judicial review as a way to lift companies' obligation to ensure that warrants are founded on an adequate legal basis.[117] Even if a company does identify an improper demand, it "may not have the resources, expertise, or even financial incentive to deny a foreign government request."[118] More importantly, their own corporate values might not match their users' values, with the result that they would not choose to object to a request even if their users might wish it.

111. *See* Smith, *supra* note 86, *The CLOUD Act Passed*, *supra* note 86.

112. *The CLOUD Act Passed*, *supra* note 86.

113. Andrew Keane Woods, *Interview: The British Perspective on the Cross-Border Data Problem*, LAWFARE (Feb. 7, 2018, 11:00 AM), https://www.lawfareblog.com/interview-british-perspective-cross-border-data-problem [https://perma.cc/S3AP-XANU].

114. *See id.*

115. Guliani & Shah, *supra* note 89.

116. Peter Swire & Justin Hemmings, *Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act*, LAWFARE (Sept. 13, 2018, 10:22 AM), https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act [https://perma.cc/6NJ4-YH24].

117. Smith, *supra* note 86.

118. Guliani & Shah, *supra* note 89.

Instead of barring U.S. judicial review entirely or requiring it in all circumstances as with the time-consuming MLAT process, the CLOUD Act should have taken a middle ground: creating a system of appeal to U.S courts. Allowing companies to appeal demands to U.S. courts would ensure that improper demands were scrutinized; and all companies, even those without the funds for international legal proceedings, could ensure they were properly responding to demands. Unfortunately, under the CLOUD Act, inclusion of due process safeguards may depend on the U.S.'s diplomatic relationships and on the political capital other countries bring to the bargaining table—not a reassuring resolution for those concerned about safeguarding due process.

B. CONFLICT OF VALUES

Just as importantly, the CLOUD Act fails to solve—and in fact introduces additional—problems relating to conflicts of values. Conflicting approaches to law enforcement behavior, criminal prosecution, and evidence collection have plagued the MLAT system. The CLOUD Act was designed to avoid these problems by creating a clear mechanism by which data disputes could be adjudicated; namely, by ironing out these issues when forming executive agreements. In fact, a letter from five major technology companies in advance of the Act's passage cited "reducing international conflicts of law" as one of their primary rationales for supporting the CLOUD Act.[119]

Yet while the CLOUD Act reduces traditional conflicts of laws by ensuring that countries can agree ahead of time on how incompatible laws will be reconciled,[120] it fails to address the conflicts of *values* that underpin the conflicts of laws. Governments would necessarily need to make compromises between conflicting laws, which would lead to the values underpinning one country's laws gaining priority over another's. The CLOUD Act's executive agreements could lead to improved transnational data sharing and cooperation due to these

119. Letter from Apple, Facebook, Google, Microsoft and Oath to CLOUD Act bill sponsors (Feb. 6, 2018), https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf [https://perma.cc/RQ38-CGYJ].

120. While the CLOUD Act has reduced many of the traditional conflicts of laws surrounding extraterritorial data access, it has left a few questions open, particularly how the Act would function when confronted with data demands involving three or more countries. For instance, if the *Microsoft* case had involved British law enforcement trying to access data stored by an American company in the Republic of Ireland, how should law enforcement proceed? Because executive agreements are implied to be strictly bilateral, the Act is not immediately equipped to address this. The problem would have to be addressed in every subsequent executive agreement, and given the lack of transparency in executive agreements, a solution to this problem would not be guaranteed. Courts might be required to handle such disputes as they arise.

compromises,[121] promoting reciprocity rather than U.S.-dominated investigative principles.[122] But because executive agreements are diplomatic documents, these compromises might be made based on diplomatic priorities rather than on a full analysis of the underpinning values. And because of the due process concerns outlined in the previous Section, the agreements would be made in the dark, without a country's citizenry being able to weigh in on what values matter most to them.

The issue of conflict of values under the CLOUD Act is likely to be raised in regard to both inbound and outbound demands. This Section will examine each of these demands in turn.

