Harvard Journal of Law & Technology
Volume 32, Number 1 Fall 2018

SOMETHING OLD, SOMETHING NEW, AND SOMETHING MOOT: THE PRIVACY CRISIS UNDER THE CLOUD ACT

*Secil Bilgic**

TABLE OF CONTENTS

I. INTRODUCTION

The ubiquitous use of the Internet has increased law enforcement agents' reliance on data stored by information and communications technology (ICT) companies. Since many of the major ICT companies are located in the U.S.,[1] courts and law enforcement agents around the globe

* Harvard Law School, LL.M. 2018; Fulbright Scholar 2017-2018; Koç University, LL.B. (*summa cum laude*) & B.A. in International Relations (*summa cum laude*), 2017. Currently practicing at GKC Partners, associated law firm of White & Case LLP, and will soon become a member of both the Istanbul and the New York State Bar. Many thanks to Professor Urs Gasser and Professor Chris Bavitz for their insightful comments on the earlier versions of this Note. Thanks also to the Article Editor Nicole Pobre and to the entire staff at JOLT for their dedication and support. As always, I would also like to thank my family, especially my mother and Yavuzhan Yilancioglu, for their continuous support and encouragement in all my endeavors.

1. Kristin Stoller, *The World's Largest Tech Companies 2017: Apple and Samsung Lead, Facebook Rises*, FORBES (May 24, 2017), https://www.forbes.com/sites/kristinstoller/2017/

have to seek the U.S. government's assistance in obtaining necessary digital evidence.[2] For instance, in an investigation regarding French citizens who reside in Paris, French law enforcement agents might have to request assistance from the U.S. Department of Justice if the suspects in question were using a U.S.-based email service.[3] Unfortunately, the available methods to obtain evidence in the U.S. are slow and opaque.[4] This prolonged cross-border data access process frustrates foreign countries, as it is hard, if not impossible, for them to access evidence about even their own citizens related to a crime occurring in their own territory.[5]

The emergence of cloud computing has exacerbated this frustration. Cloud computing refers to "storing and accessing data and programs over the Internet instead of your computer's hard drive."[6] Accordingly, the cloud prevents the loss of data due to computer crashes, is less vulnerable to theft, and provides an easy medium to share files.[7] To achieve these benefits, cloud service providers move an individual's data from one jurisdiction to another or "shard" the data and store it on servers in different jurisdictions.[8] Thus, though the user and the cloud service provider stay in a single jurisdiction, the data might travel through several jurisdictions, often unbeknownst to the user and the law enforcement

---

05/24/the-worlds-largest-tech-companies-2017-apple-and-samsung-lead-facebook-rises/#2bbbb9e2d140 [https://perma.cc/787Q-MTV7].

2. *See* U.S. DEP'T OF JUSTICE, FY 2015 BUDGET REQUEST: MUTUAL LEGAL ASSISTANCE TREATY PROCESS REFORM 1 (2014), https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf [https://perma.cc/N6ZC-R9FY] ("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.").

3. *See* Peter Swire, Justin D. Hemmings & Suzanne Vergnolle, *A Mutual Legal Assistance Case Study: The United States and France*, 34 WIS. INT'L L.J. 323, 327 (2016).

4. ANDREW K. WOODS, GLOBAL NETWORK INITIATIVE, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET AGE 3 (2015), https://uknowledge.uky.edu/cgi/viewcontent.cgi?&httpsredir=1&article=1517&context=law_facpub [https://perma.cc/F6SD-R34M].

5. *See* Swire, Hemmings & Vergnolle, *supra* note 3, at 327 ("[T]he current average response time [is] ten months for MLA requests to the United States."); Tiffany Lin & Mailyn Fidler, *Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement*, 2–4 (Berkman Klein Ctr., Paper No. 2017-7, 2017) ("Countries have grown frustrated with both the normative implications of the MLAT process and its typical lengthiness.").

6. Eric Griffith, *What Is Cloud Computing?*, PC MAG. (May 3, 2016, 12:01 A.M.), https://www.pcmag.com/article2/0,2817,2372163,00.asp [https://perma.cc/D5MK-RWCD].

7. Brief for Amici Curiae Computer and Data Science Experts in Support of Appellant Microsoft Corp. at 8, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2014) (No. 14-2985) [hereinafter Brief of Experts].

8. Margaret Rouse, *Definition: Sharding*, TECHTARGET, https://searchcloudcomputing.techtarget.com/definition/sharding [https://perma.cc/S79R-2MG7] ("In the simplest sense, sharding your database involves breaking up your big database into many, much smaller databases that share nothing and can be spread across multiple servers.").

agent.[9] This means that, to obtain a few emails, the law enforcement agent may have to initiate cross-border data access procedures in several countries, which would significantly prolong the prosecution or adjudication. As cloud computing becomes more prevalent, data travel, and thus burdensome cross-border data access procedures, may soon become the rule rather than the exception.[10]

Against this backdrop arose *United States v. Microsoft Corporation* (*Microsoft Ireland*),[11] where Microsoft refused to comply with a U.S. warrant because the requested data was stored in Ireland.[12] On March 23, 2018, while this case was pending before the Supreme Court, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was signed into law.[13] Though the *Microsoft Ireland* case was mooted by the CLOUD Act, it remains relevant as it revealed countervailing opinions regarding the impact of cross-border data access on privacy and foreign relations.[14]

This Note will primarily focus on the privacy implications of the *Microsoft Ireland* case and the CLOUD Act, especially for non-U.S. citizens. Part II of this Note provides a background of the current legal system by explaining the Fourth Amendment privacy framework, the Stored Communications Act, and how Mutual Legal Assistance Treaties (MLATs) work. Part III outlines the facts, procedural history, and holdings of the Southern District of New York and the Second Circuit in the *Microsoft Ireland* case. Part IV examines the implications of the newly enacted CLOUD Act on the digital privacy of cloud users around the world and concludes that the digital privacy of users both inside and outside of the U.S. will diminish. While many commentators have focused on the privacy implications of the CLOUD Act on U.S. citizens,[15] this

9. *See id.*

10. *See* Kasey Panetta, *Cloud Computing Enters its Second Decade*, GARTNER (Jan 30, 2017), http://www.gartner.com/smarterwithgartner/cloud-computing-enters-its-second-decade/ [https://perma.cc/Y9SC-J33P] ("By 2020, anything other than a cloud-only strategy for new IT initiatives will require justification at more than 30% of large-enterprise organizations . . . By 2021, more than half of global enterprises already using cloud today will adopt an all-in cloud strategy.").

11. 138 S. Ct. 1186 (2018).

12. *Id.* at 1187.

13. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Consolidated Appropriations Act, Pub. L. No. 115-141, div. V, 132 Stat. 348, 1213–25 (2018) [hereinafter CLOUD Act].

