INTERNATIONAL IMPACT OF THE CLARIFYING LAWFUL OVERSEAS USE OF DATA (CLOUD) ACT AND SUGGESTED AMENDMENTS TO IMPROVE FOREIGN RELATIONS

Jordan A. Klumpp[*]

TABLE OF CONTENTS

[*] Juris Doctor Candidate at the University of Georgia School of Law. Many thanks to Curtis Nesset for his guidance and helpful commentary. I am also grateful to the editors of the *Georgia Journal of International and Comparative Law* for their excellent editorial work.

I. INTRODUCTION

In the modern world, digital data is everywhere. The average person generates a huge data footprint thanks to technological advancements such as cloud storage and increased connectedness of devices. Each day yields approximately 3.5 billion Google searches and 1.5 billion people active on Facebook, and every minute there are 156 million emails sent, 4.1 million new YouTube video views, 45,000 Uber trips, and 16 million text messages received.[1]

This massive data stockpile presents opportunities to improve business efficiency, aid in criminal investigations, and even create new job markets.[2] However, it's also a logistical nightmare. The sheer volume of data presents organizational and analytical challenges.[3] Beyond the administrative problems, there are also privacy concerns and accessibility issues.[4]

These privacy and accessibility concerns are even more severe in the context of criminal investigations.[5] Because of digital data's prevalence in modern society, that type of information is sometimes used as evidence of criminal activity.[6] But there remain questions on how much of a person's digital footprint should be accessible when that person's civil liberties are on the line.[7] The issue is further complicated when data flows between multiple foreign states and the data must be shared across international borders.

Cross-border data sharing is a major hurdle to data accessibility, especially in the context of data sharing as part of criminal investigations. International entities must cooperate for effective data sharing because digital data moves

---

[1] Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018, 12:42 AM), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#642381fb60ba.

[2] *See* Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, HARV. BUS. REV. (Oct. 2012), https://hbr.org/2012/10/big-data-the-management-revolution; *See also* Sean E. Goodison, Robert C. Davis, & Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, RAND CORP. (2015), https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf.

[3] B. R. Prakash & M. Hanumanthappa, *Issues and Challenges in the Era of Big Data Mining*, 3 INTL. J. EMERGING TRENDS & TECH. COMPUTER SCI. 321 (2014).

[4] *Id.*; *see also Top 12 Common Problems in Data Mining*, BIG DATA MADE SIMPLE (Feb. 3, 2015), http://bigdata-madesimple.com/12-common-problems-in-data-mining/.

[5] Brian A. Jackson, *Using Digital Data in Criminal Investigations: Where and How to Draw the Line?*, FORENSIC MAG. (May 11, 2017), https://www.forensicmag.com/news/2017/05/using-digital-data-criminal-investigations-where-and-how-draw-line.

[6] *Id.*

[7] *Id.*

freely outside of international boundaries.[8] Consider an email sent from Atlanta, Georgia to Seattle, Washington. That email might take a direct route across the United States, but it is also possible the email could bounce through a Canadian server before reaching its final destination.[9] Cloud storage further erodes data's respect for international borders because stored data could be held in storage centers located across the globe in nations such as India, Ireland, or Chile.[10]

Various agreements and pieces of legislation have attempted to facilitate cross-border data sharing. The most recent law addressing this issue is the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which is a United States law enacted in March 2018.[11] The CLOUD Act is aimed at assisting criminal investigations by allowing law enforcement to collect data stored in foreign states.[12] The CLOUD Act achieves this purpose through two main functions.

First, the CLOUD Act forces U.S. companies to comply with domestic warrants and turn over digital data, regardless of whether the data is "physically" stored in the United States or on foreign soil.[13] As an illustration of this function, imagine an Irish citizen who allegedly commits a crime against the United States. Law enforcement wants to obtain emails held on a Microsoft account, but "physically" located on a server in Ireland, as part of their investigation. The CLOUD Act allows law enforcement to obtain this data via a U.S. warrant, without consideration of Irish law.[14]

The CLOUD Act's second function gives the executive branch of the United States power to enter into data sharing executive agreements with foreign governments.[15] For example, the United States could have a data sharing executive agreement with Australia. If the Australian government requested data held by Microsoft, or any other U.S. technology company, the United States would be inclined to turn over the data with no additional process.[16]

---

[8] Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SEC. L. & POL'Y 473, 475 (2016).

[9] *Id.*

[10] *Id.*

[11] Zarine Kharazian, *The CLOUD Act: Arguments for and Against*, INT'L ENF'T L. REP. (Apr. 10, 2018), https://ielrblog.com/index.php/2018/04/10/the-cloud-act-arguments-for-and-against/.

[12] *Id.*

[13] *Id.*

[14] This hypothetical situation mirrors the facts of *United States v. Microsoft Corp.*, 138 S. Ct. 356 (2017) (mem.) (granting government's petition for certiorari), which is the Supreme Court case that the CLOUD Act was written to address. The CLOUD Act rendered *United States v. Microsoft Corp.* moot.

[15] Kharazian, *supra* note 11.

[16] There are several caveats that could affect this situation. These caveats, and the executive agreement provision in general, will be discussed further in subsequent sections of this Note.

This Note presents a comprehensive look at cross-border data sharing, placing special emphasis on the CLOUD Act. It briefly recounts the history of U.S. legislation governing cross-border data accessibility in criminal investigations, while illustrating that modern advancements in law enforcement techniques and data management systems created a need for liberalized cross-border data sharing. This Note will explain how the CLOUD Act fulfills that need by streamlining the cumbersome process previously used to request extraterritorially stored data. This Note will further discuss both domestic and international reaction to the CLOUD Act. It will suggest that reaction within the United States was mostly positive, but the foreign response was mixed and exuded nervousness about the Act's potential impacts (especially regarding the executive agreements provision). Finally, this Note will provide recommended amendments to the executive agreements provision. The suggested amendments are aimed at maintaining positive foreign relations and protecting personal privacy interests in the wake of heightened cross-border data accessibility. This Note recommends modifications to the CLOUD Act executive data sharing agreements, including mandated compliance reviews every year instead of every five years, required congressional approval of each executive agreement, elimination of the reciprocal data sharing requirement, and adding a notice requirement.

II. CROSS-BORDER DATA SHARING

Section II of this note will provide a brief history of cross-border data sharing. It will explore the various pieces of legislation used to facilitate international flow of data, while highlighting the reasons cross-border data sharing is necessary and the problems associated with transferring data this way. This Section will demonstrate the inconsistencies between modern technology and prior legislation governing cross-border data access; it will show why the CLOUD Act was necessary.

In the 1980s, electronic communication became a main staple of society. New inventions such as personal computers, cellular phones, fax machines, and pagers ushered in a digital revolution and a new era of digital data.[17] Congress, concerned that the Fourth Amendment alone would not adequately protect electronic communication, passed the Electronic Communications Privacy Act in 1986.[18] Title II of the Electronic Communications Privacy Act, called the Stored Communications Act (SCA), was intended to protect digital

[17] *See* Gil Press, *A Very Short History of Big Data*, FORBES (May 9, 2013), https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/#487eedaf65a1.

[18] Stored Wire and Electronics Communications and Transactional Record Access (Stored Communications Act), Pub. L. No. 99-508, 100 Stat. 1860 (codified as amended in scattered sections of 18 U.S.C.); Simon M. Baker, *Unfriending the Stored Communications Act: How Technological Advancement and Legislative Inaction Have Rendered Its Protections Obsolete*, 22 DEPAUL J. ART, TECH. & INTELL. PROP. L. 75, 81 (2011).

communications from unreasonable government interference through "a set of Fourth Amendment-like privacy protections."[19]

The SCA's privacy protections were codified in 18 U.S.C. §§ 2702 and 2703. Section 2702 described the rules for whether or not a service provider could voluntarily disclose information to the government,[20] while Section 2703 detailed the procedure the government had to follow when compelling a provider to disclose information.[21]

However, the SCA also contained ambiguities and potential data accessibility problems. For example, the SCA expressly prohibited U.S. companies from turning over digital data to foreign law enforcement.[22] Because of this provision, foreign states conducting local investigations that needed data stored within their boundaries would still have to go through the U.S. government to access that data.[23] This system unnecessarily hindered foreign criminal investigations, and the United States was burdened with a large amount of requests for data.[24]

It was also not clear whether the SCA prohibited U.S. companies from providing the U.S. government with data that was physically stored in foreign nations—i.e., whether the SCA applied extraterritorially.[25] The SCA's application to data stored on foreign soil was the pinnacle issue in the once-anticipated U.S. Supreme Court case *Microsoft Corp. v. United States*; however, the CLOUD Act eliminated the need for judicial intervention by overriding this provision of the SCA.[26] The CLOUD Act's intervention will be discussed with further detail in Section III of this Note.