1. Inbound Demands

First, CLOUD Act procedures may face conflicts of values when inbound demands are made on U.S. companies. For example, a country with weaker free speech protections than the United States—such as the United Kingdom, which has a number of speech-related statutes that criminalize speech that the United States protects[123]—could demand from a United States company data that is First Amendment-protected speech in the United States. This conflict has been legally ironed out in the executive agreement between the United States and the United Kingdom (as discussed below), but the agreement does not address what could happen if government officials agree to data disclosure despite a clash with publicly-accepted norms. There is no way under the CLOUD Act for a U.S. company to object to an otherwise legal demand for data related to protected speech, and there is no requirement for notice to users so that the users could object to the disclosure of their data. The only gatekeeper in this circumstance would be the Department of Justice.

As the ACLU has noted, inbound demands could be made by countries with which the United States has a relatively sound diplomatic accord, but which call for data regarding investigations that run counter to American values. For example,

> in recent months, the Polish government has taken steps to pass laws that restrict speech and, in 2017, the government raided the offices of several human rights groups, seizing documents and computers only a day after women staged a march to protest the country's abortion laws. The [CLOUD Act] would provide no protection against requests in these situations, which wrongly target activists

121. Schwartz, *supra* note 92, at 1742.

122. *Id.* at 1745.

123. Swire & Hemmings, *supra* note 116 (detailing U.K. speech-related statutes that could conflict with First Amendment protections, including criminalizing sending electronic messages that are "indecent or grossly offensive").

> and threaten to undo the progress we have made on global human rights.[124]

Daskal and Swire are somewhat dismissive of the conflict of values problem, suggesting that the United States could use the diplomatic pressure of establishing an executive agreement to push countries into adopting more stringent privacy or civil liberties standards.[125] Daskal points to new judicial review standards for data demands the United Kingdom established in anticipation of an executive agreement with the United States.[126] However, there is no guarantee that this kind of diplomatic pressure would be successful for all countries, particularly given the opaque nature of the executive agreement process. Even if countries work to meet "adequate" data privacy standards, there is no way to measure whether "adequate" standards match what the country's citizenry or American data holders deem to be "adequate," nor to meaningfully evaluate if countries are making improvements. This also would not address sheer disparities in values, where one country might not want to compromise in the name of a diplomatic agreement; nor would it address instances where the United States might be willing to compromise its own civil liberties standards in order to establish an agreement. Either scenario would be perfectly plausible under the Act's current language.

In addition, Daskal and Swire raise the objection that requiring countries to adhere to American privacy or civil liberties standards is "imperialistic."[127] They argue that the CLOUD Act's executive agreement process must be able to compromise on some of these conflicts, particularly when conflicts are more procedural in nature—for example, the lack of truly independent judicial oversight in countries where judges play investigatory roles.[128] In such circumstances, where the conflicts arise from procedural and governmental disparities, the executive agreements could of course include compromises on some U.S. norms, like the role of the judiciary, in adapting to other countries' legal systems. However, in criticizing the imposition of U.S. privacy and civil liberties standards, Daskal and Swire do not specify who exactly would chafe at U.S. standards as "imperialistic." When this argument is applied to privacy and civil liberties conflicts, it ignores the very real plight of journalists, activists, and others in countries who may be targeted by their own governments and have their data demanded under the CLOUD Act.[129] In this case, the

124. Guliani & Shah, *supra* note 89.

125. Daskal & Swire, *supra* note 97; *see also* Cook, *supra* note 90, at 229.

126. Jennifer Daskal, Microsoft Ireland*, The CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9, 15 (2018).

127. Daskal & Swire, *supra* note 99.

128. *Id.*

129. *See* Guliani & Shah, *supra* note 89.