14. *See, e.g.*, Jennifer Daskal, *Case to Watch: Microsoft v. US on the Extraterritorial Reach of the Electronic Communications Privacy Act*, JUST SECURITY (Mar. 6, 2015), https://www.justsecurity.org/20780/case-watch-microsoft-v-united-states-extraterritorial-reach-electronic-communications-privacy-act/ [https://perma.cc/69UM-7BMP].

15. *See, e.g.*, Neema Singh Guliani, *New CLOUD Act, Supported by Major Tech, Trusts Sessions and Pompeo to Defend Our Human Rights*, THE HILL (Mar. 30, 2018, 3:20 P.M.), http://thehill.com/blogs/congress-blog/civil-rights/379367-new-cloud-act-supported-by-major-tech-trusts-sessions-and [https://perma.cc/N49D-Y6R3] ("Congress should reject the CLOUD

Note argues that the privacy ramifications of the CLOUD Act will be more severe for foreign citizens since their own countries, the U.S., and qualifying foreign governments will all have virtually unlimited access to their data with minimal safeguards. With these problems in mind, Part V proposes an alternative framework that would incorporate various stakeholders' interests more aptly than both MLATs and the CLOUD Act. Finally, Part VI concludes.

II. FOURTH AMENDMENT, STORED COMMUNICATIONS ACT, AND MLATS: OLD LAWS FOR NEW TECHNOLOGIES

Concerned with undue privacy interference by press journalists and photographers, Samuel Warren and future Justice Louis Brandeis conceived the idea of a right to privacy in their seminal article *The Right to Privacy*.[16] As the case law and doctrine evolved, five dominant species of privacy emerged: tort, Fourth Amendment, First Amendment, fundamental-decision, and state-constitutional privacy.[17] This Note is concerned with the Fourth Amendment's conception of privacy rights.

A. The Fourth Amendment

The Fourth Amendment protects individuals against "unreasonable searches and seizures" by the government.[18] Pursuant to *Katz v. United States*,[19] the Fourth Amendment applies when a person exhibits an "actual or subjective expectation of privacy" which society is prepared to recognize as reasonable.[20] However, throughout the 1980s, the Supreme Court significantly pared back this Fourth Amendment protection.[21]

The development of the third-party doctrine in cases such as *United*

Act because it fails to protect human rights or Americans' privacy . . . gives up their constitutional role, and gives far too much power to the attorney general, the secretary of state, the president and foreign governments."); David Ruiz, *Responsibility Deflected, the CLOUD Act Passes*, ELEC. FRONTIER FOUND. (Mar. 22, 2018), https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes [https://perma.cc/C253-FZQT].

16. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.").

17. Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1339 (1992) ("[L]egal privacy consists of four or five different species of legal rights which are quite distinct from each other and thus incapable of a single definition.").

18. U.S. CONST. amend. IV.

19. 389 U.S. 347 (1967).

20. *Id.* at 361 (Harlan, J., concurring).

21. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 449–52 (1989); California v. Greenwood, 486 U.S. 35, 39–40 (1988); New Jersey v. T.L.O., 469 U.S. 325, 347 (1985); *see also* Jana Nestlerode, *Re-Righting the Right to Privacy: The Supreme Court and the Constitutional Right to Privacy in Criminal Law*, 41 CLEV. ST. L. REV. 59, 71–79 (1993) (criticizing this trend).

States v. Miller[22] was particularly significant in this process.[23] Under the third-party doctrine, which is still applicable today, individuals do not enjoy a reasonable expectation of privacy in information that they have voluntarily disclosed to third parties.[24] Though the Supreme Court recently ruled in *Carpenter v. United States*[25] that access to a person's historical cell-site records constitutes an exception to this doctrine,[26] and hence amounts to a search within the meaning of the Fourth Amendment, *Carpenter's* impact beyond cell-site records is unclear.[27] Chief Justice Roberts, who penned the opinion, declared "[o]ur decision today is a narrow one."[28] If *Carpenter* only applies to cell-site records, the Fourth Amendment may not protect wire or electronic communications since these communications are necessarily disclosed to a third party.[29] Thus, in a networked environment, the Fourth Amendment provides little to no privacy protection.[30] The real protection for electronic communications comes from the Stored Communications Act (SCA).

B. The Stored Communications Act

To address this privacy gap that the third-party doctrine created,

---

22. 425 U.S. 435 (1976).

23. *See, e.g.*, *id.* at 443. ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . .").

24. *Id.*; *see also* Couch v. United States, 409 U.S. 322, 335 (1973) ("[T]here can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return."); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1151 (2002) (discussing development of third-party doctrine).

25. 138 S. Ct. 2206 (2018).

26. *Id.* at 2217.

27. *See, e.g.*, Orin Kerr, *Understanding the Supreme Court's Carpenter Decision*, LAWFARE (June 22, 2018, 1:18 P.M.), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/56Z5-H3J2].

28. *Carpenter*, 138 S. Ct. at 2220 ("We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools . . . [n]or do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.").

29. *See* Kerr, *supra* note 27 ("In effect, disclosure [to a third party] is enough to eliminate privacy when the records disclosed only involve a normal amount of privacy."); *see also* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, WM. & MARY L. REV. 2105, 2114 (2009) ("Whether Internet users have a reasonable expectation of privacy in their emails and web surfing data is largely unresolved. Unlike traditional letters, emails and web surfing communications are often copied in transit by Internet Service Providers (ISPs) and are (in theory) easily accessed by ISP employees.").

30. For an argument that third-party doctrine does not apply if it gives the government "massive powers," see Kerr, *supra* note 27 ("The way I read his opinion, the chief seems to be saying that there is an equilibrium-adjustment limit on the third-party doctrine. Once the third-party doctrine starts to give the government massive new powers, the third-party doctrine may no longer apply.")

Congress enacted the SCA.[31] The SCA forms Title II of the Electronic Communications Privacy Act (ECPA) and limits access to stored communications and records held by service providers.[32] Title I of the ECPA, the Wiretap Act, is devoted to regulating the interception of real-time communications,[33] and Title III, the Pen Register Act, regulates pen registers and trap and trace devices.[34]

Table 1: Electronic Communications Privacy Act

	Electronic Communications Privacy Act		
Section of ECPA	**Title I: <u>The Wiretap Act</u>**	**Title II: <u>The Stored Communications Act</u>**	**Title III: <u>The Pen Register Act</u>**
Regulated Activity	Prospective surveillance[35] + content information[36]	Retrospective surveillance[37] + content & non-content information	Prospective surveillance + non-content information[38]
Restrictions on collection	18 U.S.C. § 2511(1) prohibits real time interception of telephone calls and computer communications unless an exception applies or investigators have a super warrant.	18 U.S.C. §§ 2702–03 create limits on governmental power to compel disclosure and limit an internet service provider's right of voluntary disclosure of the information.	18 U.S.C. § 3121 prohibits use of a pen register or trap and trace device to discover non-content information.

The SCA was designed by taking into account the prominent func-

31. 18 U.S.C. §§ 2701–12 (2018); *see also* Eric R. Hinz, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 492 ("The SCA was passed in large part to cover areas of electronic information left open by the Fourth Amendment.").