Many critics viewed the SCA as an obstacle to cross-border data sharing in criminal investigations.[27] Modern criminal investigations often require obtaining digital evidence stored in other countries because the data is frequently held by U.S. technology companies, which have complex global data management systems.[28] For example, Microsoft stores data based on proximity to

---

[19] 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, 1212 (2004).

[20] 18 U.S.C.A. § 2702 (1986).

[21] 18 U.S.C.A. § 2703 (1986).

[22] 18 U.S.C.A. § 2702 (1986); 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, 222 (2018).

[23] Cook, *supra* note 22, at 223, 225 (under the old way, foreign states would have to petition the U.S. government, which would then require a U.S. judge to approve the transfer of data based on a finding of the U.S. standard of probable cause).

[24] *Id.*

[25] *Id.* at 223.

[26] David Katzmaier, *Supreme Court Rules Microsoft Privacy Dispute Moot*, CNET (Apr. 17, 2018), https://www.cnet.com/news/supreme-court-rules-microsoft-privacy-dispute-moot/.

[27] Cook, *supra* note 22, at 222.

[28] *Id.* at 222–23.

where the customer says he or she is physically located; Google segments and stores data by type on different servers around the world.[29]

When the SCA was created in 1986, almost all digital data was stored domestically, and the United States had undeniable jurisdiction over that data. However, the advent of cloud storage compounded the complexity of data management in a way the drafters of the SCA never comprehended.[30]

The method for states to obtain international cooperation in criminal investigations under the SCA regime was through use of mutual legal assistance treaties (MLATs).[31] These treaties are bilateral cooperation agreements between nations.[32] MLATs assist not only in data sharing, but also apply the laws of the nation where the data is stored.[33] As an example, if a member of the European Union (EU) requested U.S. data by way of an MLAT, the United States would be responsible for the investigation that procured the data, and that investigation would have to comply with U.S. constitutional requirements, including the Fourth Amendment and Fifth Amendment.[34]

The United States currently has an MLAT with every EU member state and many other countries across the world.[35] The United States entered into the multiparty MLAT with the EU in 2010, and the agreement had a specific provision dealing with data sharing in criminal investigations.[36]

While it may seem that MLATs are a step forward in terms of cross-border data sharing, the MLAT process is often criticized as being time-consuming and frustrating.[37] The process for foreign governments to receive data stored

---

[29] *Id.*; Sean Gallagher, *The Great Disk Drive in the Sky: How Web Giants Store Big-and We Mean Big-Data*, ARS TECHNICA (Jan. 26, 2012), https://arstechnica.com/information-technology/2012/01/the-big-disk-drive-in-the-sky-how-the-giants-of-the-web-store-big-data.

[30] Cook, *supra* note 22, at 223.

[31] T. MARKUS FUNK, MUTUAL LEGAL ASSISTANCE TREATIES AND LETTERS ROGATORY: A GUIDE FOR JUDGES 8 (2014).

[32] *Id.* at 4.

[33] *Id.* at 6–7.

[34] *Id.*; U.S. CONST. amend. IV (providing freedom from "unreasonable searches and seizures"); U.S. CONST. amend. V (witnesses deposed in the United States or in a foreign country retain the Fifth Amendment privilege against self-incrimination, regardless of whether they are U.S. citizens or foreign nationals). *See generally*, In re Terrorist Bombings, U.S. Embassies, E. Africa, 552 F.3d 177, 199 (2nd Cir. 2008) ("[I]t does not matter whether the defendant is a U.S. citizen or a foreign national: 'no person' tried in the civilian courts of the United States can be compelled 'to be a witness against himself.'").

[35] FUNK, *supra* note 31, at 6.

[36] Mutual Legal Assistance Agreement, art. 5 U.S.-EU, June 25, 2003, T.I.A.S. No. 10-201.1 ("The Contracting Parties shall . . . take such measures as may be necessary to enable joint investigative teams to be established and operated in the respective territories of the United States of America and each Member State for the purpose of facilitating criminal investigations or prosecution . . . .").

[37] THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD (2013), https://obamawhitehouse.archives.gov/sites/defa

in the United States requires the foreign state to submit a request through the Department of Justice Office of International Affairs, which ultimately requires a U.S. Judge to approve the request based on his or her finding of the U.S. standard of probable cause.[38] According to a study conducted by President Obama's Review Group in Intelligence and Communications Technologies, these requests take an average of ten months to complete.[39]

A ten-month delay is not conducive to criminal investigations, especially when digital data is involved. It is essential for law enforcement to move quickly in collecting digital data because there is potential for the data to be easily altered or destroyed by simple actions.[40] As a result of the frustrating delay caused by relying on MLATs, some foreign states experimented with their own solutions of collecting digital data.[41] These methods included expanding surveillance, mandating data localization, and limiting encryption.[42] Many of the methods go against U.S. interests, such as maintaining an open internet.[43]

The United States also struggled with conducting criminal investigations under the SCA. There was a question of whether domestic warrants, issued under the authority of the SCA, applied to data that was physically stored on servers located in foreign countries.[44] The Second Circuit held that data physically stored outside U.S. borders was beyond the scope of a domestic warrant's authority under the SCA.[45] Concerned that the Second Circuit's decision would exacerbate the already massive delay in digital evidence collection, the government appealed the decision to the Supreme Court, and certiorari was granted in *United States v. Microsoft Corp.*[46] Thus, the stage was set for the Supreme Court to decide a key issue of data accessibility in the modern world; however, Congress took preemptive action and hurriedly resolved this issue by passing the CLOUD Act.

---

ult/files/docs/2013-12-12_rg_final_report.pdf.

[38] Tiffany Lin & Mailyn Fidler, *Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement,* BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y AT HARV. U. (Sept. 13, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3035563.

[39] THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS, *supra* note 37, at 227.

[40] Goodison et al., *supra* note 2, at 7.

[41] Lin & Fidler, *supra* note 38, at 4.

[42] *Id.*

[43] *Id.*

[44] Cook, *supra* note 22, at 222.

[45] In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 201 (2d Cir. 2016), *cert. granted sub nom.* U.S. v. Microsoft Corp., 138 S. Ct. 356 (2017), *and vacated and remanded sub nom.* U.S. v. Microsoft Corp., 138 S. Ct. 1186 (2018).

[46] United States v. Microsoft Corp., 138 S. Ct. 356 (2017) (mem.) (granting government's petition for certiorari).

III. THE CLARIFYING LAWFUL OVERSEAS USE OF DATA (CLOUD) ACT

Section III of this note will provide a description of the CLOUD Act and its two main functions: applying SCA warrants extraterritorially and allowing the executive branch to enter international data sharing agreements. The description of the Act found in this Section includes the circumstances surrounding its enactment, as well as an explanation of the key provisions and requirements imposed by the Act.

Congress enacted the CLOUD Act to modify the SCA and provide legislative guidance on domestic warrant application to data physically stored on foreign servers.[47] When the CLOUD Act was passed, it was incorporated as part of the 2018 Omnibus Spending Bill,[48] which is a 2,232-page document that authorized $1.3 trillion of government spending in 2018.[49] Since the Act was part of a larger bill, it did not receive its own standalone floor vote in either the House or Senate.[50] It also never received a hearing and was never reviewed by a committee.[51]

Immediately following the CLOUD Act's adoption, both the Department of Justice and Microsoft filed motions to dismiss *Microsoft Corp. v. United States*, arguing the new law rendered the issue of the case moot.[52] The Supreme Court agreed and released an unsigned opinion that dismissed the case.[53]

The CLOUD Act is codified at 18 U.S.C. § 2713. It adds a provision to the SCA and 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

---

[47] Cook, *supra* note 22, at 226–27.

[48] Consolidated Appropriations Act, H.R. 1625, 115th Cong. § 102 (2018).

[49] Iain Thomson, *US Congress Quietly Slips Cloud-Spying Powers into Page 2,201 of Spending Mega-Bill*, REGISTER (Mar. 23, 2018), https://www.theregister.co.uk/2018/03/23/cloud_act_spending_bill/.

[50] 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.

[51] *Id.*; Burying the CLOUD Act inside a massive spending bill was criticized by some as a means to push through the legislation without adequate consideration of its merits and the public's concerns; however, analyzing the means by which the Act was passed is outside the scope of this Note.

[52] Monica Nickelsburg, *Microsoft and DOJ Ask Supreme Court to Dismiss Case Involving Customer's Overseas Data*, GEEKWIRE (Apr. 3, 2018), https://www.geekwire.com/2018/microsoft-doj-ask-supreme-court-dismiss-case-involving-customers-overseas-data/.

[53] David Katzmaier, *Supreme Court Rules Microsoft Privacy Dispute Moot*, CNET (Apr. 17, 2018), https://www.cnet.com/news/supreme-court-rules-microsoft-privacy-dispute-moot/.

