2021

Navigating in the Clouds: The Triumphs and Drawbacks of the CLOUD Act

Jia Zhang

Navigating in the Clouds: The Triumphs and Drawbacks of the CLOUD Act

Jia Zhang*

I. Introduction

As the world grew increasingly infatuated with cloud computing, users abandoned traditional storage methods and "entrusted" their data to network servers of communications service providers ("CSPs").[1] Along with convenience and cost-saving advantages, cloud storage presented issues in the area of cross-border data access that demanded attention from lawmakers. In particular, as cross-border data requests increased exponentially, foreign governments expressed frustrations over the lengthy process to obtain electronic information held by U.S.-based CSPs as well as the stringent U.S. legal standards they must overcome.[2] Moreover, a CSP often encounters conflicting situations where compliance with one country's data request may infringe on another country's privacy guarantees.[3] In other words, the law of the requesting country may command disclosure while the receiving country's law forbids it, or vice versa.[4]

The nature of cloud computing itself has also generated headaches for law enforcement. Some of the largest CSPs, many of which headquartered in the United States,[5] have a global presence and operate networks of data storage centers in many different countries. Frequently, data is not permanently stored in one location but travels across borders randomly and automatically.[6] This has generated jurisdictional

* J.D. Candidate, 2021, Seton Hall University School of Law; B.A., *magna cum laude*, 2017, Rutgers University, the State University of New Jersey.

[1] *See, e.g.*, U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World, White Paper, 2–3 (Apr. 2019), https://www.justice.gov/opa/press-release/file/1153446/download [hereinafter White Paper]; Andrew Keane Woods & Peter Swine, *The CLOUD Act: A Welcoming Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018, 5:49 PM), https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems.

[2] *See* Derek B. Johnson, *CLOUD Act Set to Pass in Omnibus*, FCW (Mar. 22, 2018), https://fcw.com/articles/2018/03/22/cloud-act-omnibus-johnson.aspx.

[3] White Paper, *supra* note 1.

[4] *See* 18 U.S.C. §101(4) (2018).

[5] The top three cloud providers, Amazon Web Services, Microsoft Azure, and Google Cloud Platform, as of 2019, are all U.S.-based companies. Larry Dignan, *Top Cloud Providers 2019: AWS, Microsoft Azure, Google Cloud; IBM Makes Hybrid Move; Salesforce Dominates SaaS*, ZDNET (Aug. 15, 2019), https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/.

[6] *See* Javier Lopez Gonzalez, *Hitchhiker's Guide to Cross Border Data Flows*, OECD (June 19, 2019), https://www.oecd.org/trade/hitchhikers-guide-cross-border-data-flows ("With the adoption of cloud computing, data lives in many places at once with different bits of data or copies of data stored in different countries simultaneously.").

problems for law enforcement in their effort to track down such data, particularly when the nature of the crime is serious, and the circumstances are urgent.[7] Adding to the aggravation, some U.S.-based CSPs resisted access altogether, arguing that the requested data was technically under the control of a foreign jurisdiction and outside the reach of U.S. courts.[8]

To resolve this set of difficulties unique to the digital age, Congress enacted the Clarifying Lawful Overseas Use of Data Act ("the CLOUD Act") in March 2018.[9] The CLOUD Act aims to aid qualifying foreign countries in their investigation of serious crimes by speeding up access to electronic data held by U.S.-based CSPs.[10] It contains two major components. First, it authorizes the U.S. government to form bilateral executive agreements with foreign governments that satisfy a set of criteria in order to bypass any conflict of law problems.[11] Second, it amends the Stored Communications Act of 1986 by expressly stating that a company subject to requests from a partner nation must disclose the information in its "possession, custody, or control" *regardless of* whether the communication is "stored" inside or outside the United States.[12]

While the CLOUD Act appears to favor law enforcement by providing smoother access to private data, its enforcers have declared a commitment to preserve privacy interests of individuals and carefully avoid any legal challenges in this regard.[13] The Department of Justice delineates the CLOUD Act as a "new paradigm" and "an efficient, privacy, and civil-liberties-protective approach" to ensure data access previously unavailable in light of "the revolution in electronic communications, recent innovations in the

---

[7] White Paper, *supra* note 1 at 9 ("In this technological environment, it can be impossible for investigating governments to submit multiple MLAT requests to multiple foreign governments to obtain electronic data scattered in multiple countries, especially when the governments (and sometimes the CSPs themselves) do not know where the data is stored and when the data may well have been moved to another location by the time the requests are reviewed.").
[8] The most notable example of such challenges is *United States v. Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016). Part III of this Comment will discuss this case in further details. *See also* Johnson, *supra* note 2 (citing Assistant Attorney General Richard Downing's statement that the Microsoft case had a ripple effect on the behavior of U.S. based companies who stopped complying with U.S. warrants for overseas data while the case was being considered).
[8] *See* 18 U.S.C. §101(4).
[9] White Paper, *supra* note 1, at 3.
[10] *Id.* at 1.
[11] 18 U.S.C. §2523(b).
[12] 18 U.S.C. §2713(1) (emphasis added).
[13] *See* White Paper, *supra* note 1, at 5.

way global technology companies configure their systems, and the legacy of the 20th century legal frameworks."[14] Despite its laudable attempt to balance privacy protection and the government's need to ensure public safety, the CLOUD Act raises new concerns for both foreign users and U.S.-based CSPs, some of whom worry that the legislation, though detailed, lacks meaningful safeguards for privacy.

This Comment will argue that the CLOUD Act, despite being a functional update from the current mechanism in cross-border data access, should be supplemented with procedural and substantive safeguards to further ensure efficient access without compromising user privacy. The discussion will center upon stored data and not electronic communications.[15]

Part II will lay out the relevant legal framework with regard to cross-border data access prior to enactment of the CLOUD Act. It will examine the Fourth Amendment line of cases, the relevant provisions in the Stored Communications Act, and the data request process under the Mutual Legal Assistance Treaties ("MLATs"). Part III will examine the CLOUD Act more closely. It will briefly introduce the history of the legislation. It will discuss the case that propelled the CLOUD Act's enactment, *United States v. Microsoft Corp.*[16] It will analyze the major provisions of the CLOUD Act and explore their advantages.

Part IV will introduce the shortcomings of the CLOUD Act. It will first note the concerns arising from the language of the Act. It will then address any potential protection gaps of this legislation. Part V will discuss the impact of the CLOUD Act on U.S.-based CSPs from both foreign users' perspective and data providers' perspective. Part VI will analyze some of the alternatives and possible improvements to the CLOUD Act envisioned by scholars. It will try to present a general idea as to what the future holds for the CLOUD Act. Part VII will conclude that the CLOUD Act presents practical difficulties and privacy concerns that Congress should address by supplementing a more protective measure.

---

[14] *Id.* at 2.

[15] The CLOUD Act has a wiretap provision and its implications will not be addressed in this Comment. *See* 18 U.S.C. §2523(b)(4)(D)(6). For a discussion on issues related to the interception provision in the U.S.-U.K. CLOUD Act agreement, see Albert Gidari, The Big Interception Flaw in the U.S.-UK CLOUD Act Agreement, THE CENTER FOR INTERNET AND SOCIETY (Oct. 18, 2019, 9:00 AM), http://cyberlaw.stanford.edu/blog/2019/10/big-interception-flaw-us-uk-cloud-act-agreement.

[16] 829 F.3d 197 (2d Cir. 2016).

II. The Legal Framework of Cross-Border Data Access

Cross-border data access is subject to both constitutional and statutory protection. As cloud computing becomes an increasingly popular platform of electronic surveillance, the law in this area remains multifaceted and is constantly evolving. Prior to the enactment of the CLOUD Act, at the federal level, law enforcement access to data through cloud computing mainly implicates the Fourth Amendment, the Stored Communications Act, and the Mutual Legal Assistance Treaties.