Department of Justice would need to determine whose interests executive agreements should value and prioritize: the interests of governments, or of their citizens. Due to the full executive control over the process, affected parties would have little or no opportunity to weigh in and affirm exactly which values they would like executive agreements to respect.[130]

2. Outbound Demands

Although much of the criticism of the CLOUD Act's treatment of conflicts of values has focused on inbound demands, possibly due to a perception that the United States has stricter standards for privacy and civil liberties than many other countries, conflicts are also likely to arise from outbound demands where other countries may object to the United States' legal values. A conflict that is already under debate is that of privacy norms, especially relating to the General Data Protection Regulation (GDPR) in the European Union. As the GDPR restricts when data held in the European Union can be transferred out of the European Union, European countries are likely to closely scrutinize executive agreements with the United States to ensure GDPR compliance and may require a case-by-case analysis of any outbound demands from the United States[131] or a different agreement set up with the European Union as a whole.[132] Compliance with European privacy standards is not an abstract concern: in 2015, the Irish High Court ruled that American data collection under the National Security Administration violated the privacy protections of the Irish Constitution;[133] the European Court of Justice affirmed that the United States needed to use data protection measures "essentially equivalent" to the European Union, which it was not doing at the time.[134] This might create pressure for U.S. law enforcement to comply with GDPR strictures as well, just as American companies are facilitating compliance with the GDPR by implementing privacy protections for all their users. While this could be a boon for user privacy, it could also lead to pressure on the United States to adopt policies to which civil liberties groups have

130. The primary exception to this may be the possibility of Congressional lobbying during the period of review for the executive agreement. However, as explained above, this review only takes place every five years, and given the limitations on Congressional review, would not guarantee full input from the citizenry.

131. Daskal, *supra* note 126, at 12.

132. Schwartz, *supra* note 92, at 1688.

133. Din, *supra* note 44, at 27–28.

134. Din, *supra* note 44, at 29 (citing Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, EU:C:2015:627).

already objected, such as the "right to be forgotten" or the "link tax" currently being debated in the European Union.[135]

Another prospective issue may stem from conflicts over crime and punishment norms. For instance, the United Kingdom has abolished capital punishment.[136] If American law enforcement were pursuing evidence for a capital crime, the U.K. government might be resistant to allowing law enforcement access to this data. The U.S.-U.K. executive agreement does address this issue, which is likely to surface given the U.K. government's interest in data-sharing for terrorism and other serious offenses.[137] However, public perception of British cooperation with a state execution could be politically damaging, prompting the government to take a more conservative approach towards data-sharing regardless of diplomatic pressures. Just as with conflicts of values regarding inbound demands, a government's diplomatic priorities could be pitted against the priorities of its citizenry. Depending on the outcome, this could either lower public trust in the government or hamper law enforcement investigations—either way, an undesirable result, and one the CLOUD Act was intended to avoid but fails to mitigate.

IV. THE U.S.-U.K. EXECUTIVE AGREEMENT

On October 3, 2019, the United States and the United Kingdom entered into the first executive agreement formed under the CLOUD Act ("Agreement").[138] This Agreement addresses some of the concerns about due process and conflicts of values outlined above: it establishes standards by which inbound and outbound orders will be issued,[139] mechanisms by which providers such as Google or Microsoft can raise objections to orders,[140] and

135. The European Court of Justice has ruled that European citizens have a "right to be forgotten"—that is, to request search engines to remove links to private information about them. *See The Right To Be Forgotten (Google v. Spain)*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/right-to-be-forgotten/ [https://perma.cc/LCG3-37NJ] (last visited Mar. 20, 2019). The "link tax" refers to a provision being proposed in Article 13 of the European Union's Directive on Copyright in the Digital Single Market, which requires online platforms to pay publishers to link to their articles. *See, e.g.*, Matt Reynolds, *Google's Article 13 Link Tax Threat Has Put Publishers On Red Alert*, WIRED (Nov. 21, 2018), https://www.wired.co.uk/article/article-13-link-tax-eu-11 [https://perma.cc/P5YZ-F65H].

136. The Human Rights Act 1998 (Amendment) Order 2004, no. 1574 (Eng.).

137. *See* Woods, *supra* note 113.

138. Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Oct. 3, 2019, Dept. of Justice Press Release No. 19-1065.

139. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 5 § 1–2.