> 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.[54]

The language of the act unequivocally says that warrants issued through the SCA apply to all data under the provider's "possession, custody, or control"—regardless of whether the data is physically stored within the United States or outside its borders.[55] This is an effort to facilitate domestic criminal investigation by providing improved accessibility to digital data stored in international territory.[56]

Domestic criminal investigations are streamlined by this provision because MLATs are no longer relied upon for collecting digital evidence. An SCA warrant is now, in effect, a one-stop shop to procure all digital data held by a U.S. technology company.

Nevertheless, U.S. technology companies are given an opportunity to challenge SCA warrants through the CLOUD Act.[57] The provider may file a motion to quash a warrant if the provider reasonably believes both (1) "that the customer or subscriber is not a United States person and does not reside in the United States" and (2) "that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government."[58]

The Act goes on to define the standards by which a court should evaluate motions to quash SCA warrants. A court may only quash a warrant if it finds that

> (1) turning over the data would cause the provider to violate a foreign government's laws; (2) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and (3) the customer . . . is not a United States person and does not reside in the United States.[59]

Even though the CLOUD Act provides a mechanism for U.S. technology companies to challenge SCA warrants pre-enforcement, there are no similar

---

[54] 18 U.S.C.A. § 2713 (2018).
[55] *Id.*
[56] Kharazian, *supra* note 11.
[57] 18 U.S.C.A. § 2703(h)(2) (2019).
[58] 18 U.S.C.A. § 2703(h)(2)(A)(i)–(ii).
[59] 18 U.S.C.A. § 2703(h)(2)(A)–(B).

measures that allow subscribers or customers to challenge SCA warrants pre-enforcement.[60]

The CLOUD Act streamlines domestic data accessibility, but it also addresses foreign states' access to U.S.-held data.[61] More specifically, the Act allows the U.S. executive branch to enter into data sharing executive agreements with qualifying foreign states, thus providing a means for select foreign governments to sidestep the cumbersome MLAT process.[62]

However, there are substantive and procedural requirements of these executive agreements.[63] Foreign states may only enter into a data sharing executive agreement after both the U.S. Attorney General and Secretary of State certify in writing with an accompanying explanation that the foreign state "affords robust substantive and procedural protections for privacy and civil liberties."[64] The foreign state must also agree to give the United States reciprocal access to data held by the foreign state.[65] Further, the executive branch must review and renew each executive agreement every five years to ensure these requirements continue to be adequately fulfilled.[66]

Each individual request for data issued by a foreign state under an executive agreement must meet additional requirements. The requests must be sufficiently specific (i.e., target a distinct person, account, device, or other identifier), have basis in "articulable and credible facts," be subject to review by an independent authority in the foreign state, and cannot be used to infringe free speech.[67]

However, evaluation of whether the statutory requirements of these agreements are met is a job delegated almost exclusively to the executive branch. The CLOUD Act expressly eliminates judicial review as a means of evaluating these executive agreements: "[a] determination or certification made by the Attorney General . . . shall not be subject to judicial or administrative review."[68] In fact, the only means of challenging the executive branch's decision to enter into a data sharing executive agreement is a joint resolution of disapproval passed by both the House of Representatives and the Senate within 180

---

[60] Jonathan I. Blackman, Jared Gerber, Nowell D. Bamberger, Georgia V. Stasinopoulos & Nicholas G. Amin, *CLOUD Act Establishes Framework to Access Overseas Stored Electronic Communications*, 30 No. 6 INTELL. PROP. & TECH. L.J. 10, 13 (2018).

[61] Kharazian, *supra* note 11.

[62] 18 U.S.C.A. § 2523 (2018).

[63] *Id.*; Jennifer Daskal, *Microsoft Ireland, the Cloud Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9, 13 (2018).

[64] 18 U.S.C.A. § 2523(b)(1) (2018).

[65] 18 U.S.C.A. § 2523(b)(4)(I) (2018).

[66] 18 U.S.C.A. § 2523(e) (2018).

[67] 18 U.S.C.A. § 2523(b)(4)(D)(iv) (2018); Daskal, *supra* note 63, at 14.

[68] 18 U.S.C.A. § 2523(c).

days of the Attorney General providing Congress with notice of the executive agreement.[69]

Another important feature of the CLOUD Act provides that these executive agreements do not allow foreign states to access the data of U.S. citizens; the agreements may only be used to collect data of foreign persons located outside of the United States.[70] Foreign states who wish to access data of individuals in the United States (including citizens, legal permanent residents, and others located within the physical borders of the United States) must employ the MLAT process.[71]

IV. DOMESTIC REACTION TO THE CLOUD ACT

This Section discusses the reaction to the CLOUD Act among entities within U.S. borders. It analyzes how U.S. government officials, U.S. technology companies, legal academics, and domestic civil liberties organizations responded to the Act being passed.

While the CLOUD Act was being considered, and when ultimately passed, it was met with a mixed domestic reaction. The U.S. government, many U.S. technology companies, and some legal academics voiced strong support for the Act; advocates view it as necessary for modern criminal investigations and an important answer to previously ambiguous questions regarding cross-border data accessibility.[72] On the other hand, civil liberties groups and privacy advocates saw the Act as a violation of basic human rights because it offers inadequate freedom of speech and privacy protections for activists operating in foreign states.[73]

The CLOUD Act gained bipartisan support from members of Congress due to its ability to facilitate law enforcement while providing clarity in regard

---

[69] 18 U.S.C.A. § 2523(d)(4)(B).

[70] Daskal, *supra* note 63, at 14.

[71] *Id.*

[72] *Support for the CLOUD Act of 2018*, MICROSOFT (Apr. 11, 2018), https://blogs.microsoft.com/uploads/prod/sites/5/2018/04/Support-for-the-CLOUD-Act-of-2018_4.11.18.pdf.

[73] Joint letter from Access Now, Advocacy for Principled Action in Gov't, American Civil Liberties Union, Amnesty Int'l USA, Asian American Legal Def. and Educ. Fund (AALDEF), Campaign for Liberty Ctr. for Democracy & Tech., Ctr.Link: The Cmty. of LGBT Ctrs., Constitutional Alliance, Def. Rights & Dissent, Demand Progress Action, Elec. Frontier Found., Equal. Cal., Free Press Action Fund, Gov't Accountability Project, Gov't Info. Watch, Human Rights Watch, Liberty Coalition, Nat'l Ass'n of Criminal Def. Lawyers, Nat'l Black Justice Coal., New America's Open Tech. Inst., OpenMedia, People for the American Way & Restore The Fourth, to U.S. Congress (Mar. 12, 2018) *available at* https://www.aclu.org/letter/coalition-letter-cloud-act [hereinafter Letter from Access Now et al.]. Human rights criticisms are discussed with further detail in Section IV of this Note.

to cross-border data accessibility.[74] It was widely praised among domestic legislators as a much needed update to the antiquities and ambiguities of the SCA.[75]

Most of the major U.S. technology companies (such as Apple, Facebook, Google, Microsoft, and Oath) also voiced support for the CLOUD Act.[76] The above listed companies authored a joint letter that praised the Act as "allow[ing] law enforcement to investigate cross-border crime and terrorism in a way that avoids international legal conflicts."[77] They further suggested that the Act is a necessary means to ensure legal protection for both consumers and data holders in the modern world.[78]

The Act may also be a means for the United States to ensure responsible use of data by foreign states. Some legal academics argue that the periodic compliance review requirement under the CLOUD Act presents a good opportunity to monitor how foreign states are using data and to police potential abuses.[79]

On the other hand, some see the five-year term between periodic compliance reviews as a detriment that threatens human rights.[80] In an essay written by members of the ACLU and Amnesty International, critics sharply rebuked the data sharing executive agreement provision of the CLOUD Act as offering inadequate protection: "the idea that countries can effectively be safe-listed as human-rights compliant, such that their individual data requests need no further human rights vetting—is wrong."[81] Civil rights groups maintain that the current structure of the CLOUD Act puts international human rights activists in danger. They argue that there are no safeguards in situations where a foreign state experiences "rapid deterioration in human rights," such as Turkey in mid-2016 after an attempted coup.[82]

---

[74] Sen. Orrin Hatch, *The CLOUD Act: It's Time for Our Laws to Catch up with Our Technology*, MEDIUM (Feb. 26, 2018), https://medium.com/@SenOrrinHatch/the-cloud-act-its-time-for-our-laws-to-catch-up-with-our-technology-90e90577f5ac.

[75] *See id.*; *see also* Kharazian, *supra* note 11.

[76] Letter from Apple, Facebook, Google, Microsoft & Oath, to U.S. Congress (Feb. 6, 2018) *available at* https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf.

[77] *Id.*

[78] *Id.*

[79] Jennifer Daskal & Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, LAWFARE (Mar. 14, 2018), https://lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

[80] 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://lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them.

[81] *Id.*

[82] *Id.*; Kharazian, *supra* note 11.