A. The Fourth Amendment

The Fourth Amendment safeguards the right of individuals against "unreasonable searches and seizures."[17] The test applied is a reasonable expectation of privacy which guarantees protection when one has "exhibited an actual or subjective expectation of privacy" and "society is prepared to recognize [such expectation] as 'reasonable'."[18] The judicially created third party doctrine under the Fourth Amendment jurisprudence is particularly relevant here. This controversial doctrine provides that an individual lacks a reasonable expectation of privacy for information voluntarily disclosed to third parties.[19]

In *United States v. Miller*, the Supreme Court concluded that one lacked a reasonable expectation of privacy in the financial records maintained by his or her bank.[20] Similarly, in *Smith v. Maryland*, the Court held that by voluntarily entering phone numbers and exposing such information to the telephone company during its regular course of business, the petitioner "assumed the risk that the company would reveal to police the numbers he dialed."[21]

The Supreme Court's most recent ruling on the third party doctrine does not provide much clarity on its application to digital technology in general. In *Carpenter v. United States*, the Court declined to

---

[17] U.S. CONST. amend. IV.
[18] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
[19] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").
[20] *Id.* at 442.
[21] Smith v. Maryland, 442 U.S. 735, 744 (1979).

extend the third party doctrine to cell-site location information.[22] In other words, absent a Warrant, a cell phone user's location history is not subject to a Fourth Amendment search simply because the user consented to the service of the telephone company.

While *Carpenter* limited the scope of the third party doctrine and extended further protection to individual privacy, the Court emphasized that the decision was "a narrow one" limited to cell-site location information (CSLI) and does not address business records that do or do not reveal location information.[23] The reasoning of *Carpenter*, however, opens the door for privacy protection beyond this category.[24] The Court distinguished CSLI from bank records at issue in *United States v. Miller* and call records at issue in *Smith v. Maryland* because CSLI is not voluntarily shared in the same way in light of its "deeply revealing nature . . . its depth, breadth, and comprehensive reach, and inescapable and automatic nature of its collection."[25] Given the wide use of cloud computing by both individuals and corporations, one could potentially analogize sensitive information stored in a cloud with CSLI. Afterall, taking advantage of a multi-device friendly, network sharing platform does not necessarily signal that the user voluntarily consented to a warrantless search. On the other hand, one could also argue that cloud computing is subject to less privacy protection given the availability of encryption and that the nature of the data is not as universally private or deeply revealing as one's location information.

Because electronic communications are often not territorially based and the nature of such technology is more complex than traditional storage methods, the third party doctrine is less if at all workable in this area.[26] Without further guidance from the Supreme Court, it is unclear whether the Fourth

---

[22] 138 S. Ct. 2206 (2018).
[23] *Id.* at 2220 ("We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools . . . nor do we address other business records that might incidentally reveal location information . . . [or] other collection techniques involving foreign affairs or national security.").
[24] Evan Caminker, *Article: Location Tracking and Digital Data: Can Carpenter Build A Stable Privacy Doctrine,* 2018 Sup. Ct. Rev. 411, 415 (2019).
[25] Carpenter, 138 S. Ct. at 2219, 2223.
[26] *See* Christopher J. Borchert, Fernando M. Pinguelo, and David Thaw, *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 38 (2015).

Amendment has teeth as far as cloud computing is concerned.[27] In terms of statutory guidance, the Stored Communications Act lays out the framework of privacy protection for electronic communications.

B. The Stored Communications Act

Title II of the Electronic Communications Privacy Act (ECPA), also known as the Stored Communications Act ("the SCA") extended privacy protections to electronic communications before the enactment of the CLOUD Act.[28]

In 1986, Congress enacted the SCA in an effort to keep up with the seismic development in technology.[29] Because the Fourth Amendment's application in the area of remotely stored files presented many uncertainties for litigants, the SCA sought to clarify how privacy protection extends to network account holders.[30] Particularly, it regulates the relationship between governmental investigatory power and service providers in possession of private user information by establishing a set of Fourth Amendment-like provisions."[31]

The SCA protects providers of electronic communications services ("ECS") and remote computing services ("RCS").[32] ECS includes "any service which provides to users . . . the ability to send or receive wire or electronic communications."[33] RCS is defined as "the provision to the public of computer storage

---

[27] Secil Bilgic, *Something Old, Something New, and Something Moot: the Privacy Crisis under the CLOUD Act*, 32 HARV. J. LAW & TEC 321, 325 (Fall 2018). The author notes the argument that Chief Justice Roberts, writing for the majority in *Carpenter*, seems to be saying that there is an "equilibrium adjustment limit on the third-party doctrine" and that it may no longer apply if it gives the government massive new powers. *Id.* at n.30 (citing Orin Kerr, *Understanding the Supreme Court's Carpenter Decisinon*, LAWFARE (June 22, 2018, 1:18 P.M.), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision).

[28] 18 U.S.C. §§2701-2712 (2012).

[29] S. REP. NO. 99-541, at 1 (1986) ("This bill amends the 1968 law to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.").

[30] 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 (2004), 1210–11. Professor Kerr suggests three reasons why the Fourth Amendment protections may not reach electronic communications remotely stored. Notably, because all internet communications are shared with a third party network service provider, the third party doctrine applies, and users may not be entitled to a reasonable expectation of privacy.

[31] *Id.* at 1212.

[32] 18 U.S.C. §2702(a)(1)-(2) (2012).

[33] 18 U.S.C. §2510(15). For example, Google acts as an ECS when it provides a user the ability to send an email from his or her Gmail account.

or processing services by means of an electronic communications system."[34]

A Warrant is required if the government seeks to obtain electronic communications from an ECS that is in storage for 180 days or less.[35] To obtain disclosure from a RCS, the government has the option to issue a Warrant, a subpoena with prior notice, or a qualified court order under §2703(d) of the SCA plus prior notice.[36]

In applying the SCA, courts have "embraced varying and often contradictory interpretations of [its] language," especially when the subject technologies did not exist at the time of its enactment.[37] It has been argued that the SCA, enacted more than thirty years ago, is outdated and does not apply seamlessly to the recent advancement in technology.[38]

C. Mutual Legal Assistance Treaties

Prior to the CLOUD Act's enactment, foreign governments relied heavily on a treaty-based procedural system, the MLATs, to access data stored by U.S.-based CSPs. To utilize this system, a country has to have formed a mutual legal assistance treaty with the U.S. government. Countries without such treaties typically use Letters Rogatory as a slower and less reliable alternative.[39]

The MLAT system involves a series of steps. To take advantage of a MLAT treaty with the U.S. and execute a Warrant for information held by a U.S.-based provider, a foreign investigative body has to first file a request with the central processing agency within its own government.[40] Once approved, the

---

[34] 18 U.S.C. §2711(2). For example, Google acts as an RCS when it allows users to store data online in a Google Drive for safekeeping.
[35] 18 U.S.C. §2703(a).
[36] 18 U.S.C. §2703(b).
[37] Borchert, *supra* note 26, at 48. For example, in the context of social media, the SCA's application is not completely straightforward. *Id.* at 53 (explaining that while the scope of the SCA is limited to electronic communications unavailable to public access, "recent court decisions suggest that some communications made via social media networking platforms may receive SCA protections, even if they were disclosed to hundreds or even thousands of third parties").
[38] *See, e.g.*, Mitchol Dunham, *Arbitrary and Outdated: Reforming the Stored Communications Act* (August 14, 2018), https://ssrn.com/abstract=3258774 (arguing that the SCA is ill-equipped with arbitrary and antiquated rules that do not account for the recent development in technology).
[39] Tiffany Lin & Marylyn Fidler, Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement, Berklett Cybersecurity, 9 at n.3 (Sept. 7, 2017), https://dash.harvard.edu/bitstream/handle/1/33867385/2017-09_berklett.pdf?sequence=1&isAllowed=y.
[40] *Id.* at 2.