140. *Id.* at § 11.

constraints against the use of data when the essential interests of the United States are implicated by freedom of speech concerns or those of the United Kingdom by capital punishment, unless the receiving country gives permission.[141] In particular, the Agreement has been praised for implementing additional procedural safeguards beyond the baseline established by the CLOUD Act.[142] Specifically, orders must be issued under the issuing party's law based on "articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation," with review and certification by a representative of the Attorney General if the United States is the issuing party, and the Secretary of State for the Home Department if the United Kingdom is the issuing party.[143] The orders are subject to minimization procedures which include sealing or deleting unnecessary information, appropriate targeting procedures, and provisions prohibiting the targeting of U.S. persons by the United Kingdom and targeting of persons within the United Kingdom by the United States. When providers receive an order, they may raise reasonable objections with the issuing party's designated authority (in the case of inbound orders to the United States, with the U.K. government).[144] If such objections cannot be resolved, the provider may then raise objections to the receiving party's designated authority (such as to the Attorney General of the United States), and then both parties may confer to resolve objections.[145] The Agreement also adds privacy protection: for example, guidelines for orders to be issued in accordance with the issuing party's privacy and freedom of information laws,[146] consent requirements for transfer of data to third parties,[147] extension of extant privacy laws to data shared under the Agreement,[148] and periodic review of compliance and of the Agreement

141. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 8 § 4.

142. *See* Jennifer Daskal & Peter Swire, *The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards*, LAWFARE (Oct. 8, 2019, 2:33 PM), https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards [https://perma.cc/25WT-SZA9].

143. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 7.

144. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 5 § 11.

145. *Id.*

146. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 8 § 1.

147. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 8 § 2.

148. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 9.

itself.[149] Finally, the Agreement restricts orders to those concerning offenses "punishable by a maximum term of imprisonment of at least three years."[150] By detailing its data-sharing processes, the Agreement takes significant steps to clarify how conflicts between providers and governments can be addressed. Given the breadth of interpretation possible under the CLOUD Act, this Agreement is more promising than might have been expected.

Nevertheless, concerns remain. While the Agreement codifies some due process protections, it has not addressed other blind spots in the CLOUD Act. The Agreement has been criticized by a coalition of human rights and privacy organizations[151] as well as by academics[152] for not requiring prior judicial authorization for data demands, not providing notice to the data subject or individual remedies to individuals whose data is targeted, and permitting interception of communications sent by those in third countries. These issues perpetuate the due process problems in the CLOUD Act as outlined above, placing significant responsibility on providers to monitor and challenge any faulty orders on behalf of their customers—and just as in the CLOUD Act, under the Agreement service providers can only challenge orders in the courts of the issuing party, without any recourse in their own jurisdictions.[153] The Agreement may have made improvements, but the problems that remain indicate that the Agreement is not necessarily a model by which other Agreements should be constructed.

Further, the due process protections the Agreement does establish are not necessarily generalizable for future executive agreements. The Agreement emphasizes that it is based on "standards such as probable cause, necessity and proportionality, independent judicial oversight, and the requirements of laws

149. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 12.

150. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 1 § 14.

151. Letter from Access Now, American-Arab Anti-Discrimination Committee (ADC), Constitutional Alliance, Consumer Action, Defending Rights & Dissent, European Digital Rights (EDRi), Electronic Frontier Finland, Electronic Frontier Foundation, Electronic Privacy Information Center (EPIC), Government Accountability Project, Homo Digitalis, Human Rights Watch, Initiative für Netzfreiheit, Liberty Coalition, Open Rights Group, New America's Open Technology Institute, Restore the Fourth, State Watch, TechFreedom, and Vrijschrift, to the United States Congress (Oct. 29, 2019).

152. *See, e.g.*, Albert Gidari, *Can the US-UK CLOUD Act Agreement Be Fixed?*, CTR. FOR INTERNET & SOC'Y AT STAN. L. SCH. (Nov. 18, 2019, 1:07 PM), http://cyberlaw.stanford.edu/blog/2019/11/can-us-uk-cloud-act-agreement-be-fixed [https://perma.cc/DW3E-HRNE].