Critics also take issue with the level of discretion the Act gives to the executive branch and the vagueness of the standards used to evaluate individual data requests.[83] It is possible that foreign states with good overall human rights protections could abuse the executive agreements on an individual level. For example, Poland is a country with strong political rights and civil liberties protections; therefore, Poland would most likely be able to enter a data sharing executive agreement under the CLOUD Act.[84] But, in 2017, Poland engaged in an abuse of data collection by raiding the offices of several women's rights groups and confiscating hard drives containing sensitive personal data.[85] The CLOUD Act could theoretically be used in a similar capacity—to seize data and stunt the progress of activists and other political opponents.[86]

Proponents of the CLOUD Act counter that it is a step forward in protecting civil liberties because it disincentivizes foreign states from turning to local legislation to avoid the MLAT process.[87] As foreign states became frustrated with the cumbersome MLAT process, they faced pressure to pass laws that mandated data localization, such as requiring all citizens' digital data to be stored within that country's borders.[88] Mandated data localization means all information would be available to foreign governments under local laws. In many countries, that could lead to police access to data "without any judicial process."[89]

Alternatively, foreign states could rely on invasive data collection techniques to get around MLATs, such as expanding surveillance and limiting use of encryption.[90] None of these options are desirable outcomes from a privacy and civil liberties perspective.[91] They infringe upon individual privacy rights and are contrary to the goal of an open internet.[92]

V. FOREIGN REACTION TO THE CLOUD ACT

Section V of this Note illustrates foreign response to the CLOUD Act. This Section looks at the governments of various foreign states, as well as international human rights organizations, to provide a complete picture of the impact passing the CLOUD Act had on the international community. It also provides

---

[83] *See* Guliani & Shah, *supra* note 80.

[84] *Freedom in the World 2018: Poland*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-world/2018/poland (last visited Jan. 9, 2019).

[85] *Poland 2017/2018*, AMNESTY INT'L, https://www.amnesty.org/en/countries/europe-and-central-asia/poland/report-poland/ (last visited Jan. 25, 2020).

[86] Guliani & Shah, *supra* note 80.

[87] Daskal & Swire, *supra* note 79.

[88] *Id.*

[89] *Id.*

[90] Cook, *supra* note 22, at 225–26.

[91] *Id.*

[92] *Id.*

analysis and suggests reasons why foreign governments may have reacted similarly. This Section further explores potential conflicts of laws and other foreign regulations that may be oppositional to the Act.

The Australian government wholly supports the CLOUD Act. Australia released a statement after the law was passed, which complimented the Act's ability to improve law enforcement efficiency while protecting personal data.[93] However, Australia's positive reaction is not consistent with the overall foreign response to this legislation. The general foreign reaction is better characterized as one of uncertainty and unease, especially among the United Kingdom (UK) and other EU member states.[94]

Concerns about the rushed nature of the CLOUD Act and the Act's lack of compatibility with the EU's newly passed General Data Protection Regulation (GDPR) led to a foreign backlash against the Act.[95] EU justice commissioner Vera Jourova described the Act's adoption as a "fast-track procedure, which narrows the room for the potential compatible solution between the EU and the U.S."[96] Another European critic described the CLOUD Act as an "unstoppable weapon" that would allow the United States "to dominate the world" and further argued that data held by U.S. technology companies can no longer be considered secure.[97]

Adoption of the CLOUD Act came at a time when the EU was working toward more robust personal privacy protections of digital data. Two months after the CLOUD Act was signed into law, the EU's General Data Protection Regulation (GDPR), a sweeping privacy regulation, was enacted.[98] The GDPR is a binding piece of legislation that is enforceable in all EU member states.[99] Among other privacy regulations, the GDPR gives citizens in the EU control over their personal data and establishes a right for citizens to demand their personal data be deleted, even if that data is stored in a different country.[100] Another important provision of the GDPR prevents transferring

---

[93] Byron Connolly, *Government Backs New U.S. CLOUD Law*, CIO (Apr. 8, 2018), https://www.cio.com.au/article/635858/government-backs-new-u-cloud-law/.

[94] Dana Heide, Moritz Koch & Dietmar Neuerer, *European Criticism of New US CLOUD Act Mounts*, HANDELSBLATT TODAY (Apr. 24, 2018), https://global.handelsblatt.com/politics/with-new-us-law-how-safe-is-online-data-in-europe-914956.

[95] Nikolaj Nielsen, *Rushed US CLOUD Act Triggers EU Backlash*, EU OBSERVER (Mar. 26, 2018), https://euobserver.com/justice/141446.

[96] *Id.*

[97] Michel Cabirol, *Les Sept Armes Imparables qui Permettent aux États-Unis de Dominer le Monde,* LA TRIBUNE (Nov. 10, 2018), https://www.latribune.fr/economie/international/les-sept-armes-imparables-qui-permettent-aux-etats-unis-de-dominer-le-monde-789141.html.

[98] *The EU General Data Protection Regulation (GDPR) Information Page*, https://eugdpr.org/ (last visited Jan. 9, 2019).

[99] GENERAL DATA PROTECTION REGULATION (GDPR), https://gdpr-info.eu/ (last visited Jan. 25, 2020).

[100] Heide et al., *supra* note 94.

personal data to a foreign state in any manner which is otherwise inconsistent with the GDPR.[101] Any potential conflict between restricted data sharing under the GDPR and the CLOUD Act's reciprocal requirement is further explored in Section VI of this Note.

Likewise, China also has local data sharing regulations that could conflict with the CLOUD Act. The recently enacted Cyber Security Law (CSL) requires sensitive data (e.g., information on Chinese citizens or relating to national security) to be stored domestically on Chinese servers.[102] The law also prohibits Chinese companies from transferring sensitive data to authorities abroad without undergoing clearance from the Chinese government first.[103]

China is not the only foreign state requiring data localization; India recently issued a directive mandating that all data related to financial transactions conducted in India must be stored on local Indian servers.[104] Further, the Indian Parliament is also considering a bill that would require all data collected, shared, or processed in India to be physically stored within India's borders.[105]

The National Assembly of Vietnam recently passed a similar law.[106] This new Vietnamese legislation, which is entitled the Law on Cybersecurity No. 24/2018/QH14 (Cybersecurity Law) and took effect January 1, 2019,[i] requires data localization within the territory of Vietnam.[107] The data localization mandate applies to foreign and domestic enterprises that provide services via the internet in Vietnam and are involved in collection, analysis, and processing of personal data; and data generated by users in Vietnam.[108][109]

Data localization mandates are rationalized based on a fear of unwarranted foreign surveillance and a need to bolster law enforcement by local

---

[101] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 48.

[102] Sophia Yan, *China's New Cybersecurity Law Takes Effect Today, and Many are Confused*, CNBC (May 31, 2017), https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html; *see also* Blackman et al., *supra* note 60, at 14.

[103] Blackman et al., *supra* note 60, at 14.

[104] *Notifications, Storage of Payment System Data*, RESERVE BANK OF INDIA, (Apr. 6, 2018), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0.

[105] Personal Data Protection Act, ch. 2 § 8, Acts of Parliament, 2018 (India).

[106] Hà Vũ, *Toàn Văn Luật An Ninh Mạng Trình Quốc Hội Thông Qua*, VNECONOMY (Dec. 6, 2018), http://vneconomy.vn/toan-van-luat-an-ninh-mang-trinh-quoc-hoi-thong-qua-20 180612081624814.htm.

[107] Thuy Thuy, *Overview of the Law on Cybersecurity*, VCI LEGAL (Aug. 4, 2018), http://www.vci-legal.com/2018/08/overview-of-the-law-on-cybersecurity/.

[108] Nguyễn Lê, *Luật An Ninh Mạng Dã Dược Chỉnh Sửa Thế Nào?*, VNECONOMY (Dec. 6, 2018), http://vneconomy.vn/luat-an-ninh-mang-da-duoc-chinh-sua-the-nao-20180612073002562.htm.

[109] *Id.*

agencies.[110] However, these laws do more harm than good in terms of both privacy rights and data security.[111] Data localization does nothing to curtail foreign surveillance—due to sophisticated data surveillance techniques, physical access is not necessary for international spies to conduct surveillance.[112] Also, data security experts argue these international wrongdoers "are not deterred by new laws; keeping data within a border won't stop those who believe that rules don't apply to them."[113]

Data localization does, however, open the door to privacy abuses from local entities.[114] It also creates a vulnerability to natural disasters destroying all copies of data,[115] increases cost of data storage,[116] and negatively impacts international trade.[117] Additionally, mandated data localization is contrary to the idea of a free internet, which is a value traditionally championed by the United States.[118] It instead leads to a "balkanization" of the internet, fragmenting a once cohesive entity into many separate and distinct versions of the internet spread out across the globe.[119]

Advocates of the CLOUD Act argue that the executive data sharing agreements hold down on mandated data localization; because foreign states could rely on an efficient way to get U.S.-held data, the theory was those states would be more open to allowing their citizens' data to be stored via U.S. companies and extraterritorial servers.[120] However, that desired result was not achieved. The previously discussed data localization efforts in China, India, and Vietnam indicate the CLOUD Act was not successful in deterring recent pushes toward localization.[121] In fact, these Asian countries appear to be doubling down on localization efforts in the wake of the CLOUD Act. Data

---

[110] Ashi Bhat & Suneeth Katarki, *The Debate – Data Localization and Its Efficacy*, MONDAQ (Sept. 17, 2018), http://www.mondaq.com/india/x/736934/Data+Protection+Privacy/.