central processing agency will send the request to the Office of Internal Affairs (OIA) at the U.S. Department of Justice for clearance.[41] After confirming that the request meets applicable U.S. standards, the OIA then works with a U.S. Attorney's Office to have the "qualified request" reviewed by a U.S. magistrate judge, who will determine whether the request aligns with relevant U.S. law, "notably including the Fourth Amendment's probable cause standard, rules of privilege, and the Fifth Amendment."[42]

A qualified request is then served on the U.S. company.[43] The OIA will review the submitted evidence "to ensure it meets data minimization and human rights standards" and once satisfied, it will finally send it back to the foreign government's central processing agency.[44] Depending on the quality of the request and the requesting country, this multi-step process can take months to complete.[45]

In addition to being lengthy and onerous, the MLAT system is arguably irreconcilable with cloud computing.[46] The MLAT formulation originally assumed all evidence "consisted of tangible, physical objects located somewhere specific on a given country's territory."[47] Cloud computing, however, involves data storage that exceeds or dissolves territorial boundaries. The territorial assumptions of the MLAT system are thus troublesome when applied to the free-flowing or multi-territorial electronic communications.[48]

---

[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.* at 3.
[45] Lin *supra* note 39, at 3. *See also* Jennifer Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9, 13 (May 2018) ("[A]ccording to the 2013 Report and Recommendations of the President's Review Group on Intelligence and Communications Technology, delays have averaged almost a year for such requests.").
[46] Vivek Krishnamurthy, *Cloudy with a Conflict of Laws* 1 (Berkman Klein Ctr., Paper No. 2016-3, Feb. 16, 2016) ("[T]he territorially-based MLAT system fundamentally does not work with the physical, technological, and corporate structures that are used to deliver cloud-based services.").
[47] *Id.* at 4.
[48] *Id*. Krishnamurthy argues that for at least three reasons, the MLAT system no longer holds in the digital age. First, data is being increasingly stored with multinational cloud service providers (MCPs) that operate in different countries rather than within one country's borders. *Id.* Second, for performance and reliability reasons, MCPs "shard" their data into many small pieces that are stored and backed up in many different places. *Id.* Neither party can tell where the data is physically stored until it is retrieved. *Id.* at 5. Third, the ownership of an electronic account often cannot be identified until the content is revealed. *Id.*

Furthermore, the MLAT system does not properly resolve conflicting legal obligations and unilaterally subject foreign governments to U.S. legal standards. In fact, certain governments have begun to circumvent this problem by requiring companies operating within their borders, including those that are headquartered in the U.S., to store certain data domestically.[49] Such data localization policies are notably problematic for undermining web openness and restricting a company's ability to "manage data traffic in ways that enhance efficiency, security, and interoperability."[50] In light of such challenges, many argued that as an alternative to the MLATs, the CLOUD Act achieves efficiency without sacrificing privacy guarantees and human rights protections.[51]

III. The CLOUD Act

As the number of MLAT requests multiplied,[52] so did the demand for new legislation that responds directly to the frustrations of foreign law enforcement without compromising privacy protection for individual users. For years, Congress and private groups debated about a new program to better address cross-border data requests. What prompted Congress to turn such debates into action was the case *Microsoft Corp. v. United States.*[53]

The central dispute in *Microsoft* was whether the SCA reached electronic communications controlled by a U.S.-based company but stored in a foreign country.[54] This question presents difficulties because it required courts "to divine the intent of an act written well before there was a globally interconnected internet."[55]

In *Microsoft*, after a magistrate judge found probable cause that an account was used in furtherance

---

[49] Christine Galvagna, *The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform*, 9 NOTRE DAME J. INT'L & COMP. L. 57, 61 (2019).
[50] *Id*.
[51] *See, e.g.*, Jennifer Daska & Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, LAW FARE (Mar. 14, 2018, 12:00 PM), https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.
[52] U.S. DEPARTMENT OF JUSTICE, FY 2015 BUDGET FACT SHEET 1 (2015), https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf ("Over the past decade the number of requests for assistance from foreign authorities handled by the Criminal Division's Office of International Affairs (OIA) has increased nearly 60 percent, and the number of requests for computer records has increased ten-fold.").
[53] *See* 829 F.3d 197 (2d Cir. 2016).
[54] *See Id.*
[55] Daskal, *supra* note 45, at 9.

of narcotics tracking, the U.S. government served a Warrant on Microsoft at its Washington headquarters.[56] Microsoft produced non-content information[57] stored in the U.S. but declined to provide access to customer content that required importation from a server in Ireland.[58] The District Court denied Microsoft's request to quash the Warrant and held the company in contempt.[59] On appeal, the Second Circuit sided with Microsoft that the SCA sought to afford "heightened privacy protection" for domestic users and its presumption against extraterritoriality cannot be easily abandoned by a Warrant requesting a service provider to retrieve cross-border material.[60]

On July 15, 2016, the day after the Second Circuit handed down its decision in *Microsoft*, the Department of Justice submitted a draft legislation to the Senate that would "help resolve potential conflicting legal obligations that U.S. electronic communications service providers may face when required to disclose electronic data by foreign governments investigating serious crime, including terrorism."[61] This predecessor of the CLOUD Act proposed "streamlined solutions" by reaching a bilateral agreement with the U.K. and subsequently establishing a framework that would set in motion more similar agreements with countries that have strong laws protecting privacy and human rights.[62]

On October 16, 2017, the Supreme Court granted the government's petition for certiorari in *Microsoft*.[63] But there was no need for the Court to decide the merits of the case. Less than a month after the parties argued the case in front of the Court, which indicated that Congress should step in to resolve the

---

[56] *See* 829 F.3d 197.
[57] Non-content information, as opposed to content information, which includes the actual content of the files stored in a customer's account, refers to "subscriber information such as name, address, email address, billing information, data of account creation, and certain purchase history and service usage information." Liz Woolery, Ryan Budish, and Kevin Bankston, *The Transparency Reporting Toolkit*, THE BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY 61 (Mar. 2016), https://cyber.harvard.edu/sites/cyber.harvard.edu/files/Final_Transparency.pdf.
[58] 928 F.3d at 200.
[59] *Id.*
[60] 928 F.3d at 201. RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090 (2016) (reiterating the principal that United States law governs domestically and absent express Congressional intent to the contrary, federal laws will be construed to apply only domestically).
[61] Letter from Peter J. Kadzik to Joseph R. Biden (July 15, 2016) at 1.
[62] *Id.* at 2.
[63] United States v. Microsoft, 138 S. Ct. 356 (2017), *cert. granted*, 138 S. Ct. 1186 (2018) (No. 17-2).

extraterritorial application of the SCA,[64] on March 23, 2018, the CLOUD Act was signed into law as an attachment to a $1.3 trillion, 2,232-page spending bill.[65] The Government obtained a Warrant pursuant to the new law and the parties no longer contested the jurisdictional validity of the alleged cross-border data request.[66]

A. Main Components of the CLOUD Act

The CLOUD Act authorizes the United States government to enter into executive agreements with qualifying foreign counties and prescribes the criteria they must meet.[67] In general, the domestic laws of the country subject to this agreement must afford "robust substantive and procedural protections for privacy and civil liberties."[68]

With the concurrence of the Secretary of State, the Attorney General is to make such determinations and submit a written certification after evaluating a list of factors that are consistent with requirements set forth in the Budapest Convention on Cybercrime.[69] In addition, the qualifying foreign government has to have "adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning U.S. persons subject to the agreement."[70]

Once an agreement is formed, if both countries find the circumstances appropriate, the U.S. government and its foreign counterpart will agree to remove any legal restriction to a provider's ability to

---

[64] Transcript of Oral Argument at 6, 11–12, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2) ("Justice Ginsberg: so wouldn't it be wiser just to say let's leave things as they are; if - - if Congress wants to regulate in this brave new world, it should do it?"; "Justice Sotomayor: Why shouldn't we leave the status quo as it is and let Congress pass a bill in this new age.").