32. 18 U.S.C. § 2702.

33. *Id.* §§ 2510–22.

34. *Id.* §§ 3121–27.

35. Prospective interception is the interception of communications in transit while retrospective interception refers to the collection of stored communications. *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 616 (2002) ("Is the surveillance designed to capture future communications that have not yet been sent over the network ("prospective" surveillance), or is it designed to look for stored records and past communications that may be retained in the network ("retrospective" surveillance)? Wiretapping a telephone provides the classic example of prospective surveillance.").

36. "Contents" is defined as "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8).

37. *See* Kerr, *supra* note 35, at 616.

38. Non-content information includes any "dialing, routing, addressing, or signaling information," other than content information, associated with an electronic communication. 18 U.S.C. § 3127(3)–(4).

tions computers performed when the act was enacted in 1986.[39] For instance, the SCA regulates only two types of service providers — Electronic Communication Service (ECS) providers and Remote Computing Service (RCS) providers — because those were the primary services used by computers in 1980s.[40] ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[41] For example, "telephone companies and electronic mail companies" are ECSs since they allow people to send and receive wire or electronic communications.[42] RCS, on the other hand, "is the provision to the public of computer storage or processing services by means of an electronic communications system."[43] For instance, Google Drive and other cloud storage services are RCSs.[44] To compel an ECS provider to disclose contents in storage for more than 180 days or to compel a RCS provider to disclose contents, the government has three options: warrant, subpoena plus notice, or a § 2703(d) order ("super search warrant") plus notice.[45]

With such requirements, the SCA limits both the government's ability to compel internet service providers ("ISPs") to disclose information in their possession about their customers and subscribers as well as ISPs' ability to voluntarily disclose information to the government. Thus, the SCA "extend[s] to electronic records privacy protections analogous to those provided by the Fourth Amendment."[46]

However, today, most providers undertake both functions.[47] Thus, technological developments complicated the implementation of the SCA.[48] For the purposes of the *Microsoft Ireland* case, the focal question

---

39. 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, 1214 (2004) (noting SCA "fr[oze] into the law the understandings of computer network use as of 1986").

40. *Id.*

41. 18 U.S.C. § 2510(15).

42. *See* S. REP. No. 99-541, at 14.

43. 18 U.S.C. § 2711(2).

44. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act,* 162 U. PA. L. REV. 373, 387 (2014) (noting Google Drive is a service included under RCS rules).

45. *See* 18 U.S.C. § 2703. Note that under the third-party doctrine, the government could obtain the data with a simple subpoena, which unlike a warrant, does not require probable cause. *See* Kerr, *supra* note 39, at 1211.

46. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 206 (2d Cir. 2016).

47. *See* Kerr, *supra* note 39, at 1215–16; Hinz, *supra* note 31, at 496 ("[W]hen one person sends electronic communication to another person, the provider of the service remains an ECS during the process up until the point when the message is opened . . . [When opened], the provider is holding the message in storage and is acting as an RCS." (footnotes omitted)).

48. Kerr, *supra* note 39, at 1230 ("But how to interpret what counts as a 'processing service'? The invention of the World Wide Web is the primary source of the difficulty. Consider a website such as the popular online auction site eBay. Does eBay provide RCS?" (footnote omitted)).

was whether a § 2703(d) order is a type of warrant, a subpoena, or a hybrid form because depending on the answer, the Supreme Court could have come to different conclusions as to the extraterritorial application of the SCA.[49] As I will discuss later, the CLOUD Act answered this question by amending the SCA[50] and specifically authorizing a government entity to compel a U.S.-based provider to turn over data stored in another country.[51]

C. Mutual Legal Assistance Treaties

Currently, the U.S. has two types of treaties that govern obtaining evidence abroad: Mutual Legal Assistance Treaties (MLATs) for criminal investigations and the Hague Convention on Taking Evidence Abroad in Civil or Commercial Matters ("Hague Convention").[52] While the Hague Convention is a multilateral treaty, MLATs are bilateral due to the United States' insistence.[53] The bilateral nature of MLATs means that "progress in mutual assistance in criminal matters can fairly be said to be half a century behind."[54]

To request data access in the absence of an existing MLAT with the U.S., a foreign court must write a "letter rogatory" to the proper U.S. court through diplomatic channels.[55] However, the U.S. court is not under any obligation to assist the requesting court.[56] As the name suggests,

---

49. *See In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 471 (S.D.N.Y. 2014) [hereinafter *Microsoft Ireland SDNY*] (explaining that an SCA warrant is "obtained like a search warrant . . . upon a showing of probable cause . . . [but] is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP."); *Microsoft*, 829 F.3d at 212–15 (rejecting lower court's hybrid approach and interpreting SCA's "warrant" as term of art).

50. *See infra* Section IV.

, at 17.

51. CLOUD Act § 103(1); *see also* Taylor Hatmaker, *As the CLOUD Act Sneaks into the Omnibus, Big Tech Butts Heads with Privacy Advocates*, TECHCRUNCH (Mar. 23, 2018), https://techcrunch.com/2018/03/22/cloud-act-omnibus-bill-house/ [https://perma.cc/4CAP-FN2Q].

52. T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, FED. JUD. CTR., at 1 (2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf [https://perma.cc/MEG7-L2ZX].

53. C. Gane & M. Mackarel, *The Admissibility of Evidence Obtained from Abroad into Criminal Proceedings — The Interpretation of Mutual Legal Assistance Treaties and Use of Evidence Irregularly Obtained*, 4 EUR. J. CRIME CRIM. L. & CRIM. JUST. 98, 99–100 (1996) ("[A]ttempts to develop a multilateral treaty on judicial assistance in penal matters were thwarted by opposition from those states which preferred bilateral arrangements, (principally the United States and the United Kingdom).").

54. DAVID MCCLEAN, CO-OPERATION IN CRIMINAL AND CIVIL MATTERS 153 (2012).

55. Gane & Mackarel, *supra* note 53, at 99 ("Until comparatively recently, the international exchange of evidence on an organized basis involved the exchange of letters rogatory . . . .").