[111] *Id.*; Frank Heidt, *The Harms of Forced Data Localization*, LEVIATHAN SEC. GRP. (Feb. 25, 2015), https://www.leviathansecurity.com/blog/the-harms-of-forced-data-localization.

[112] Bhat & Katarki, *supra* note 110.

[113] Heidt, *supra* note 111.

[114] Bhat & Katarki, *supra* note 110.

[115] Heidt, *supra* note 111.

[116] Letter from Daniel Castro, Vice President, Info. Tech. and Innovation Found., Nigel Cory Assoc. Dir., Info. Tech. and Innovation Found. & Alan McQuinn, Senior Policy Analyst, Info. Tech. and Innovation Found., to Fiona Alexander, Assoc. Adm'r, Nat'l Telecomm. and Info. Admin., U.S. Dep't of Commerce (July 17, 2018), *available at* http://www2.itif.org/2018-international-internet-priorities.pdf); *see also* Bhat & Katarki, *supra* note 110.

[117] Erica Fraser, *Data Localisation and the Balkanisation of the Internet*, 13 SCRIPTED 359, 368–69 (2016).

[118] Cook, *supra* note 22, at 226.

[119] Fraser, *supra* note 117, at 361–62.

[120] Cook, *supra* note 22.

[121] Yan, *supra* note 102; RESERVE BANK OF INDIA, *supra* note 104; Thuy, *supra* note 107.

localization mandates show that, even under the CLOUD Act's regime, foreign states are hesitant to allow free access by the United States to their local data.

Much like many foreign governments, international human rights organizations are also made uneasy by the CLOUD Act's potential to spread personal data across borders.[122] There are no major international human rights groups that support the Act.[123] Amnesty International's U.S. director Naureen Shah expressed "grave misgivings" for the CLOUD Act, stating that it "jeopardizes the lives and safety of thousands of human rights defenders."[124] Similarly, Human Rights Watch, which is a nonprofit organization that investigates and reports on human rights abuses across the globe, argues the new international data sharing process under the Act gutted prior human rights protections.[125]

The main issues that human rights advocates have with the CLOUD Act are directed at the executive agreements section; more specifically, the five-year window between U.S. compliance reviews and the concentration of power solely in the executive branch are causes for concern.[126] The lengthy amount of time between U.S. evaluations of a foreign state's privacy and human rights protections could allow a once-compliant nation to rapidly deteriorate and abuse data collection for an extended period between compliance reviews.[127] Some critics also argue that there is risk the U.S. government will enter into these executive agreements for political reasons, even if the foreign state is known to abuse privacy rights.[128] That risk is further exacerbated by the lack of congressional input into the validity of the executive agreements.[129]

VI. PROPOSED AMENDMENTS TO THE CLOUD ACT

The remaining portion of this Note focuses on proposed amendments to the CLOUD Act's executive agreements provision. The intent is to provide legislators with suggestions of how to adjust the law in order to better foster positive international relations, further encourage foreign states to participate

---

[122] Guliani & Shah, *supra* note 80.

[123] *Id.*

[124] Adam Klasfeld, *Human Rights Groups Denounce Proposed Global Data Sharing*, COURTHOUSE NEWS SERV. (Mar. 16, 2018), https://www.courthousenews.com/privacy-groups-denounce-proposed-global-data-sharing/.

[125] Sarah St.Vincent, *US May Give Foreign Governments – and Itself – Easier Access to Data*, HUM. RTS. WATCH (Feb. 13, 2018), https://www.hrw.org/news/2018/02/13/us-may-give-foreign-governments-and-itself-easier-access-data.

[126] Guliani & Shah, *supra* note 80; *see also* St. Vincent, *supra* note 125.

[127] Guliani & Shah, *supra* note 80.

[128] St. Vincent, *supra* note 125.

[129] Guliani & Shah, *supra* note 80.

in these agreements, and provide more stringent protections for international human rights.

The proposed amendments are suggestions to improve the CLOUD Act; however, this Note does not take the position that the Act is a harmful piece of legislation. On the contrary, this Note argues the Act represents positive change. The CLOUD Act is necessary for effective law enforcement in the modern world. Though digital forensics and collection of digital evidence are relatively new concepts for law enforcement, investigators rely heavily on digital data in modern criminal investigations.[130] Because data management systems are complex and much of this important data is stored across the globe,[131] law enforcement must frequently obtain digital evidence that is physically stored in a foreign state. The already overburdened MLAT process was not equipped to handle collection of data for criminal investigations; a ten-month delay in the investigation, caused by relying on MLATs, cannot yield effective law enforcement.[132]

The CLOUD Act's extraterritorial application of SCA warrants improved accessibility and solved the time delay problem involved with criminal investigations on a domestic level. It relieved the strain placed on the overburdened MLAT system and made clear that U.S. law will apply in evidence collection where a U.S. technology company has custody of the digital data.

The concerns raised by privacy advocates are not as potent when evaluating domestic investigations. United States law, and its robust privacy protections under the Fourth Amendment, still apply to extraterritorial SCA warrants.[133] The full process must be satisfied, including showing a finding of probable cause.[134] Even though the United States would not be required to follow the exact law of the foreign state where the evidence was physically stored, it still would safeguard against abuses through its own privacy protections. There is little fear that applying SCA warrants extraterritorially will lead to domestic privacy abuses within the boundaries of the United States. In fact, the ACLU and other human rights organizations aim their privacy criticisms solely at the executive agreements provision of the CLOUD Act, not its application to SCA warrants.[135]

It makes logical sense that U.S. law would apply in digital evidence collection for an alleged crime against the United States, where a U.S. company has control over the evidence—regardless of the data storage facility's

---

[130] Goodison et al., *supra* note 2.

[131] Anand, *Lessons to Learn From How Google Stores Its Data*, SMART DATA COLLECTIVE (July 7, 2016), https://www.smartdatacollective.com/lessons-learn-how-google-stores-its-data/.

[132] THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., *supra* note 37, at 227.

[133] 18 U.S.C.A. § 2713 (2018).

[134] *Id.*

[135] Guliani & Shah, *supra* note 80.

geographic location. The United States government, most major U.S. technology companies, and many legal academics all agree that SCA warrants applying to data physically stored outside of the United States is a positive, necessary step aligned with the needs of modern technology.[136]

Conversely, there is room to improve the second function of the CLOUD Act: its executive agreements provision. The idea to create a means for foreign states to enter mutual agreements that allow for easier data sharing across borders is a positive change; however, the CLOUD Act misses the mark on various functional points.

The Act was a rushed piece of legislation, buried as part of a larger spending bill and passed without thorough vetting or consideration on international impact.[137] This is the reason for the overall negative response from foreign governments and international human rights groups regarding these new executive agreements.[138] There also exists domestic distrust regarding these executive agreements.[139] However, with a few key changes suggested below, the data sharing agreements could be improved without hindering their functionality.

A. Mandatory Annual Compliance Review

Human rights protections are an important consideration when discussing cross-border data sharing agreements because increased data accessibility could potentially infringe on the right to privacy.[140] Therefore, only foreign states with adequate human rights protections and privacy protections should be permitted to participate in these agreements. The CLOUD Act recognized the need for stringent protections; thus, the Act imposed a lengthy set of human rights prerequisites on foreign states looking to enter an executive agreement.[141] Both the U.S. Attorney General and Secretary of State certify in writing with an accompanying explanation that the foreign state has adequate privacy and civil liberties protections before an executive agreement may exist with that foreign state.[142]

---

[136] Stephen P. Mulligan, Cong. Research Serv., R45173, Cross-Border Data Sharing Under the CLOUD Act (2018), https://fas.org/sgp/crs/misc/R45173.pdf; Letter from Apple, et al., to U.S. Congress, *supra* note 76; Daskal & Swire, *supra* note 79.

[137] Ruiz, *supra* note 50.

[138] Nielsen, *supra* note 95; St. Vincent, *supra* note 125.

[139] Guliani & Shah, *supra* note 80.

[140] U.N. Human Rights Office of the High Comm'r, *A Human Rights-Based Approach to Data: Leaving No One Behind in the 2030 Agenda for Sustainable Development* (2018), https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf.

[141] 18 U.S.C.A. § 2523(b) (2018).