[65] Johnson, *supra* note 2. *See also Responsibility Deflected, the CLOUD Act Passes*, ELECTRONIC FRONTIER FOUNDATION (Mar. 23, 2018), https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes (noting how the CLOUD Act was unrelated to the omnibus spending bill which must be passed to avoid another government shut-down).

[66] Microsoft, 138 S. Ct. 1186.

[67] 18 U.S.C. § 2523.

[68] 18 U.S.C. § 2523(b)(1).

[69] *Id.* The Budapest Convention on Cybercrime is a multi-national agreement on cybercrime and electronic evidence and it "provides States with (i) the criminalisation of a list of attacks against and by means of computers; (ii) procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and (iii) international police and judicial cooperation on cybercrime and e-evidence." *The Budapest Convention on Cybercrime: a Framework for Capacity Building*, GLOBAL FORUM ON CYBER EXPERTISE (July 12, 2006), https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime.

[70] 18 U.S.C. § 2523(b)(2).

comply with orders issued under the agreement.[71] Then, both parties will be able to utilize their domestic legal process to acquire the requested data. In other words, the CLOUD Act allows the foreign government to bypass the several steps of intermediary review mandated by the MLATs and directly seek data from U.S.-based CSPs, and vice versa.

The second major component of the CLOUD Act resolves the *Microsoft* line of conflicts by amending the Stored Communications Act of 1986 with § 2713. § 2713 prescribes that once a user data request is properly made, the provider must preserve, backup, or disclose the requested content "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."[72] In short, the CLOUD Act makes clear that SCA Warrants cover not only data stored domestically but have an international reach regardless of its physical location. Under this framework, a U.S.-based CSP can no longer challenge a Warrant issued on information stored in one of its foreign data centers.

B. Advantages of the CLOUD Act

The CLOUD Act's passage received support from Microsoft and other tech giants in the U.S.[73] This phenomenon is unsurprising. After all, the CLOUD Act is a rational response to new demands in the age of the internet and embodies many advantages envisioned by both law enforcement and private parties.

Efficiency is one of the most notable advantages of the CLOUD Act. First, it simplifies the process of cross-border data requests for large tech companies like Microsoft, Apple, Facebook, Google, and Oath, who, in the wake of *Microsoft*, stressed that "dialogue and legislation—not litigation—is the best approach."[74] As the *Microsoft* case demonstrated, before the CLOUD Act's passage, companies were

[71] White Paper, *supra* note 1, at 11.
[72] 18 U.S.C. § 2713.
[73] Johnson, *supra* note 2. *See also* Brad Smith, *A Problem Congress Should Solve,* MICROSOFT ON THE ISSUES, (Feb. 27, 2018), https://blogs.microsoft.com/on-the-issues/2018/02/27/a-problem-congress-should-solve/ ("The CLOUD Act creates both the incentive and the framework for governments to sit down and negotiate modern bi-lateral agreements . . . [and] it ensures these agreements have appropriate protections for privacy and human rights and gives the technology companies that host customer data new statutory rights to stand up for the privacy rights of their customers around the world.").
[74] Letter from Apple, Facebook, Google, Microsoft, Oath to Senators Hatch, Coons, Graham, and Whitehouse (Feb. 5, 2018).

hesitant to release user information stored in a foreign country based on the complex jurisdictional issues presented. While Microsoft commendably sought to safeguard user privacy by investing significant time and resources to contest an executed U.S. Warrant all the way up to the Supreme Court, many companies understandably gave in. The CLOUD Act clarified the process for these companies, who no longer had to balance the need to comply with the government against privacy concerns of their valued customers.

On a broader note, the CLOUD Act aids international criminal investigations and furthers public safety by serving as a useful alternative to the dreaded MLAT process. By removing the intermediary vetting process and replacing it with a direct but qualified request under an international agreement, the CLOUD Act helps prevent administrative delays, especially when conflicts of law arise.[75] Under the MLAT system, there is a lack of focus on how disclosed evidence is ultimately used.[76] The CLOUD Act addresses this issue by requiring secure data storage, mandating destruction of nonrelevant data, and limiting the dissemination of acquired data.[77]

Importantly, the CLOUD Act supplements but does not displace the MLAT system or other available mechanisms.[78] This allows foreign countries that are not entitled to executive agreement privileges to nevertheless obtain information that meets the relevant U.S. legal standards. To ensure an executive agreement carries out its full force without loopholes, the CLOUD Act expressly provides that a foreign government cannot issue an order at the request of the U.S. government or a third party country, nor can it share any information obtained under an executive agreement with a non-party.[79] Thus, neither the U.S. government nor any foreign government can seek to get around the pre-condition of forming an executive agreement or exceed the boundary of a valid disclosure request.

In order not to deviate too far from a detailed, case-by-case mechanism, the CLOUD Act sets forth specific requirements for any data-request order issued by a qualified foreign partner.[80] Among other

[75] *See* White Paper, *supra* note 1, at 4.
[76] *See* Jennifer Daskal, Privacy and Security Across Borders, 128 YALE L. J. F. 1029, 1049 (Apr. 1, 2019).
[77] *Id.*
[78] White Paper, *supra* note 1 at 5.
[79] 18 U.S.C. §2523(b)(4)(C).
[80] 18 U.S.C. §2523(b)(4)(D).

applicable criteria, the order must "identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order."[81]

The CLOUD Act, by making clear that data stored by a U.S.-based CSP is discoverable regardless of its location, diminishes data evasion concerns, namely, the risk that a company might assist criminals by moving data outside the United States to avoid detection.[82]

The Department of Justice also noted that the CLOUD Act reduces the resources needed to process MLAT requests from qualifying countries, and it "should allow the United States to respond to other MLAT requests more expeditiously."[83] As a result, the CLOUD Act also gives both the U.S. government and foreign sovereigns a timely opportunity to invest those resources elsewhere, such as toimprove the MLAT system itself.[84]

Furthermore, while the CLOUD Act is largely consistent with the government's position in *Microsoft*, it provides a new statutory safeguard that involves a comity analysis.[85] When the recipient of a data request reasonably believes that the sought information belongs to a non-U.S. person residing outside the U.S. and disclosure would create a "material risk" of violating a foreign law, it may seek judicial redress by filing a motion to quash or modify.[86] To many, the availability of a judicial remedy reenforces the idea that the CLOUD Act is a "privacy win."[87]

The CLOUD Act is an effort by the U.S. government to influence international lawmaking by domestic regulations.[88] It has been suggested that by preconditioning bilateral agreements upon substantive and procedural privacy guidelines, the CLOUD Act incentivizes a growing list of foreign countries to adopt

---

[81] 18 U.S.C. §2523(b)(4)(D)(ii).
[82] Dunham, *supra* note 38, at 19 ("This provision [§2713] draws to an end the common concern that some nefarious but enterprising companies might help criminals cover their tracks by moving data around outside of the United States and then delete it when notified that the United States government is looking for the information.").
[83] White Paper, *supra* note 1 at 5.
[84] *Experts Share International Perspectives on the CLOUD Act at Capitol Hill Event*, GLOBAL NETWORK INITIATIVE (Oct. 2018), https://globalnetworkinitiative.org/international-perspectives-cloud-act/.
[85] 18 U.S.C. §2713 (h).
[86] 18 U.S.C. §2713 (h)(2). *See* Letter from Apple, Facebook, Google, Microsoft, and Oath to CLOUD Act Bill Sponsors, *supra* note 74 ("The legislation provides mechanisms to notify foreign governments when a legal request implicates their residents, and to initiate a direct legal challenge when necessary.").
[87] Daskal & Swire, *supra* note 51.
[88] *See* Daskal, *supra* note 45, at 15.

more rigorous privacy safeguards, thereby raising privacy standards on an international scale.[89] It has also been said that the CLOUD Act disincentivizes foreign governments from further localizing data to prevent outside access.[90]. Moreover, from a technological standpoint, the CLOUD Act largely renders obselete the concern that different types of cloud computing should be subject to different standards.[91]

IV. Privacy Shortcomings of the CLOUD Act

Along with its avid supporters, the CLOUD Act invited strong opposition from privacy, civil liberties, and human rights groups.[92] Some foreign companies went as far as accusing the U.S. government of wanting to conduct economic espionage in furtherance of U.S. economic interests.[93] The CLOUD Act, while a functional improvement from the MLATs, is not a be-all and end-all solution. In fact, it poses privacy shortcomings and does not immunize communication service providers from practical uncertainties

---

[89] *Id.*

[90] Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUMB. L. REV. 1681, 1688 (Oct. 2018) ("In doing so, [the CLOUD Act] reduces the significance of data localization for data access requests and thereby promotes the maintenance of a globally inoperative internet"). *But see id.* ("But in encouraging this documentation and location of cloud customers, the CLOUD Act moves providers closer to the paradigm in place for U.S. banks and financial service entities, which collect detailed identification information about customers and are even legally required to file reports proactively when their customers engage in suspicious activities").