56. *See, e.g.*, *In re* Letters Rogatory from Tokyo Dist., Tokyo, Japan, 539 F.2d 1216, 1219 (9th Cir. 1976) ("[T]he district court is given discretion in determining whether letters rogatory

MLATs were designed to solve this problem and create international law obligations for the parties to assist each other in criminal investigations.[57]

Under the MLAT process, to request data access, a foreign country contacts the Office of International Affairs ("OIA") of the U.S. Department of Justice ("DOJ").[58] If the DOJ deems the request appropriate and in line with U.S. standards, the Department sends the request to a local U.S. magistrate judge.[59] The court then reviews the foreign agency's request in light of all "relevant U.S. law, notably including the Fourth Amendment's probable cause standard, rules of privilege, and the Fifth Amendment."[60] If the court is satisfied, it issues a warrant addressed to the relevant ISP.[61] The ISP then submits the relevant data to OIA.[62] After the office reviews it under "data minimization and human rights standards," OIA sends the data to the requesting country.[63] Accordingly, OIA and magistrate judges have robust gatekeeping powers concerning the incoming data access request. However, these gatekeeping powers significantly prolong the process.[64]

The rise of cloud computing has highlighted additional problems with digital evidence access through the MLAT process. Cloud computing is the on-demand delivery of computing power, database storage, applications, and other IT resources through a cloud services platform via the Internet.[65] Cloud computing complicates cross-border data access in three ways. First, when data is shared and stored across multiple data

---

should be honored."); *In re* Letters Rogatory Issued by Nat'l Court of First Instance in Commercial Matters N. 23 of Fed. Capital of Argentinean Republic, 144 F.R.D. 272, 274 (E.D. Pa. 1992) ("Because this is a subpoena granted pursuant to Letters Rogatory, this Court has broad discretion to decide whether to honor requests for foreign assistance."); *see also* Funk, *supra* note 52, at 3 ("The process for letters rogatory is more time-consuming and unpredictable than that for MLATs. This is in large part because the enforcement of letters rogatory is a matter of comity between courts, rather than treaty-based.").

57. Funk, *supra* note 52, at 5 ("MLATs are legally binding negotiated commitments.").

58. *Id.* at 3.

59. Lin & Fidler, *supra* note 5, at 2.

60. *Id.*

61. *Id.*

62. *Id.* at 3.

63. *Id.*; *see also* United States v. Global Fishing (*In re* Premises Located at 840 140th Ave., NE, Bellevue, Wash.), 634 F.3d 557, 572 (9th Cir. 2011) (stating that district courts might not be able to enforce subpoena that would result in "egregious violation of human rights.").

64. Lin & Fidler, *supra* note 5, at 4; Mailyn Fidler, *MLAT Reform: Some Thoughts from Civil Society*, LAWFARE (Sept. 11, 2015), https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society [https://perma.cc/GW7K-8E5P] ("[The MLAT] process contains checks and balances that protect rights but contribute to delays, pushing countries towards faster ways of accessing data that lack protections.").

65. Steve Ranger, *What is Cloud Computing? Everything You Need to Know About the Cloud, Explained*, ZDNET (Jan. 24, 2018, 5:50 PST) https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-from-public-and-private-cloud-to-software-as-a/ [https://perma.cc/E8PG-RWSK].

servers, there may be more than one home state of the requested piece of evidence. Theoretically, email providers like Google or Microsoft could shard email messages of an account and store the resulting "slices of data" in servers in California, Ireland, and Japan.[66] Thus, with cloud computing, a law enforcement agent in the U.K. attempting to access several email messages might have to initiate several MLAT processes to access a single piece of evidence. This assumes that the law enforcement agent can first successfully predict where the data might be stored, not an easy task due to the vast number of global servers.[67] Assume, for instance, an Indian prosecutor begins an MLAT process with the U.S. to obtain a defendant's emails from his Gmail account. However, unbeknownst to the prosecutor, Gmail's data dispersal algorithm sliced the requested mailbox and stored some of the emails in Thailand. In this hypothetical, the data access process is likely to be both time-consuming and fruitless since the requested data is not on the U.S. servers.

The second and related problem is the fact that data dispersal algorithms, a key part of cloud computing, may move data from one server to another based on users' locations, available bandwidth, or even legal constraints.[68] When data is sharded and on the go, "neither the requesting country's authorities nor the [Multinational Cloud Service Provider] itself can tell where the data being requested is physically stored until it is retrieved."[69]

The last problem is the nature of digital evidence. Legal scholar Vivek Krishnamurthy notes that "[u]nlike physical places and things — whose ownership is comparatively easy to determine up front — the ownership of an electronic account often can't be identified without first rifling through its contents."[70] Indeed, when creating a Microsoft email account, a U.S. citizen might declare herself as an Irish citizen, which

66. *But see* Brief of Experts, *supra* note 7, at 19–20 (noting that email providers choose not to store closely related slices of data across different countries since such an approach would be "a very inefficient use of these techniques.").

67. *See Mark* Walsh, *Microsoft Case Underscores Legal Complications of Cloud Computing*, ABA JOURNAL (Feb. 2018), http://www.abajournal.com/magazine/article/microsoft_case_underscores_legal_complications_of_cloud_computing [https://perma.cc/7KSY-JU8M] (For instance, "Microsoft manages more than 1 million server computers in over 100 data centers in 40-plus countries across the globe . . . The company migrates customer emails daily from one data center to another for various business reasons but typically sends them to a center close to the customer's location.").

68. Vivek Krishnamurthy, *Cloudy with a Conflict of Laws* 5 (Berkman Klein Ctr., Paper No. 2016-3, 2016). *But see*, Brief of Experts, *supra* note 7, at 17 (arguing that email accounts are not frequently transferred between various servers because "simply copying data to a new location does not remove the data from its initial physical location" and frequently moving data would be "inefficient and expensive and require[s] bandwidth that could otherwise be used to satisfy customer requests.").

69. Krishnamurthy, *supra* note 68, at 5. *But see* Brief of Experts, *supra* note 7, at 16 (arguing that cloud computing does "not render the data more difficult to locate").

70. Krishnamurthy, *supra* note 68.

will lead Microsoft to store her data in Ireland.[71] Mere retrieval of the data would not help the authorities or Microsoft in understanding the user's actual citizenship. As the next part analyzes in more detail, this was a prominent concern for the government and the Supreme Court.

III. SOMETHING OLD, SOMETHING NEW, AND SOMETHING MOOT: *UNITED STATES V. MICROSOFT CORPORATION*

The *Microsoft Ireland* saga began when a magistrate judge of the Southern District of New York issued a warrant to Microsoft, directing the company to seize and produce the contents of a customer email account.[72] Microsoft moved to quash the warrant as the requested data was stored in Ireland.[73] The Southern District of New York denied Microsoft's motion to quash a warrant issued under § 2703 of the Stored Communications Act ("SCA warrant"), and held Microsoft in contempt for refusing to execute the warrant.[74] Arguing that the SCA warrant was subject to territorial limits, Microsoft appealed.[75] The Second Circuit ruled in favor of Microsoft and quashed the warrant.[76] Subsequently, the Supreme Court granted certiorari.[77]

Before the introduction of the CLOUD Act, the parties' perception of cross-border data access was diametrically opposite. On one hand, the U.S. government was deeply concerned about data evasion. Chief Justice Roberts seemed to share this concern, as he asked whether Microsoft was arguing:

> there is nothing . . . that prevents Microsoft from storing United States communications, every one of them,

---

71. Petition for a Writ of Certiorari, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, 138 S. Ct. 1186 (2018) (No. 17-2), 3 [hereinafter *Microsoft Ireland* Petition for Certiorari] ("When a user signs up for a Microsoft email service, he is asked to identify where he is "from." Microsoft does not verify his location. Rather, Microsoft runs an automatic scan on newly created accounts and then "migrate[s]" the account data to a datacenter near the user's reported location.") (citations omitted).