[142] *Id.*

However, the U.S. government's evaluation of a foreign state's human rights compliance is insufficient. Evaluation of privacy and civil liberties protections occurs prior to entering the agreement, with follow-up compliance reviews in subsequent five-year intervals.[143] This process effectively whitelists foreign states as human rights compliant for an extended period; it allows continued access to data, even in situations where a state experiences rapid decline in its human rights protections.[144] To combat this problem, mandatory reviews of the foreign state's privacy and human rights protections should occur once every year.

Following an attempted coup in 2016, Turkey declared an ongoing state of emergency and waged war on all government criticism.[145] The Turkish government imprisoned hundreds of journalists and media workers, raided offices of human rights organizations, disrupted peaceful protests, and tortured activists in police custody.[146] This drastic decay of human rights protections occurred within one year.[147] If Turkey had an executive data sharing agreement with the United States prior to these events, the current compliance review scheme under the CLOUD Act would be insufficient to diagnose and prevent abuses in data collection. Events in Turkey illustrate that a five year window between compliance reviews will not safeguard against a foreign state that bottoms out its human rights protections within those five years.

More frequent compliance reviews are necessary to prevent abuse. While it is true that increased resources would be required to administer more frequent compliance reviews, the additional protection would be worth any marginal inconvenience. Further, there are methods that could help facilitate administrability; for example, the process could include an incentive program that makes the burden of showing compliance lighter for foreign states with a demonstrated history of high protections on privacy and human rights.[148] Annual compliance reviews under this proposed system would keep a closer watch for data collection abuses, while still maintaining an efficient level of administrability. Further, the level of administrability would still be far superior than its predecessor, the MLAT system.[149]

Annual compliance reviews would have the further benefit of collecting more results on compliance trends, which would give the U.S. government an

---

[143] 18 U.S.C.A. § 2523(e).

[144] Guliani & Shah, *supra* note 80.

[145] *Turkey 2017/2018*, AMNESTY INT'L, https://www.amnesty.org/en/countries/europe-and-central-asia/turkey/report-turkey/ (last visited Jan. 25, 2020).

[146] *Id.*

[147] *Id.*

[148] ORG. FOR ECON. CO-OPERATION & DEV., REDUCING THE RISK OF POLICY FAILURE: CHALLENGES FOR REGULATORY COMPLIANCE (2000), https://www.oecd.org/gov/regulatory-policy/1910833.pdf

[149] THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., *supra* note 37, at 227.

opportunity to identify overall problem areas and evaluate whether the regulations baked into the CLOUD Act had the desired effect on foreign states.[150]

In addition, the main contention international human rights groups, such as the ACLU and Amnesty International, have with the CLOUD Act is its relatively infrequent compliance reviews of human rights protections.[151] Changing to an annual compliance review model would help appease these groups and may even garner their support for changes made under the CLOUD Act, which could improve foreign reaction to the executive agreements and encourage adoption.

B. Congressional Approval of Executive Agreements

As its name suggests, executive agreements under the CLOUD Act are almost entirely within the purview of the executive branch. The judiciary is taken out of this process through statutory language that expressly eliminates judicial review.[152] Similarly, the legislature's role is severely limited. Congress has 180 days from notice of the agreement to pass a joint resolution of disapproval in both the House of Representatives and the Senate;[153] otherwise, Congress has no recourse to challenge these executive data-sharing agreements. The CLOUD Act is an example that highlights the common phenomenon of international agreements made by the executive branch acting alone, which also raises questions about separation of powers and equitable international lawmaking.[154] A better approach is to require congressional approval of each individual data sharing agreement, while creating a "fast track" system that would streamline the process. Congressional supervision would create a more balanced, democratic, and effective approach without sacrificing much efficiency.

There is no problem with the CLOUD Act expressly eliminating judicial review. In accordance with the political question doctrine, the judicial branch defers on issues related to international agreements approved by Congress.[155] As the Eleventh Circuit Court of Appeals stated in *Made in the USA Foundation v. United States*, "the choice of what procedure to use for a given agreement is committed to the discretion and expertise of the Legislative and

---

[150] ORG. FOR ECON. CO-OPERATION & DEV., *supra* note 148, at 49.

[151] Letter from Access Now et al., *supra* note 73.

[152] 18 U.S.C.A. § 2523(c) (2018).

[153] 18 U.S.C.A. § 2523(d)(2).

[154] Oona A. Hathaway, *Presidential Power over International Law: Restoring the Balance*, 119 YALE L.J. 140, 146 (2009).

[155] John H. Knox, *The United States, Environmental Agreements, and the Political Question Doctrine*, 40 N.C. J. INT'L L. & COM. REG. 933, 954 (2015).

Executive Branches by virtue of the political question doctrine."[156] Therefore, statutory language eliminating judicial review in the context of cross-border data sharing executive agreements is proper; it puts an articulable point on a concept already followed by the courts.

Congressional involvement in executive agreements, however, is necessary to ensure democratic accountability. Unfortunately, congressional involvement is typically limited in the context of international agreements. The legislature's role in conducting international agreements was evaporated post-World War II by a systematic yielding of power to the President.[157] Congress passed a wide variety of statutes, many of which were vague and open-ended, that allowed the President to put executive agreements into force without further legislative involvement.[158]

Agreements enacted by the executive branch under advanced authority granted by Congress are often called "*ex ante*" congressional-executive agreements, and they account for approximately eighty percent of all U.S. international legal commitments.[159] Executive agreements under the CLOUD Act are examples of *ex ante* congressional-executive agreements.

Utilizing *ex ante* congressional-executive agreements presents a problem because it centralizes international lawmaking ability within the executive branch.[160] Congress has very little power regarding these agreements.[161] In theory, Congress has the power to adjust *ex ante* congressional-executive agreements through passing subsequent legislation; however, this is rarely achieved in reality because any effort to revoke or limit executive power can be vetoed by the President.[162]

Some argue that this change is a good thing, that international agreements are best left to the sole discretion of the executive branch. They contend that separation of powers concerns are not as strong when the consequences mostly affect institutions outside the United States.[163] Further, they assert that sole executive power might have the added benefits of ensuring consistent leadership in foreign relations while giving the President stronger negotiating power.[164]

---

[156] Made in the USA Found. v. United States, 242 F.3d 1300, 1311 (11th Cir. 2001) (constitutionality of the North American Free Trade Agreement was a nonjusticiable political question).

[157] Hathaway, *supra* note 154, at 144–45.

[158] *Id.*

[159] *Id.*

[160] *Id.* at 149–150.

[161] *Id.* at 145.

[162] *Id.*

[163] Curtis A. Bradley & Jack L. Goldsmith, *Presidential Control over International Law*, 131 HARV. L. REV. 1201, 1252–53 (2018).

[164] Hathaway, *supra* note 154, at 230.

These arguments are misguided. Even though executive agreements deal with institutions and actors beyond U.S. borders, unilateral international lawmaking by the executive branch produces significant domestic impact.[165] The United States is held to follow the rules of foreign interaction prescribed by the President—he or she alone dictates how the rest of the country must act regarding many matters such as foreign commerce and diplomacy.[166]

Additionally, placing all international lawmaking power on the President does not lead to more effective lawmaking. Creating effective international law requires adequate political support to ensure that international commitments created under the agreements are actually performed.[167] While agreements negotiated by the president acting alone may be easier to create, those agreements are less likely to be followed. For example, a subsequent presidential administration might withdraw from or fail to observe an agreement made by a previous president acting on their own. That same subsequent administration would be much more cautious about failing to honor an agreement that was passed with consent of Congress.[168]

Placing the power to conduct international lawmaking in a single branch of government also violates separation of powers. Government power must be divided into separated institutions; the system is designed to prevent the distinct branches of government from controlling the functions of other branches.[169] *Ex ante* congressional-executive agreements, such as agreements under the CLOUD Act, completely destroy this purpose by giving the executive branch the ability to create international law. The President is given the ability to "write" international laws by exercising sole discretion over which foreign states will have an executive data sharing agreement with the United States. Creating laws is a power of the legislative branch of the U.S. government. Even though the President is, in effect, creating international law, the executive branch remains immune from democratic accountability. There is potential risk that a President could use executive agreements as political tools, even if those agreements are contrary to democratic interests.

The risk of politicizing executive agreements is especially dangerous in the context of data sharing. As discussed previously, the CLOUD Act authorizes agreements that are integral to aiding modern law enforcement; presidents may use these highly desirable agreements as bargaining chips to advance political agendas. However, these agreements are also volatile because of the sensitivity of information and risk that governments could use that

---

165 Bradley & Goldsmith, *supra* note 163, at 1253.

166 *See id.* (discussing in detail the various impacts unilateral presidential international lawmaking has on all forms of domestic institutions, including later presidents, Congress, courts, states, American individuals and private firms.)

167 Hathaway, *supra* note 154, at 231.

168 *Id.* at 232.