[91] Three existing models are Data Shard, Data Localization, and Data Trust clouds and they differ from each other in terms of how information can be accessed. In the Data Shard cloud, information is stored in multiple international locations. *Id.* at 1695 ("[T]he network itself distributes data to domestic and international servers. A single file can be broken into components and stored in different countries, and intelligence embedded in the network decides where to send and store the data."). An example of this model is the Google cloud, which "automatically moves data from one location on Google's network to another . . . to optimize for performance, reliability, and other efficiencies." *Google Pennsylvania*, 232 F. Supp. 3d 708, 723 (E.D. Pa. 2017). In the Data Localization cloud, information is stored in a single country or region. Schwartz, *supra* note 90, at 1696. This model was the one used by Microsoft and as at the center of the *Microsoft Ireland* litigation. *Id.* As for the Data Trust model, information can be located within one country or a single region, but a further step is taken "to separate network management from the ability to access data." *Id.* at 1697. Here, only the Data Manager oversees the network hardware and software while a separate party, the Data Trustee, is the exclusive party who can access the data. *Id.* The only company that currently employs the Data Trust model is Microsoft. *Id.* at 1698.

[92] *See, e.g.*, Coalition Letter on CLOUD Act (Mar. 12, 2018), https://www.aclu.org/letter/coalition-letter-cloud-act (arguing the CLOUD Act undermines privacy and democratic safeguards). Opponents of the CLOUD Act often emphasize their concern that it was an unrelated data bill attached to a lengthy $1.3 trillion government spending bill. *See* David Ruiz, *Responsibility Deflected, the CLOUD Act Passes*, ELECTRONIC FRONTIER FOUNDATION (Mar. 23, 2018), https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes ("[The CLOUD Act] was robbed of a stand-alone floor vote because Congressional leadership decided, behind closed doors, to attach this un-vetted, unrelated data bill to the $1.3 trillion government spending bill.").

[93] Justin Hemmings & Nathan Sire, *The CLOUD Act is Not a Tool for Theft of Trade Secrets*, LAWFARE (Apr. 23, 2019, 8:00 AM), https://www.lawfareblog.com/cloud-act-not-tool-theft-trade-secrets. The CEO of a French service provider said that "some of his French clients come to his company specifically to avoid handling payroll information to the U.S. government or other services under U.S. control." *Id.* This sentiment was shared by many actors in the French private sector as well as the French government. *Id* (noting that the French government has asked industries to use "Cloud-Act-safe" data providers).

or user privacy violations.

A. Broad Discretion to the Executive Branch and Weak Congressional Control

Most notably, despite its detailed provisions, the CLOUD Act grants broad discretion to the Executive Branch.[94] To support a written certification to Congress that the prospective foreign ally is qualified to enter into an executive agreement with the U.S., the Attorney General will rely upon a multitude of broadly defined factors.[95] For instance, it requires that the foreign government "demonstrates respect for the rule of law and principles of nondiscrimination" and "adheres to applicable international human rights obligations" including "protection from arbitrary and unlawful interference with privacy," "fair trial rights," and "prohibitions and arbitrary arrest and detention."[96] Such abstract language lacks the specificity and detailedness needed as helpful guidance on whether a country truly qualifies as one that guarantees robust privacy protections.[97] It also does not define or limit the scope of the Attorney General's discretion and leaves much to one's broad interpretation. Furthermore, the CLOUD Act instructs that the Attorney General's determination is *not* subject to judicial review.[98] This is especially problematic and a significant drawback considering the MLAT system's mandatory judicial review process on a case-by-case basis.

As for congressional review, the CLOUD Act also lacks a genuinely helpful mechanism. The CLOUD Act serves as an "ex ante" staturory authorization. No after-the-fact congressional ratification is required for the negotiation or establishment of bilateral agreements.[99] Such a bilateral agreement is unlike an Article II treaty that requires two-thirds consent of the Senate.[100] The CLOUD Act provides that the

---

[94] *See* Neema Singh Guliani, *New CLOUD Act, Supported by Major Tech, Trusts Sessions and Pompeo to Defend Our Human Rights*, THE HILL (Mar. 20, 2018), https://thehill.com/blogs/congress-blog/civil-rights/379367-new-cloud-act-supported-by-major-tech-trusts-sessions-and (arguing the CLOUD Act "strips power away from Congress and the judicial branch" while giving Executive Branch officials "unchecked authority to negotiate data exchange agreements with foreign nations, regardless of whether they respect human rights of not").
[95] §2523(b)(1)(B).
[96] *Id*.
[97] *See* Guliani, *supra* note 94 ("[T]he bill only stipulates that the Executive Branch consider as a factor whether a government 'demonstrates respect' for human rights and is similarly vague as to what practices would exclude a particular country from consideration."); Galvagna, *supra* note 49, at 68 ("Though the legislation's long list of conditions and requirements may at first glance seem impressive, upon greater scrutiny, most are meaningless.").
[98] §2523(c).
[99] *See* Robyn Green, Somewhat Improved, the CLOUD Act Still Poses a Threat to Privacy and Human Rights, JUST SECURITY (Mar. 23, 2018), https://justsecurity.org/54242/improved-cloud-act-poses-threat-prviacy-human-rights/.
[100] U.S. CONST. ART. II. §2.

Senate and the House of Representatives enter into a joint resolution of disapproval within 180 days after receiving notice of the executive agreement.[101] Deprived of the power of prior approval, in a case of disagreement, they will face the difficult task to convince the President not to exercise his veto power or overcome the veto themselves.[102] The CLOUD Act exemplifies the increased use of "congressional-executive agreements" authorized by statute. Ex-post congressional executive agreements are rare and are mainly used in trade agreements.[103] Despite the benefit of efficiency and preservation of foreign relations, such agreements are problematic due to the lack of administrative rigor in the agreement-making process.[104]

B. Lowering Evidentiary Threshold and Under-specificity Issues

The CLOUD Act also lowers the evidentiary threshold required for foreign countries to obtain data stored by U.S.-based CSPs. Unlike the MLATs, the CLOUD Act exempts foreign data requests from review by the Department of Justice or a magistrate judge. In general, its privacy safeguard falls short of that offered by the MLATs.[105]

The CLOUD Act forbids a foreign government from intentionally targeting a United States person or a person located in the United States; the same restriction applies if the request targets "a non-United States person located outside the United states if the purpose is to obtain information concerning a United States person or a person located in the United States."[106] The relevant subsection also requires the foreign

---

[101] §2523(d)(4)(C).

[102] *See* Guliani, *supra* note 94. *See also* Green, *supra* note 99 ("This leaves Congress in the impossible position of stopping the certification of a foreign government only if it has a veto proof majority, or if somehow, the President decides to reject the determination of the AG and the secretary of State."). *But see* Paul M. Schwartz, *supra* note 90, at 1750 (Oct. 2018) ("On the other hand, giving greater power to Congress may slow the process of reaching executive agreements and even hinder the President's ability to effectively negotiate with foreign governments.").