153. *See* Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 5 § 11.

relating to the handling and processing of data relating to individuals"[154]—standards that the United States and the United Kingdom generally have in common, whether from their shared common law history or from the U.K.'s Crime (Overseas Production Orders) Act 2019, which revised how the United Kingdom handles foreign data orders in order to allow the subsequent Agreement under the CLOUD Act.[155] Other countries which lack either shared criminal procedure standards or laws aligning data production with U.S. laws may struggle to establish an agreement with the same level of due process protection as the U.K.'s Agreement.

Finally, while the Agreement does address two major conflicts of laws outlined in Section III.B, free speech and capital punishment, it does not address the conflict of values underpinning the conflict of laws. The Agreement resolves the conflict of laws by prohibiting the use of contested data unless the country receiving the demand for the data grants permission "subject to such conditions as it deems necessary."[156] Although the agreement does expressly recognize the different values the United Kingdom and the United States hold regarding individual rights, it allows such values to be overridden solely at the discretion of an executive branch official: the determination to release information is made by the Attorney General in the United States or the Secretary of State for the Home Department in the United Kingdom,[157] without any opportunity for the public to comment on the appropriateness of the conditions set or the decision itself. Even if this solves the problem of any direct legal contradictions, it does not address whether the public would accord this decision legal legitimacy or object to the use of data stored in their country for a prosecution they fundamentally do not support. Rather, the Agreement perpetuates a conflict between the countries' executive branches and the countries' citizens, where the executive branches may waive particular rights without the citizens approving or even knowing of the executive branches' actions.

As with the issue of due process, conflicts of values are likely to continue as additional agreements are established—for instance, the differences in perceptions of data privacy between the United States and the European Union discussed above. The uncertainties regarding both due process and conflicts of values might even compound each other. For instance, countries

154. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 2 § 3(d).

155. The Crime (Overseas Production Orders) Act 2019 (c.5) (Eng.).

156. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 8 § 4.

157. *See* Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Art. 1 § 8.

will need to amend their criminal laws to allow for inbound and outbound data demands in order to establish an executive agreement; citizens of these countries may strongly object to even the idea of U.S. law enforcement gaining access to data from their country's providers.[158] Even as such conflicts are addressed legally and diplomatically under executive agreements, the full impact of values conflicts will not be seen until the first demands under the CLOUD Act are served.

V. CONCLUSION

It is likely that the next executive agreement to be formed under the CLOUD Act will be with Australia: diplomatic talks are already underway between the two countries.[159] This executive agreement will test whether the U.S.-U.K. Agreement was a high-water mark for due process protections or whether the weak points in the Agreement will be addressed. Yet given the tension between diplomatic pressure to form an agreement and distinct differences in legal norms surrounding issues such as civil liberties and punishment, it remains to be seen which pattern will emerge as further agreements are signed: cooperative data-sharing at any cost, or protections of user privacy and due process based on careful consideration of each country's legal norms. It also remains to be seen whether the Department of Justice will undertake a transparent and equitable process when forming future executive agreements.

The CLOUD Act has addressed many of the issues that plagued the MLAT process, and could pave the way for rapid, targeted acquisition of data for legitimate law enforcement investigations. However, the vague language of the Act means there is no guarantee of this outcome. The world instead could be faced with widespread data exchange between companies and governments with very little protection of privacy and civil liberties. The choice between the two now lies in the hands of the Department of Justice and the countries with which it forms executive agreements.

158. *See* David T.S. Fraser, *What a CLOUD Act Agreement Will Look Like for Canada*, CANADIAN PRIVACY L. BLOG (Oct. 14, 2019), https://blog.privacylawyer.ca/2019/10/what-cloud-act-agreement-will-look-like.html [https://perma.cc/JK5F-6K64] (raising potential concerns about Canadian conflicts of values with American data demands).

159. *Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton*, Department of Justice Office of Public Affairs Press Release No. 19-1,075 (Oct. 7, 2019).