72. *Microsoft Ireland SDNY*, supra note 49, at 467–68.

73. *Id.* at 468.

74. *Id.* at 477.

75. Sam Thielman, *Microsoft Case: DOJ Says It Can Demand Every Email from Any US-Based Provider,* GUARDIAN (Sept. 9, 2015), http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant [https://perma.cc/FK37-3ZM7].

76. Microsoft Corp. v. United States (*In re* a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 201–02 (2d Cir. 2016).

77. Microsoft Corp. v. United States (*In re* a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 2017 U.S. LEXIS 6343 (Oct. 16, 2017) (granting certiorari).

> either in Canada or Mexico or anywhere else, and then telling their customers: Don't worry if the government wants to get access to your communications; they won't be able to, unless they go through this MLAT procedure, which — which is costly and time-consuming.[78]

Microsoft, however, downplayed the likelihood of such evasion, claiming that only 54 of 60,000 requests related to information stored abroad.[79] Microsoft's counsel also argued that those seeking to prevent the U.S. government from seizing their emails do not use Microsoft, but opt for ISPs that specifically promise that the data is outside the U.S. government's reach.[80]

In his concurring opinion, Judge Lynch of the Second Circuit also showed concern about data evasion.[81] He stated that if the SCA lacks extraterritorial reach, Microsoft could thwart the government's demand for the emails simply by choosing to store them on a server in another country.[82] Therefore, privacy protection would not depend on traditional safeguards of judicial oversight, but rather on "business decisions" by private corporations.[83] Accordingly, he noted that "Congress would do well to take the occasion to address thoughtfully and dispassionately the suitability of many of the statute's provisions to serving contemporary needs."[84] Congress accepted this invitation and enacted the CLOUD Act.

Passed only two months before the end of the Court's term, the CLOUD Act revised portions of the SCA to explicitly permit the use of a warrant to obtain electronic communications stored by a U.S. company on foreign servers.[85] Upon the introduction of the CLOUD Act, the Department of Justice issued a new warrant for the requested Microsoft

78. Transcript of Oral Argument at 48, United States v. Microsoft Corporation, 138 S. Ct. 1186 (2018) (No. 17-2).

79. *Id.* at 50.

80. For instance, promising that data is stored in a country that does not have an MLAT with the U.S. *See id.* at 51.

81. *Microsoft*, 829 F.3d at 222 (Lynch, J., concurring) ("I write separately to clarify what, in my view, is at stake and not at stake in this case; to explain why I believe that the government's arguments are stronger than the Court's opinion acknowledges; and to emphasize the need for congressional action to revise a badly outdated statute.").

82. *Id.* at 224.

83. *Id.*

84. *Id.* at 233.

85. CLOUD Act § 103(a)(1).

data.[86] Microsoft agreed that the new warrant replaced the old one.[87] Subsequently, the Supreme Court ruled that the case had become moot.[88]

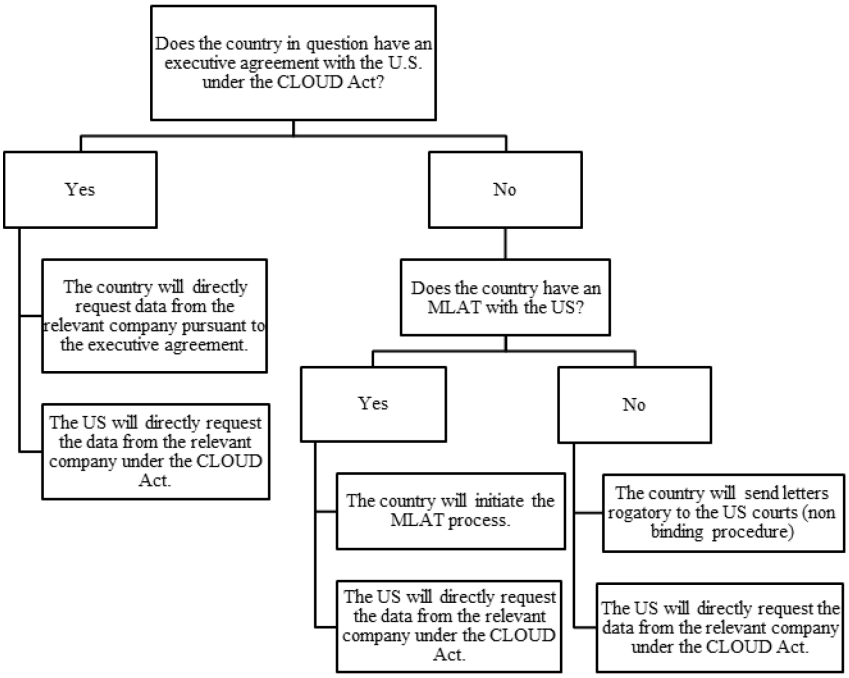

Figure 1: Cross-Border Data Access Processes to be followed by the U.S. and by another country in light of the CLOUD Act[89]

IV. THE CLOUD ACT

The CLOUD Act introduces two novelties to cross-border data access. First, it carves out an exception for "qualifying foreign governments," allowing them to bypass the MLAT process.[90] Qualifying

86. United States v. Microsoft, 138 S. Ct. 1186, 1188 (2018).

87. *Id.*

88. *Id.* ("No live dispute remains between the parties over the issue with respect to which certiorari was granted. Further, the parties agree that the new warrant has replaced the original warrant. This case, therefore, has become moot." (citation omitted)).

89. This table assumes that the data is stored by a U.S.-based company.

90. Robyn Greene, *OTI to Congress: Vote No On Omnibus Bill H.R. 1625 Unless Cloud Act is Removed*, NEW AM.'S OPEN TECH. INST., https://na-production.s3.amazonaws.com/

foreign governments are those that have an executive agreement with the United States and have enacted laws that provide "substantive and procedural opportunities" specified in the CLOUD Act to electronic communication service providers and remote computer providers.[91] While the U.S. has not signed any such executive agreements as of December 2018, negotiations with the U.K. are currently underway.[92] If the countries come to terms and execute the agreement, there will be three types of foreign governmental access to the data stored in the U.S. One, qualifying foreign governments will be able to directly retrieve data from U.S. companies. Two, countries with an MLAT in place with the U.S. (but that do not have an executive agreement) will be able to initiate the MLAT process. Lastly, those with neither an MLAT nor an executive agreement will have to seek data through letters rogatory.

Second, the CLOUD Act resolves the central question in the Microsoft Ireland case by creating § 2713 of the SCA.[93] Under § 2713, ECS and RCS providers must "comply with the obligations of [the SCA] . . . regardless of whether such communication, record, or other information is located within or outside of the United States."[94] Thus, the CLOUD Act clarifies the ambiguity in federal law and affirms the extraterritorial reach of the SCA.