[103] Curtis Bradley, Jack Goldsmith & Oona Hathaway, *Executive Agreements: International Lawmaking Without Accountability?*, LAWFARE (Jan. 9, 2019, 10:30 AM), https://www.lawfareblog.com/executive-agreements-international-lawmaking-without-accountability (noting that ex-post congressional-executive agreements are even rarer than Article II treaties and as an example, the Trump administration's proposed United States-Mexico-Canada Agreement designed to replace the North American Free Trade Agreement will go through such a process).

[104] With a sharp decline in the presidential use of Article II treaties, the U.S. government "makes dozens of binding international agreements each year—often more than 100—but it usually does so as 'congressional-executive agreements.'" *Id.* Thus, the United States has "effectively shifted to an administrative regime for making international agreements, but it has yet to craft an adequate system of oversight and accountability to go along with that regime." *Id.*

[105] Bilgic, *supra* note 27, at 337.

[106] § 2523(b)(4)(A)–(B).

government adopt targeting procedures to satisfy this condition without specifying what standards should be met or what the potential remedies may be.[107]

Notwithstanding its lack of specificity, this attempt to safeguard the privacy of domestic residents presents practical uncertainties. Unless the user details his or her personal information publicly, it is difficult, if not impossible, to identify the residency or citizenship of a user without looking into the content of the requested communications.[108] As a result, the protected information of a U.S. person or resident could be disclosed before privacy precautions may be taken.[109] Thus, while this promise not to target U.S. persons appears reassuring, its execution will be met with uncertainties.

Moreover, this protective measure does not specify any remedial action when an executed request *incidentally* intrudes upon the privacy rights of covered individuals.[110] If a U.S. company, in response to a valid request under an executive agreement, sends a document addressed to a third party whom it later found out to be a U.S. person, the CLOUD Act does not indicate whether the unintentionally targeted person should be implicated.

To illustrate, under a valid U.K.-U.S. executive agreement, a London detective who wants access to a Londoner's private files stored in his OneDrive account could go directly to Microsoft, a U.S.-based CSP, to collect such information. The detective is not required to notify U.S. law enforcement about this, nor is a Warrant required. Because the CLOUD Act does not clarify whether a user, rather than a company, has standing to challenge the request, the Londoner would not be able to do anything if abuses occurred. Also, if the Londoner's account just happened to belong to a U.S. citizen, it is unclear what his or her remedy might be either.

Although the CLOUD Act sets forth detailed limitations on the foreign order, some criteria designed to narrow its application fall short as a substantive privacy guarantee. For example, the CLOUD

---

[107] § 2523(b)(4)(A).
[108] *See* Bilgic, *supra* note 27, at 338.
[109] *See Id.* ("[W]ithout accurate citizenship information prior to data collection, electronic communications of U.S. citizens could be collected not under U.S. standards, but by standards used by the qualifying foreign government").
[110] *See* Coalition Letter on CLOUD Act (Mar. 12, 2018), https://www.aclu.org/letter/coalition-letter-cloud-act.

Act only applies when a foreign government has initiated the prosecution of a "serious crime."[111] Other than noting the inclusion of "terrorism,"[112] the CLOUD Act does not define or explain what constitutes a "serious crime" for the purposes of cross-border data access that would trigger its application. This gap "leaves interpretation of that inherently vague concept to the discretion of the foreign government."[113] It is worth noting that the U.S. Supreme Court has held that a crime punishable by a two-year prison term is a serious crime,[114] and noted that for purposes of the Sixth Amendment, a serious crime includes any offense that carries a maximum penalty of more than a six-month prison term."[115] Assuming this standard serves as a guideline, the CLOUD Act reaches a wide range of offenses that do not remotely implicate national security and subject private information to how a foreign government prescribes sentencing for a crime.

The CLOUD Act also provides that the order issued by the foreign government is "subject to review or oversight by a court, magistrate, or other independent authority before *or* in proceedings" regarding its enforcement.[116] The language of this provision makes clear that independent review, notably court review, is *not* required prior to an enforcement proceeding. It is only a viable option, which does not create much incentive for requesters to take actively steps in ensuring that privacy risks are minimized. Moreover, this provision does not specify the procedures for such review should it become necessary prior to the enforcement of the order.

Additionally, the order issued by the foreign government "may not be used to infringe freedom of speech."[117] This provision again utilizes broad language and fails to mention any particular applicable legal standard, especially concerning the CLOUD Act's international application. A qualifying foreign nation could potentially infringe one's freedom of speech in the First Amendment sense without violating this provision if its domestic laws are less strict. Reciprocally, the same applies to the U.S. government.

---

[111] §2523(b)(1)(4)(D)(i).
[112] *Id*.
[113] Green, *supra* note 99.
[114] Duncan v. Louisiana, 391 U.S. 145, 162 (1968).
[115] Lewis v. United States, 518 U.S. 322, 331 (1996) (citing Duncan v. Louisiana, 391 U.S. 145, 159–160).
[116] §2523(b)(1)(4)(D)(v) (emphasis added).
[117] §2523(b)(1)(4)(E).

Because of its bilateral effect, the CLOUD Act does not only allow foreign governments to obtain data stored in the U.S., it also gives U.S. law enforcement access to data located abroad without having to find probable cause or comply with foreign privacy law requirements.[118] This disadvantage is mitigated by the Supreme Court's holding in *United States v. Verdugo-Urquidez* that the search and seizure restrictions of the Fourth Amendment do not apply extraterritorially to people "without voluntary connection[s] to the United States."[119] However, *Verdugo-Urquidez* has also been interpreted to mean that the Fourth Amendment restrictions do apply to extraterritorial searches, but only if the targeted individual has significant contact with the United States.[120] Therefore, the CLOUD Act undermines privacy interests of certain foreign users who would have otherwise been entitled to protections under the Fourth Amendment.

C. Absence of a Notice Requirement and Its Related Impact

Notably, the CLOUD Act does not afford a notice requirement.[121] There is no provision in the statute that requires notice under any circumstances "to the person targeted, to the country where the person resides, and to the country where the data is stored."[122] This is problematic because a targeted foreign person or an incidentally targeted U.S. person would not have the opportunity to seek redress beforehand or afterwards when abuses do occur.[123] Another related concern arises when a country that is not an immediate party to the executive agreement becomes affected by the data request, considering that the same set of data can be simultaneously stored in multiple countries. The CLOUD Act does not provide a remedy for such countries who seek to protect the privacy rights of their citizens incidentally affected by disclosures pursuant to executive agreements.[124]

---

[118] *See* Galvagna, *supra* note 49, at 67 (noting that the CLOUD Act creates "reciprocal access that remove barriers to direct cooperation between law enforcement agencies in one state and service providers in another").
[119] United States v. Verdugo-Urquidez, 494 U.S. 259, 261, 271 (1990).
[120] *See* Schwartz, *supra* note 90, at 1711.
[121] *See* Coalition Letter on CLOUD Act (Mar. 12, 2018), https://www.aclu.org/letter/coalition-letter-cloud-act ("The bill would not ensure that users whose information is demanded are notified, so that they may challenge improper requests.").
[122] Camille Fischer, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data*, ELEC. FRONTIER FOUND. (Feb. 18, 2018), https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data.
[123] *See* Bilgic, *supra* note 27, at 340.
[124] *See* Galvagna *supra* 49, at 67.