169 Jack M. Beermann, *An Inductive Understanding of Separation of Powers*, 63 ADMIN. L. REV. 467, 468 (2011).

information to abuse human rights; this is the reason each agreement is scrutinized through robust human rights protections. Nonetheless, it is easy to imagine situations where a president might bend the rules on enforcing human rights protections in order to push through an executive data sharing agreement that would result in political gain.

If this type of misbehavior occurred, Congress would be powerless to stop it. The only recourse available to Congress (or any other entity) would be to pass subsequent legislation, which the President could veto. Abuses in creating cross-border data sharing agreements are egregious because they result in threats against the privacy and safety of people across the globe. It is imperative for the United States to take all reasonable measures in order to protect against those abuses, including congressional approval of each agreement as a check on executive power.

Congressional approval of the individual agreements would add a step to the process, but it would not result in a substantial loss of efficiency if a "fast track" procedure was adopted. This type of expedited approval is sometimes used in the context of trade agreements.[170]

The fast track procedure required the leaders of the House and Senate to introduce trade agreements proposed by the President on the same day the agreement was submitted or on the next day possible if a house was not in session.[171] The agreement could not be amended,[172] debate on the agreement was limited to "not more than 20 hours" in each house,[173] filibusters were not permitted in the Senate,[174] and the agreement would pass by a simple majority vote in each house.[175] These votes were required to take place "on or before the close of the 15th day" after the implementing bill or approval resolution was reported out of committee.[176]

A similar procedural framework could speed up the congressional approval process of executive data sharing agreements. Though fast track has

---

[170] The fast track process was first created in the Trade Act of 1974, Pub. L. No. 93-618, §§ 151–154, 88 Stat. 1978, 2001-08 (codified as amended at 19 U.S.C. §§ 2191–2194 (2015)). The Trade Act of 2002 extended and conditioned application of the process, but its fast track authority ultimately expired in July 2007. Pub. L. No. 107-210, §§ 2103–2105, 116 Stat. 933, 1004-16 (codified as amended at 19 U.S.C. §§ 3803-3805 (Supp. 2006)). In 2015, the Bipartisan Congressional Trade Priorities and Accountability Act once again created fast track authority. It currently allows fast track to be used for legislation to implement trade agreements reached before July 1, 2021. Pub. L. 114-26, title I, §110(a)(6), June 29, 2015, 129 Stat. 358.

[171] 19 U.S.C.A. § 2191(c)(1) (2015).

[172] 19 U.S.C.A. § 2191(d).

[173] 19 U.S.C.A. § 2191(f)–(g).

[174] 19 U.S.C.A. § 2191(f)–(g).

[175] 19 U.S.C.A. § 2191(f)–(g).

[176] 19 U.S.C.A. § 2191(e)(2). In addition, each house's committee was required to report a bill or resolution no later than the close of the 45th day after the proposed agreement was introduced, pursuant to 19 U.S.C.A. § 2191(e)(2).

never been used outside the scope of trade agreements, legal academic Oona Hathaway argues that a fast track process could apply to "approval of international agreements in any area of international law."[177] Therefore, this process could be adopted on a narrow basis to facilitate congressional approval of cross-border data sharing executive agreements under the CLOUD Act and any other agreement that involves sharing of sensitive personal data. Narrowing the scope of the fast track process would limit inefficiency by not burdening Congress with approval of every executive agreement.

While the features of a fast track process (such as limited debate and prohibition of amendments) may seem disadvantageous to Congress, fast track would still provide Congress with an important check on executive power. It would do so in a way that is easy to administer and would not sacrifice efficiency, while also protecting against abuses in creating these potentially dangerous data sharing agreements.

The risk of politicizing executive data sharing agreements requires implementation of a congressional approval system. A fast track procedure, similar to what has been previously utilized in trade agreements, is the most efficient way to do so. Adding this protection might not have a huge impact on affecting foreign perception of the changes made under the CLOUD Act; however, a congressional approval protection is an important measure to ensure separation of powers and equitable international lawmaking. Both of those concepts have the potential to cause a major impact on both a domestic and international scale.

C. Eliminate Reciprocal Data Sharing Requirement for Executive Agreements

Included in the CLOUD Act's executive agreement provision is a reciprocal data sharing requirement.[178] In order to enter an executive agreement, the foreign state must grant the U.S. reciprocal access to data held by the foreign state.[179] This requirement presents a problem because compliance with reciprocal data sharing could be contrary to local laws of the foreign state.[180] The EU's recently passed GDPR makes it unlawful to transfer data unless certain conditions are met.[181] With mandated reciprocal data sharing, situations could arise where an EU member state would be forced to compel a local service

---

[177] Hathaway, *supra* note 154, at 264.

[178] 18 U.S.C.A. § 2523(b)4(I) (2018).

[179] *Id.*

[180] *See, e.g.*, Yan, *supra* note 102.

[181] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1Regulation (EU) 2016/679 of the European Parliament (GDPR), arts. 44–49.

provider to turn over data to the United States when that transfer would otherwise be unlawful under the GDPR.

Article 48 of the GDPR does carve out an exception that allows transfers made pursuant to an international agreement, such as an MLAT.[182] But it is not yet known whether executive agreements under the CLOUD Act will satisfy Article 48.[183] Because the executive agreements would offer fewer privacy protections on an individual level, GDPR protection authorities could determine the CLOUD Act agreements are inconsistent with the protections contemplated by Article 48.[184]

China enacted the Cyber Security Law (CSL) in 2017,[185] which is a robust piece of legislation intended to prevent cyberattacks and protect data privacy. Article 37 of the CSL requires personal and other important information to be physically stored on servers in China; it also prevents transferring that data abroad without prior approval and a security assessment from Chinese regulators.[186] This is another example of a conflict between the CLOUD Act and local laws of a foreign state. Even though a CLOUD Act executive agreement would require China to reciprocally share their data with the United States, the CSL would prohibit them from doing so.

Forced reciprocity among data-sharing agreements may contribute to the unease many foreign states have for these agreements. The majority of the world's digital data is held by U.S. technology companies,[187] so the United States has a bargaining chip to entice foreign states into an executive data-sharing agreement. However, to get easier access to this wealth of U.S. held data, the foreign state must also make data held by its entities available to the U.S. The EU, China, and other countries that have recently increased data protections might see this as invasive. These countries, and many others, are avoiding measures that liberalize cross-border data accessibility (such as the CLOUD Act executive agreements) and instead are restricting data flow through laws that block cross-border transfers and mandate data localization.[188]

---

[182] *Id.*

[183] Bart W. Huffman, Cynthia O'Donoghue, Andreas Splittgerber, Sheek Shah & Maxwell J. Eichenberger, *Potential Conflict and Harmony Between GDPR and the CLOUD Act*, REED SMITH (June 14, 2018), https://www.reedsmith.com/en/perspectives/2018/06/potential-conflict-and-harmony-between-gdpr-and-the-cloud-act.

[184] *Id.*

[185] *China's cybersecurity Law and its Impacts - Key Requirements Business Need to Understand to Ensure Compliance*, PROTIVITI (2017), https://www.protiviti.com/CN-en/insights/china-cybersecurity-law-and-impacts.

[186] Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 79 (2018).

[187] Zarine Kharazian & Bruce Zagaris, *Cross-Border Law Enforcement Access to E-Evidence: The State of the Playing Field After the Passage of the U.S. CLOUD Act*, 34 No. 10 INT'L ENF'T L. REP. 518 (2018).

[188] Yan, *supra* note 102; RESERVE BANK OF INDIA, *supra* note 104; Thuy, *supra* note 107.

Restricting data accessibility fractures the digital world and leads to undesirable outcomes. When all data is forcibly stored in one state, there is increased risk of privacy abuses from the government of that state or other entities.[189] Restricted data accessibility also restricts international trade[190] and increases data storage costs.[191] The United States must do everything it can to ensure effective accessibility of data across borders, which includes encouraging adoption of as many data sharing agreements as possible.

Some may have a gut reaction that it is "unfair" to provide foreign states with easier access to U.S.-held data without receiving reciprocal access, but reciprocal data sharing does not have much value to the U.S. because most digital data is already held by U.S. technology companies,[192] and the CLOUD Act gives the United States easy access to that data, regardless of where it is physically stored, through SCA warrants.[193] In the rare instances where the United States needs access to data held by a foreign company in a foreign state, the United States can still rely on MLATs to retrieve the data.[194]

More positive outcomes for the U.S. would be achieved through eliminating the reciprocal data sharing requirement of CLOUD Act executive agreements. If foreign states did not have the pressure of reciprocal data sharing, they would be further incentivized to join in these agreements; there would be no reason for any qualified country not to have an agreement with the U.S.