However, the CLOUD Act does not change the MLAT system. Countries with an existing MLAT but no executive agreement will continue to follow the MLAT process. If the U.S. signs an executive agreement with a foreign country, the country will have both the MLAT and the executive agreement at its disposal. Since executive agreements offer direct and virtually unlimited access, countries with an executive agreement are likely to rely solely on the agreement. However, in a scenario in which the U.S. rescinds an executive agreement, the foreign country

documents/OTI_Cloud_Act.pdf [https://perma.cc/7AL7-HDFN] ("It would also create an exception to the Stored Communications Act to allow qualifying foreign governments to enter into an executive agreement to bypass the human rights protective Mutual Legal Assistance Treaty (MLAT) process when seeking data in criminal investigations and to seek data directly from U.S. technology companies.").

91. CLOUD Act § 103(b) (to be codified at 18 U.S.C. § 2713(h)(1)(A)).

92. Ellen Nakashima & Andrea Peterson, *The British Want to Come to America — With Wiretap Orders and Search Warrants*, WASH. POST (Feb. 4, 2016), https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america-with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html [https://perma.cc/6KVX-26YW]; *see also* Beth George & Brett Weinstein, *Congress Enacts the CLOUD Act, Granting Law Enforcement Access to Information Stored Abroad, and Mooting U.S. v. Microsoft*, WSGR DATA ADVISOR (May 23, 2018), https://www.wsgrdataadvisor.com/2018/05/congress-enacts-cloud-act/ [https://perma.cc/M4GT-DY96] ("The United Kingdom is widely expected to be the first foreign nation to enter into an executive agreement under the CLOUD Act, as the U.S. had entered into negotiations with the UK on a similar executive agreement before the CLOUD Act was proposed.").

93. CLOUD Act § 103(a)(1) (to be codified at 18 U.S.C. § 2713).

94. *Id.*

would still be able to initiate cross-border data access under the MLAT system.

Overall, the new scheme created by the CLOUD Act raises three major privacy concerns. First, it gives unlimited access to qualifying foreign governments. Second, by excluding non-qualifying foreign governments while allowing the U.S. to access data everywhere, it creates an unwelcoming U.S. exceptionalism to foreign governments, which will likely lead to an increase in other countries' efforts to enact data localization laws — that is, mandating that data is stored on servers physically located within the country where the data was created.[95] As I will explain in Section IV.C, these laws will also threaten the digital privacy of foreign citizens. Third, by giving global access to the U.S. government, the Act frustrates efforts by other countries to protect their citizens' data from surveillance by the U.S. Thus, the CLOUD Act is not the resolution of the *Microsoft Ireland* case, but only the beginning of a future privacy crisis, especially for foreign citizens.

Table 2: Possible Approaches to Cross-Border Data Access from a Policy Perspective

If Requesting Country:	**Criteria to access data stored in the U.S.**	**Disadvantages of approach**	**Nature of obligations**
Utilizes MLAT Process	DOJ must be satisfied & *U.S.* Magistrate judge must issue warrant supported by probable cause	Slow and burdensome process	Same obligations for parties
Utilizes an executive agreement pursuant to the CLOUD Act	To get executive agreement, Attorney General must conclude domestic law of country affords robust protections; *foreign country's own standards* will then apply	Qualifying foreign governments will obtain virtually unlimited access to data stored in U.S.	U.S. will follow its domestic process & qualifying governments will follow executive agreements

95. Jennifer Granick, The Microsoft Ireland Case and the Future of Digital Privacy, JUST SECURITY, (July 18, 2016) https://www.justsecurity.org/32076/microsoft-ireland-case-future-digital-privacy/ [https://perma.cc/3JV6-LD8A] ("If the mere fact that data isn't stored in the US means US law enforcement can't get at it, will that incentivize other nations to demand their citizens data be stored outside the US, and in their own countries? These data localization demands . . . often have public support.")

If Requesting Country:	Criteria to access data stored in the U.S.	Disadvantages of approach	Nature of obligations
Has a Data Localization law	*Foreign country's own standards* without vetting process by Attorney General	Fragmentation of Internet, cybersecurity vulnerabilities, and misuse of data by countries with bad human rights records	U.S. can still access data held outside U.S. if held by U.S.-based company; other country gets unlimited access to data, subject to its domestic standards
Is a party to the Multilateral Treaty	*International law standards* foreseen by multilateral treaty	Slow to create & compromise, may lead to vague standards	Same obligations for the parties.

A. Privacy Problems with Respect to Qualifying Foreign Governments

Pursuant to the CLOUD Act, a country becomes a qualifying foreign government if it has entered into an executive agreement with the U.S. that would "allow each government to acquire users' data stored in the other country, without following each other's privacy laws."[96] A prerequisite for such a bilateral agreement is a written certification by the Attorney General finding that "the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties."[97] If Congress fails to act within 90 days after receiving notice about the executive agreement, the agreement automatically enters into force. That is, once the executive branch enters into an executive agreement, Congress may stop such an agreement only if both the Senate and the House enact a joint resolution disapproving the agreement.[98] Even then, the executive agreement would remain valid if the president vetoes the joint resolution.[99]

Aside from sidelining Congress, the CLOUD Act also bestows virtually unchecked powers to the Attorney General since it merely lists

96. Camille Fischer, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data*, ELEC. FRONTIER FOUND. (Feb. 8, 2018), https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data [https://perma.cc/LMN7-PVXG].

97. 18 U.S.C. § 2523(b)(1) (2018).

98. Guliani, *supra* note 15 (suggesting CLOUD Act severely limits Congressional oversight over executive agreements).

99. *Id.*

"factors to be considered" rather than imposing mandatory standards.[100] Though § 2523(b)(1)(B) lists several factors that the Attorney General must consider before such certification, the non-binding nature of these factors led many commentators to state that the Executive can enter into an agreement with any country — even those without high human rights standards.[101]

For instance, the Attorney General must consider the "domestic law of the foreign government" and whether it "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection."[102] However, since the CLOUD Act neither adopts U.S. legal standards nor refers to international human rights treaties, the meaning of the words "robust," "protection," and "privacy" is left entirely to the discretion of the Attorney General. Moreover, a determination or certification by the Attorney General is not subject to judicial or administrative review.[103] As the dearth of checks on the Attorney General shows, this bilateral agreement scheme puts overly broad discretion in the hands of the executive branch.[104]

Admittedly, the CLOUD Act puts several procedural and substantive protections in place.[105] However, each safeguard falls short of the protection offered by the MLATs. Under the MLAT system, the probable cause standard applies to foreign requests.[106] Each request is scrutinized individually, ensuring that the probable cause standard will be applied by

---

100. Robyn Greene, *Skydiving Without a Parachute*, NEW AM.'S OPEN TECH. INST. 6 (Feb. 22, 2018), https://na-production.s3.amazonaws.com/documents/Cloud_Act.pdf [https://perma.cc/RX5Z-65U2].