D. Persistent Issues of Data Localization

Another blemish of the CLOUD Act is its limited role in remediating data localization issues. In attempts to safeguard against U.S. surveillance, benefit local law enforcement, and boster domestic trade,[125] many countries implemented data localization laws and policies that either force Internet content hosts to store user information domestically on servers located within the jurisdictional reach of their national government or route data packets transmitted between users within their jurisdiction across in-jurisidction networks only.[126] Other than being criticized as a protectionist measure and imposing high costs for corporations,[127] data localization limits the ability of U.S.-based companies to "defend fundamental rights abroad, and monopoliz[es] the competitive market for privacy controls."[128]

The CLOUD Act will not adequately disincentivize data localization unless an executive agreement is formed. So far, only one executive agreement has been entered into with the United Kingdom.[129] In other words, in practice, the CLOUD Act has not made any impact in terms of impeding data localization and will not likely do so in the immediate future. Furthermore, a country that formulated data localization policies to countract U.S. surveillance will be less incentivized to compromise its previous effort and "share" information in accordance with the CLOUD Act. On the other hand, when contemplating an executive agreement with a foreign partner, the U.S. government should bear in mind how its enforcement would affect domestic business entities or isolate them from their foreign clients. It should not, however, ignore the interests of countries with large markets and indirectly incentivize them to localize their data.[130] Such economic considerations arguably bear little relevance in this inquiry, but it is not difficult to see how the

[125] H Jacqueline Brehmer, *Note: Data Localization: the Unintended Consequences of Privacy Litigation*, 67 AM. U.L. REV. 927, 932.
[126] John Selby, *Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?*, 25 INT J LAW INFO TECH, Issue 3, 213 (2017).
[127] Brehmer, *supra* note 125, at 932–33 (noting that in 2013, it was predicted that data localization would cost cloud computing services between $21.5 billion and $35 billion by 2016 and that "the majority of this high cost stems from the development and staffing of necessary technical infrastructure essential for compliance with data localization requirements").
[128] *Id.* at 960.
[129] Gidari, *supra* note 15.
[130] *See* Woods & Swire, *supra* note 1 (noting that if the U.S. government enters into an executive with the U.K. but no one else, some of the world's biggest markets, such as India and Brazil, would be left in the cold and be incentivized to mandate localization).

government could easily prioritize such concerns and push privacy protection considerations to the side.

E. The Long-arm "Control" Requirement

The CLOUD Act resolves the jurisdictional dilemma raised in *Microsoft* by providing that electronic communications are subject to disclosure if it is in the provider's "possession, custody, or control."[131] This is the same language used for subpoenas in the civil discovery context under Federal Rules of Civil Procedure 34 and 45.[132] Considering the abstract and often interconnectedness of cloud computing, the question of "control" is difficult to resolve.

The "control" issue eventually boils down to a factual inquiry about whether a U.S.-based service provider has a legal right or practical ability for the overseas data access.[133] Problems often arise when businesses are unaware of a subleasing agreement or a sister corporate entity in the U.S. that could place their user data under the control of a U.S. CSPs, and thus become accessible to the U.S. government and its partner countries.[134] Another potential feature of cloud computing that could complicate the "control" analysis is encryption. If a U.S. company offered its client the option of "client-side encryption," whether such security protection could shield the client from the reach of the CLOUD Act or how it plays out in the "control" analysis requires further interpretation.[135] Additionally, unlike the traditional method of physical storage, there are different types of cloud storage that could require separate modes of legal analysis under the catch-all "control" requirement.[136]

V. Impact of the CLOUD Act on Communications Service Providers

As aforementioned, the CLOUD Act generated many benefits for companies that are subject to cross-border data requests. U.S.-based CSPs with dominance in large global presence like Microsoft may

---

[131] 18 U.S.C. §2713.
[132] FED. R. CIV. P. 34 and 45.
[133] William Ridgway & Jordan Blain, *How the CLOUD Act Can Reach Stored Data Across Borders*, LAW360 (Jan. 2, 2019).
[134] *Id.* (cautioning that businesses should investigate the proposed arrangement to carefully determine whether a company with a U.S. presence would enable access to its unencrypted overseas data).
[135] *Id.*
[136] Schwartz, *supra* note 90, at 1684–86 (arguing that legal policy in the area of cloud computing and data access should be aware of the underlying management model of a cloud network and "legal decision making about access to global clouds must be grounded in knowledge of how existing clouds differ from one another").

be motivated to support the CLOUD Act because of their distaste for data localization measures foreign nations adopted to bypass the MLATs. The impact of the CLOUD Act on communication service providers generally is not entirely positive, however, and such negative impact could manifest more evidently in the long run as the CLOUD Act becomes more widely adopted.

The CLOUD Act continues to implicate the concern that in response to the U.S. government's heightened authority in cross-border data access, foreign customers will be incentivized to move their business to foreign companies without a presence in the United States.[137] In particular, foreign users will be attracted to countries that mandate data localization to protect their native companies.[138]

From a foreign law enforcement perspective, this might not be negative as it will lighten their need to conduct cross-border data requests. From a U.S.-based company's perspective, however, this form of protectionism means a potential loss of customers and increased difficulty to conduct businesses abroad. For companies that rely heavily on foreign user traffic, the CLOUD Act's impact could be particularly problematic.

Moreover, the CLOUD Act continues to raise practical uncertainties as to conflict of law issues. While the law does allow a company to file a motion to quash or modify when it believes a foreign request is improper, such challenges are limited. Two elements must both be satisfied. The company has to reasonably believe that the customer or subscriber is neither a U.S. person[139] nor a resident of the U.S. and that "the required disclosure would create a material risk that the provider would violate the laws of a qualifying government."[140] In addition, absent other agreement or court permission, such a motion must be filed no later than fourteen days after the company was served with the request.[141]

---

[137] *See* Brief of Verizon Commc'ns Inc. et al. as Amici Curiae in Support of Appellant at 11, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985-cv).

[138] For instance, Germany requires providers of publicly available telecommunications services to store certain traffic data within Germany. *See* Lothar Determann & Michaela Weigi, Data Residency Requirements Creeping into German Law, 3 World Data Protecion Rep. (BNA) (Mar. 24, 2016).

[139] §2523(a)(2) ("The term 'United States person' means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United State.").

[140] §2713(h)(2).

[141] *Id.*

In order to "reasonably believe" that the targeted person is neither a U.S. person nor a resident of the U.S., companies must implement systems to carefully track and record the information of their customers. Because it would often be difficult to determine the nationality or residency of the person behind a profile, it is easy to imagine a situation where a company would be forced to examine the requested information first without the user's knowledge in order to get a better idea of the customer's identity. Here, the law does not specify or further define what constitutes "a material risk." Because the CLOUD Act removes the U.S. government's gatekeeping role and allows foreign law enforcement agencies to serve requests directly to the company itself, private entities, who frequently are not seasoned experts in assessing foreign conflict of law issues, will be less incentivized to scrutinize such requests and raise legal challenges.

The CLOUD Act applies not only to U.S. companies but also foreign companies that are present in the U.S. Despite having minimum contact with the U.S., they are nevertheless subject to reach of the CLOUD Act. As a result, certain foreign governments can bypass their own privacy laws by requesting data directly from the company's U.S. branch. For these companies, they will continue to face conflicting obligations between their domestic policies and U.S. legal requirements.

VI. Looking Forward

In spite of its shortcomings, the CLOUD Act is a critical step forward as governments attempt to tailor their ruling-making power to the modern technological landscape. As a pioneer in setting legal standards for cross-border data access, the CLOUD Act is an improvement from the antiquated rules and a reasonable alternative to a system that proved to be too cumbersome. By setting forth a list of preconditions, the CLOUD Act could motivate foreign nations to adopt similar safeguards and thereby increase the privacy standards that apply.[142] With such possibilities in mind, outright opposition to such legislations arguably misses the forest for the trees because "absent workable, transparent mechanisms to access data across

[142] Daskal, *supra* note 45, at 15. The author notes that this increase has already started as the U.S. government adopted a new judicial review provision with respect to compelled disclosure orders for data in part because it anticipated that provision being a precondition to be eligible for an executive agreement with the United States. She expects that other countries will be motivated to raise privacy protections as well. *See also* Jennifer Daskal & Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, JUST SECURITY (Mar. 14, 2018), https://www.justsecurity.org/54163/privacy-civil-liberties-cloud-act-response/.

borders, governments will seek access by other means, whether via data localization mandates or other, more surreptitious means."[143]

A. Potential Measures of Improvement

With its undeniable advantages, absent a case-by-case analysis, the CLOUD Act could potentially pave the way for other legislations that broaden the scope of law enforcement's access to private information. While it is a step in the right direction, further safeguards, such as an amendment or implementation of other mechanisms, are needed to address privacy protection concerns.[144]

To address the most notable criticism that the CLOUD Act grants too much discretion in the Executive Branch, the CLOUD Act should set forth guidelines to assist companies in directly complying with the requests of foreign governments while also remaining vigilant in protecting their clients' privacy rights. Particularly, the CLOUD Act could expressly clarify the methods a U.S.-based CSP may use to seek judicial redress or elicit instructions from domestic agencies before turning requested data to law enforcement.