Entering into agreements with as many foreign states as possible is in the best interests of the United States because it would improve foreign perception of the CLOUD Act, encourage adoption of these executive agreements, discourage mandated data localization laws, and thus encourage foreign states (and the people in foreign states) to use U.S. technology companies. This would ultimately give the United States better accessibility to more data than would be achieved by reciprocation under the executive agreements.

D. Notice Requirement

The right to notice when a search warrant is executed and personal property is seized is a common principle of U.S. law.[195] A notice requirement is important because it affords the owner of the property due process and allows

---

189 Bhat & Katarki, *supra* note 110.

190 Fraser, *supra* note 118, at 368.

191 Letter from Daniel Castro et al., to Fiona Alexander, *supra* note 116, at 4–5; Bhat & Katarki, *supra* note 110.

192 Kharazian & Zagaris, *supra* note 187.

193 18 U.S.C.A. § 2713 (2018).

194 Mulligan, *supra* note 136, at 23.

195 *See* City of West Covina v. Perkins, 525 U.S. 234, 240 (1999) (imposing notice requirements when officers executing a search warrant seize property).

him or her to manage or retrieve the seized property.[196] It follows that the same principle would apply when an SCA warrant is executed and personal data is seized. While there may be an argument that the notice requirement under U.S. law would apply to domestic search warrants, the executive agreement provision does not have a notice requirement.[197] The CLOUD Act does not require notice to be provided to a foreign person whose data is targeted and seized via an executive data sharing agreement.[198]

A requirement of notice when personal property is taken (including personal data) is a phenomenon adopted by many countries around the world. In fact, over 100 countries have data protection laws, and many of those laws include a right to notice.[199]

The EU and its member states are particularly concerned with data privacy and providing citizens autonomy over their personal data.[200] In addition to severely limited circumstances imposed by the GDPR that restrict when personal data can be collected and transferred across international borders,[201] the GDPR also expands the type of notice data owners must receive when their data is transferred.[202]

Asian, Latin American, and African countries also have their own notice requirements and data protection obligations.[203] These laws tend to have some commonality, inclusive of a notice requirement.[204] Generally speaking, notice requirements in these nations typically consist of notifying the data owner of "what personal information is collected, why it is collected, and with whom it is shared."[205]

Notice is an important concept to many foreign states in the context of collecting and sharing personal data. Because of this, the CLOUD Act executive agreements provision should be amended to include a notice requirement. When personal data is transferred via an executive data-sharing agreement, the owner of that data should be notified of the process. At minimum, notice

---

196 *Id.*

197 *The CLOUD Act*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/cloud-act/ (last visited Jan. 11, 2019).

198 *Id.*

199 John P. Carlin, James M. Koukios, David A. Newman & Suhna N. Pierce, *Data Privacy and Transfers in Cross-Border Investigations*, GLOB. INVESTIGATIONS REV. (Aug. 9, 2017), https://globalinvestigationsreview.com/benchmarking/the-investigations-review-of-the-americas-2018/1145431/data-privacy-and-transfers-in-cross-border-investigations.

200 *Id.*

201 *Id.*; Section V, subsection B of this Note discusses potential conflicts between the CLOUD Act and these restrictions of the GDPR.

202 Carlin et al., *supra* note 199.

203 *Id.*

204 *Id.*

205 *Id.*

of what personal data was accessed and that the government has the data should be required when a request under a data-sharing agreement is fulfilled.

Adopting this type of notice requirement would stay in line with the data protection schemes that many countries have across the globe.[206] It would reduce potential conflicts of laws by ensuring data transfers under executive agreements were held to the same or similar data protection restrictions of the particular jurisdiction.

Adding a notice requirement would also make executive data sharing agreements under the CLOUD Act more appealing to foreign states and the people of those nations. Because the constituents of a foreign state are better protected and informed through a notice requirement, adding this measure will likely lead to greater local support among a foreign state. A notice requirement would also reduce complexity by remedying potential conflicts of laws, provide clearer expectations, and help demonstrate government transparency within a foreign state.

All of these benefits suggest that a notice requirement would incentivize adoption of executive data-sharing agreements. As discussed in Section V, Subsection C of this Note, the interests of the U.S., and the international community at large will be best served by encouraging the adoption of international agreements and eliminating the need for alternative, harmful measures such as mandated data localization.

VII. CONCLUSION

The CLOUD Act was a necessary piece of legislation that solved data access problems faced by modern law enforcement. Due to changes in technology, the prior version of the SCA was insufficient, and changes affected by the CLOUD Act needed to be made. Cloud storage and complex data management systems necessitate extraterritorial application of SCA warrants.

It is unreasonable to require law enforcement to rely on cumbersome, time-consuming MLATs when conducting criminal investigations. A ten-month delay on received data via MLAT is detrimental to criminal investigations; modern law enforcement could not operate effectively under that system. Extraterritorial SCA warrants solve the time delay problem by streamlining the process, while keeping in line with the intentions of the SCA.

The executive data-sharing agreements allowed by the CLOUD Act also have potential to be meaningful tools in the modern world. They can facilitate data-sharing across borders and ensure that the internet continues to be one open, free-flowing entity. Productive results such as these are the reason many people and entities in the U.S. support the CLOUD Act.

Without data-sharing agreements of this kind, foreign states turn to other, more harmful methods to regulate data. Measures such as mandated data

---

[206] *The CLOUD Act*, *supra* note 198.

localization "balkanize" the internet and lead to host of other issues including negative impact on international trade, increased data storage costs, and greater susceptibility to destruction of data by natural disasters. It is imperative that the U.S. uses all means available to improve these executive agreements and encourage their adoption. Utilizing responsible cross-border data sharing agreements is a better way to ensure proper management of data on an international level, compared to the potentially harmful alternatives.

Though the Act was met by mostly positive reaction from domestic institutions, there were some domestic entities that criticized the Act as offering a means for foreign states to abuse civil liberties while offering inadequate protections on human rights. The domestic criticisms of the CLOUD Act pertain to the executive agreements provision. Therefore, improving executive agreements to better protect privacy and civil liberties of foreign persons would have the added benefit of improving domestic perception and support for the Act.

Overall foreign response to the CLOUD Act was not positive; many foreign states were uneasy about the Act, seeing it as an extension of United States power into the international sphere. These concerns could be alleviated through improvements to the executive agreements provision of the Act.

The CLOUD Act is a good start, but it's an imperfect document. Several key amendments to the Act could improve upon it and help alleviate the concern expressed domestically and abroad. Mandatory annual compliance reviews would improve the CLOUD Act because they would ensure that only foreign states who maintained human rights and privacy protections could access sensitive data.

A compliance review of these protections conducted every year would defend against a country that experiences a rapid decline in human rights; more frequent compliance reviews would prevent "whitelisting" foreign states as human rights compliant for extended periods of time.

Congressional approval of each individual agreement is another change that would improve the CLOUD Act's executive agreements provision. Centralizing the ability to enter the agreements solely within the purview of the executive branch violates separation of powers and is not an effective means of international lawmaking. Due to the sensitivity of information distributed under these agreements and its desirable nature, a risk exists that the executive branch could abuse the agreements for political gain. Congress must be involved in order to inject democratic accountability into the process while providing a check on presidential power. Congress could achieve this purpose without sacrificing efficiency by adopting a "fast track" method to approve the agreements.

The CLOUD Act would also be improved by removing the reciprocal data-sharing requirement. For the reasons stated previously, it is important for the U.S. to encourage foreign states to adopt executive data sharing agreements. Fear over U.S. access to data is a main factor in the overall foreign unease

surrounding the CLOUD Act; that fear will be a barrier to encouraging adoption of these agreements. The U.S. will not get much benefit from reciprocal data-sharing because most of the world's data is already held by U.S. companies, and thus accessible to the United States via SCA warrants.

The U.S. would receive more benefit from the increased adoption of executive data-sharing agreements than the reciprocal requirement, which is hindering the agreements' adoption. Without a reciprocal data-sharing requirement, foreign states previously focused on data localization may even be incentivized to allow use of U.S. technology company services—which would lead to more people in those countries using U.S. technology services and in turn would give the U.S. greater access to that data in the long run.

Finally, a notice requirement should be added that would require the owner of any personal data to be notified when a transfer via executive agreement is fulfilled. This measure would reduce conflict of laws issues, improve local approval of data-sharing agreements, and foster government transparency in the foreign state.

These changes would lead to increased positive reaction to the Act, better foreign relations, and more robust international human rights protections. They would also encourage maintaining an open internet and disincentivize laws in foreign states that mandate data localization.

The CLOUD Act is already a domestic success. Most people within U.S. borders support it and the changes it represents. Although foreign reaction is not as favorable, minor changes in the CLOUD Act could go a long way in bettering its international impact. The amendments expressed in this Note will help improve domestic impression, while also bettering the Act's international impact and its role in U.S. foreign relations. Nevertheless, the CLOUD Act is an important piece of legislation in the modern era of digital data proliferation, and it will affect meaningful change on a global scale.