101. 18 U.S.C. § 2523(b)(1)(B) (noting that the Attorney General must take into account whether the foreign country "has adequate substantive and procedural laws on cybercrime and electronic evidence," "demonstrates respect for the rule of law and principles of nondiscrimination," adheres to international human rights law and protects free expression, prohibits torture and "arbitrary arrest and detention," and requires "fair trial rights"); *see also* Adam Schwartz & Lee Tien, *Protect the Privacy of Cross-Border Data: Stop the DOJ Bill*, ELEC. FRONTIER FOUND. (Sept. 14, 2017), https://www.eff.org/deeplinks/2017/09/protect-privacy-cross-border-data-stop-doj-bill [https://perma.cc/K5NZ-NZS9].

102. 18 U.S.C. § 2523(b)(1).

103. *Id.* § 2523(c).

104. Fischer, *supra* note 96.

105. *See, e.g.*, 18 U.S.C. § 2523(b)(2) (requiring data minimization); *id*. § 2523(b)(4)(A) (prohibiting targeting of U.S. citizens); *id.* § 2523(b)(4)(C) (prohibiting indirect targeting of U.S. citizens); *id.* § 2523(b)(4)(D)(v) (requiring that requests by qualified foreign government be subject to "review or oversight by a court, judge, magistrate, or other independent authority").

106. *Coalition Letter Against DOJ's XBD Bill*, ELEC. FRONTIER FOUND. 2 (Sept. 20, 2017), https://www.eff.org/document/2017-09-20-coalition-letter-against-dojs-xbd-bill [https://perma.cc/6C8N-E4HL] [hereinafter *Coalition Letter*] ("The [CLOUD Act] only requires that the order by the foreign government be based 'on requirements for a reasonable justification based on articulable and credible facts . . . a lower standard than the U.S. probable cause standard that applies to foreign requests for the content of communications under current law . . . .").

a U.S. magistrate judge.[107] The CLOUD Act, on the other hand, lacks an individualized review mechanism. The following three examples aim to illustrate the possible protection gaps caused by the lack of an individualized review mechanism under the CLOUD Act.

First, the Act prohibits targeting of U.S. citizen and resident data.[108] However, it is difficult to identify the citizenship of a user without first examining the content of the requested information, especially when the requesting government only provides an account name.[109] Even if the account profile includes citizenship information, the user might intentionally or unintentionally provide false information as to their citizenship. By the time the requesting government realizes that data belongs to a U.S. citizen, it might be too late for the U.S. citizen's privacy.[110] That is, without 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.

Second, the CLOUD Act generally prohibits the foreign government from sharing the obtained data with the U.S.[111] The foreign government may only share data with the U.S. government if the foreign government believes that the collected communication "relates to significant harm or the threat of such harm to the United States or United States persons."[112] Since the CLOUD Act does not provide a definition of "significant harm," the ambiguity of this term might cause substantial damage to U.S. citizens' digital privacy.[113] As the Snowden revelations illustrated, the U.S. government has historically engaged in extensive surveillance techniques to prevent or preempt terrorism.[114] In the future, the U.S. gov-

---

107. *See* Funk, *supra* note 52, ("U.S. district courts, for their part, have considerable discretion concerning whether to authorize a foreign request. Put another way, while MLATs are legally binding commitments, *each individual application* a "requesting country" sends to a "requested country" is carefully reviewed prior to being enforced.") (emphasis added)

108. 18 U.S.C. § 2703(h)(2)(i).

109. Krishnamurthy, *supra* note 68.

110. *Microsoft Ireland* Petition for Certiorari, *supra* note 71, at 44a, n.28 ("[I]t is possible that the identity, citizenship, and location of the user of an online communication account could be unknown to the service provider, the government, and the official issuing the warrant, even when the government can show probable cause that a particular account contains evidence of a crime.")

111. 18 U.S.C. § 2523(b)(4)(C) (2018) (prohibiting indirect targeting of U.S. citizens).

112. *Id.* § 2523(b)(4)(H).

113. *See Coalition Letter*, *supra* note 106, at 2 ("In some cases, foreign governments could then voluntarily share such information about U.S. persons with the U.S. government, even though it was collected without the safeguards that would otherwise apply under the Fourth Amendment and the Wiretap Act.").

114. *See* Ewen Macaskill & Gabriel Dance, *NSA Files: Decoded*, GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2 [https://perma.cc/F6RR-BZFR] ("Since the Snowden disclosures began, the NSA and the Obama administration have justified the agency's programs by claiming they have been crucial to 'successes' in counter-terrorism.").

ernment may determine that terrorism concerns trump privacy interests once again and may begin relying on the data obtained by a qualifying foreign government. Electronic surveillance by the U.S. government in domestic security matters must comply with the Fourth Amendment or ECPA.[115] A qualifying foreign government, on the other hand, does not have to follow U.S. standards of probable cause or limitations on the Wiretap Act when requesting data from U.S. companies.[116] Thus, rather than the super warrant requirement of the Wiretap Act[117] or the notice requirement of the SCA, the more relaxed standards of a foreign country may govern the U.S. government's access.[118] For instance, the United Kingdom, which is likely the first country to become a qualified foreign government, has a concerning state surveillance law that allows the police to read texts, online instant messages and emails, and listen in on calls en masse, without requiring suspicion of criminal activity.[119] The law also prohibits notification of an interception of communications to the data subjects and forbids the introduction of evidence that an interception occurred to be used in court.[120] Thus, thanks to the CLOUD Act, "Big Brother" will watch both the U.K. and the U.S. citizens.

Third, under the CLOUD Act, requests from a qualifying foreign government must be particularized, based on "articulable and credible facts," and be subject to "review or oversight by a court, judge, magis-

115. *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 321 (1972) ("Thus, we conclude that the Government's concerns do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of a search or surveillance.").

116. Greene, *supra* note 100 ("The CLOUD Act's MLAT bypass process means that we would rely solely on review by the foreign government. However, the bill's safeguards are insufficient to ensure that the foreign government's review would protect individual rights.").

117. The "super warrant" under the Wiretap Act is a "special search warrant . . . that adds threshold requirements beyond those of ordinary search warrants (e.g. requiring the government to exhaust all other means of obtaining the information, requiring special authorization)." *See* Kerr, *supra* note 35 at 621.

118. *Coalition Letter*, *supra* note 106, at 2 ("Moreover, since the bill also permits foreign governments to voluntarily share collected U.S. person communications with third-party governments in certain situations, including those that do not meet baseline human rights standards, it further threatens the rights of people in the United States.").

119. Alan Travis, *EU Ruling Means UK Snooper's Charter May Be Open to Challenge*, GUARDIAN (Dec. 21, 2016), https://www.theguardian.com/world/2016/dec/21/eu-ruling-means-uk-snoopers-charter-may-be-open-to-challenge [https://perma.cc/3RVZ-V4EE] ("These databases can be accessed not just by the police and security services but by dozens of other public authorities, and in the case of communications data, without the need for suspicion of criminality or prior sign-off from a judge or other independent official.").