External possibilities for improvement exist as well. One option is to strengthen the existing process under the MLATs. Because the major issue that led to the enactment of the CLOUD Act was how cumbersome it was to procure cross-border data access using the MLAT system, both the U.S. law enforcement and its foreign counterparts could benefit without raising more privacy concerns by implementing "improved resources, training, and streamlining."[145]

Another option is to allow a multilateral treaty that incorporates "not just the U.S.'s but multiple stakeholders' interests."[146] By creating a streamlined process, a multilateral treaty will help overcome any

[143] Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L. J. F. 1029, 1046–47 (Apr. 1, 2019).
[144] *See, e.g.,* Green, *supra* note 99 (arguing that the improvements it made "are not enough to shift the balance so that the CLOUD Act will be a boon, rather than a threat, to privacy and human rights.").
[145] The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data.
[146] Bilgic, *supra* note 27, at 351. The author does note that treaty-making is costly and time consuming. Moreover, to countries who are not as concerned about the implications of the CLOUD Act, they will be less likely to abide by a uniform international standard. Instead, data localization might be an easier way to protect their domestic users.

potential conflicts of law issues.[147] At the same time, because all countries, including the U.S., have to undertake the same cross-border data access process, foreign users would not have to fear that their data is targeted by a particular country.[148]

B. A Glimpse into the Future of the CLOUD Act

On October 3, 2019, the United States and the United Kingdom entered into the first executive agreement under the CLOUD Act.[149] This agreement addresses some of the criticisms about the CLOUD Act and reinforces the notion that the law provides incentives in the positive direction. Among other improvements, the agreement provides an additional qualify control mechanism by specifying that cross-border orders must be reviewed and certified as lawful by a designated authority, such as a government entity chosen by the Attorney General in the U.S., or the Secretary of State for the Home Department for the U.K.[150] A recipient can raise objections to the designated authority, who retains the ultimate veto power to block enforcement of the order.[151]

This historical partnership is not without drawbacks.[152] For instance, the agreement allows disclosure of content information when there is "reasonable justification based on articulable and credible facts, particularity, legality, and severity."[153] Once again, this requirement is vague and arguably weaker than the probable cause standard.[154] Additionally, the agreement clarifies that "serious crime" as applied between the two countries includes crimes that require a maximum punishment of three or more years of

---

[147] *Id.*
[148] *Id.* at 352.
[149] *See, e.g.*, Gidari, *supra* note 15.
[150] Jennifer Daksal & 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 (listing a number of other privacy and civil liberties safeguards by the UK.-U.S. agreement that go beyond the text of the CLOUD Act).
[151] *Id.*
[152] The most contested provision of the U.K.-U.S. CLOUD Act agreement is related to its wiretap provision, allowing either the U.S. or U.K. to require a CSP to wiretap a user located in a third country without that government's prior approval. *See* Gidari, *supra* note 15.
[153] U.S-U.K Agreement art. 5(1).
[154] Sign On: Coalition Statement Re. U.S.-U.K. Cloud Act Executive Agreement, Government Accountability Project (Oct. 29, 2019), https://www.whistleblower.org/sign-on-letter/sign-on-coalition-statement-re-u-s-u-k-cloud-act-executive-agreement/.

incarceration, excluding misdemeanors and minor felonies.[155] While this confronts one of the "specificity" concerns, the result falls flat. While three years is more than what the *Duncan* Court envisioned for purposes of the Sixth Amendment, the agreement seems to prove that the scope of "serious crime" as defined by the CLOUD Act is flexibly tailored to the considerations of negotiating parties, and not modeled after an established legal standard.

It should be noted that other CLOUD Act negotiations are also under way. On October 7, 2019, the Department of Justice announced that the United States and Australia have entered into formal negotiations for a bilateral agreement under the CLOUD Act.[156] On Febuary 5, 2019, the European Commission recommended a Council decision authorizing the opening of CLOUD Act negotiations between the European Union and the United States.[157] A prospective U.S.-EU agreement presents more complications due to the European Union's own privacy laws and potential conflict of law claims could be raised. The Committee on Civil Liberties, Justice, and Home Affairs of the European Parliament noted several incompatibilities between the CLOUD Act and the EU e-evidence proposal.[158] A U.S.-based CSP that collects or store data in a third country but also offers services in the European Union could be subject to both the CLOUD Act and the proposed EU e-evidence rule which stipulates the appointment in the EU of a legal representative of the U.S.-based CSP.[159] If the data is located in the U.S., the CLOUD Act applies if there is an executive agreemet with the third country but the e-evidence proposal has no such requirement.[160] The CLOUD Act and the e-evidence proposal have two different review procedures and it

[155] Daskal & Swire, *supra* note 150.
[156] Joint Statement Announcing United States and Australian Negotiations of a CLOUD Act Agreement by Attorney General William Barr and Minister for Home Affairs Peter Dutton, JUSTICE NEWS (Oct. 7, 2019), https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.
[157] Recommendation for a Council Decision Authorizing the Opening of Negotiations in View of an Agreement between the European Union and the United States of American on cross-border access to electronic evidence for judicial cooperation in criminal matters, EUROPEAN COMMISSION (Feb. 2, 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019PC0070.
[158] 4th Working Document (B), Committee on Civil Liberties, Justice and Home Affairs, 3 (Mar. 11, 2019), http://www.europarl.europa.eu/doceo/document/LIBE-DT-636344_EN.pdf?redirect.
[159] *Id.*
[160] *Id.*

is unclear which standard applies if a conflicting obligation arises.[161] The European Union's General Data Protection Regulation (GDPR) which took effect in May 2018 and contains specific rules governing data transfer outside the EU[162] is another barrier to a U.S.-EU alliance under the CLOUD Act.[163]

The signing of the first executive agreement is only a glimpse of how the CLOUD Act will appease its supporters and confront its challengers. Without executions of cross-border data requests under the CLOUD Act, the task of ascertaining the validity of its criticisms remains a strenuous one.

VII. Conclusion

The conflict between the government's need to ensure security and private individuals' interest to safeguard their personal information will continue to concern lawmakers, law enforcement agencies, communications service providers, and private users alike. The increased volume and significance of electronic evidence in a global scale have given rise to higher burden on law enforcement agencies, who must grapple with the phenomenon that technology frequently defies traditional legal means. Such increased burden, however, does not necessitate weaker privacy protection.

The CLOUD Act is a successful beginning to a resolution of this conflict. Nevertheless, it must be equipped with further procedural and substantive safeguards to properly address the need for efficiency without eroding digital privacy.

---

[161] *Id.*

[162] Theodore Christakis, *Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?*, 2 (May 27, 2019), https://ssrn.com/abstract=3397047.

[163] Bart W. Huffman, Cynthia O'Donoghue, et al, *Potential Conflicts 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. Generally speaking, the current situation regarding the interplay between the CLOUD Act and the GDPR is unclear. Christakis, *supra* note 162. To illustrate a potential conflict, for instance, the CLOUD Act allows a motion to quash or modify only if the targeted person is a non-U.S. person living outside the United States, while the GDPR applies "even to 'controller' processing of the personal data of U.S. citizens living in the EU" and this person protected under the GDPR may have to disclose his or her personal data under the CLOUD Act. *Id.*