120. *See* Investigatory Powers Act 2016, c. 3, § 56 (UK); *see also* Schwartz & Tien, *supra* note 101 ("Indeed, the long-standing tradition in the United Kingdom is to prohibit service providers from notifying anyone of an interception order, and to prohibit from court proceedings any evidence that reveals an interception has ever taken place.").

trate, or other independent authority."[121] However, "oversight" does not offer the protection of judicial review since "[s]uch 'oversight' might be generalized (as opposed to case by case), and might occur after the seizure (as opposed to before it)."[122] Thus, such an oversight mechanism may not protect all of the requested data.

Protection gaps within the existing safeguards are just one part of the problem. Another issue is the CLOUD Act's failure to require qualifying foreign governments to adhere to the safeguards put in place by the Fourth Amendment and relevant privacy statutes. For instance, the CLOUD Act does not impose a notice mechanism on qualifying foreign governments. Even after the fact, the target of a data request, whether a U.S. or foreign citizen, will not receive notice and thus will not have an opportunity to ask a court to vindicate her rights and seek redress where abuses occur.[123]

As for live intercepting, the CLOUD Act merely requires orders to be for a "fixed, limited duration," "not last any longer than is reasonably necessary to accomplish the approved purposes," and be issued only if no alternative reasonable and less intrusive means exists for obtaining the information.[124] This protection falls short of that offered by the Wiretap Act, Title I of the ECPA governing prospective surveillance, which requires the government to obtain a "super warrant" to intercept contents of wire communications.[125] For many, live interception is more intrusive than interception of stored communications as it allows the government to obtain both relevant and irrelevant communications.126 This is why, unlike a regular warrant, the Wiretap Act's super warrant requires the government to exhaust all other means of obtaining the necessary information and demand a special authorization.127 In case the government

121. 18 U.S.C. § 2523(b)(3)(D)(iv) (2018). Some authors suggest that "articulable and credible facts" is essentially similar to "probable cause." *See, e.g.*, Jennifer Daskal & Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, LAWFARE (Mar. 14, 2018), https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights [https://perma.cc/BPM2-LAG4].

122. Schwartz & Tien, *supra* note 101.

123. Fischer, *supra* note 96.

124. *See* Daskal & Swire, *supra* note 121 (summarizing and defending CLOUD Act requirements for live intercept orders).

125. *See In re* Application of the U.S. for an Order, 396 F. Supp. 2d 294, 304–05 (E.D.N.Y. 2005) (noting that a wiretap order "requires additional showings not necessary to obtain a more traditional warrant"); *see also* 18 U.S.C. § 2516 (describing procedure for the super warrant); *id.* § 2518 (describing the requirements for a super warrant).

126. *See* Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring) ("The traditional wiretap or electronic eavesdropping device constitutes a dragnet, sweeping in all conversations within its scope — without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime, and intercepts the most intimate of conversations.").

127. Kerr, *supra* note 35 at 621; *see also* Michael D. Roundy, *The Wiretap Act — Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communica-*

fails to follow the super warrant process, the Wiretap Act also provides a suppression remedy.[128] The qualifying foreign governments that collect live communications of their targets, on the other hand, would not need to exhaust other remedies, require a special authorization process, or suppress the communications that were intercepted in violation of the CLOUD Act.[129]

Moreover, the CLOUD Act obligates the qualifying foreign government not to use the data obtained to infringe on freedom of speech.[130] Ostensibly, this clause aims to prevent censorship in the name of criminal investigation. However, it will most likely fail to achieve its goal for lack of specificity. Protections under freedom of speech vary in different jurisdictions. For instance, while Germany prohibits the use of Nazi symbols and hate speech, Turkey prohibits defamation of the president.[131] The CLOUD Act does not require the qualifying foreign government to follow U.S. free speech standards, does not define "freedom of speech," and does not provide an international law source for this right. Importantly, the CLOUD Act allows data requests for "serious crimes" and does not involve a "double criminality" requirement.[132] Thus, "serious crimes" might effectively mean any crime under the qualifying foreign government's domestic legislation, even one with a severe chilling effect on freedom of speech. Thus, the CLOUD Act contains yet another nebulous provision that may be abused in the wrong hands.

To make matters worse, the CLOUD Act does not regulate the ways the qualifying foreign government can convince U.S. companies to store data locally or to provide encryption backdoors.[133] As Sharon Bradford Franklin wrote, "as part of their data demands, countries could seek to require tech companies to provide 'technical assistance' that would in-

---

tions Following United States v. Councilman's Rejection of the Storage/Transit Dichotomy, 28 W. NEW ENG. L. REV. 403, 412 (2006) ("A wiretap can only be requested by certain designated state or federal prosecuting attorneys.").

128. *See* 18 U.S.C. § 2515 (2018) (for oral communications); *id.* § 2518(10) (for wire communications). Note that there is no suppression remedy for instances where the government collects data in violation of the SCA. *See* JAMES P. MARTIN & HARRY CENDROWSKI, CLOUD COMPUTING AND ELECTRONIC DISCOVERY 146 (2014).

129. Schwartz & Tien, *supra* note 101.

130. 18 U.S.C. § 2523(b)(4)(H).

131. STRAFGESETZBUCH [StGB] [Penal Code], § 86a, *translation at* https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p0877 [https://perma.cc/H72M-72BD] (Ger.) (foreseeing imprisonment for not more than three years or a fine for use of symbols of unconstitutional organizations); Türk Ceza Kanunu Madde 299 [Turkish Penal Code Article 299], *available at* http://siteresources.worldbank.org/INTINFRANDLAW/Resources/040926TurkeyCriminalCode.pdf [https://perma.cc/T7TC-GMEC] (foreseeing imprisonment for one to four years for insulting the president of the Turkish Republic).

132. *See* Funk, *supra* note 52, at 11. Double criminality or dual criminality requirement means "that the offense for which the foreign state seeks assistance also constitutes a crime in the requested state." *See id.*

133. Greene, *supra* note 100, at 8.

clude guaranteeing access to encrypted communications — an encryption backdoor."[134] Thus, if the qualifying foreign government wishes to expand its access, under the CLOUD Act, it can.[135]

One might argue that all the problems foreseen above might be overcome by the periodic compliance review. Adopting this view, Jennifer Daskal defines the review process as "a remarkable and novel development that, for the first time, would enable the United States to track how data obtained by foreign governments is used and thereby protect against abuse."[136] However, even if this system works efficiently, it aims to prevent systemic abuses rather than individual mishaps.[137] Those mishaps, however, might mean violation of the most intimate communications of individuals.

Even if the U.S. government enters into executive agreements only with nations that respect privacy rights, a country's protection of privacy rights can be fleeting — and sometimes those protections flee too quickly.[138] The last decade has seen quasi-democratic countries sliding into authoritarianism and many democratic states taking drastic measures to fight terrorism.[139] This raises many questions regarding the implementation of the executive agreements. The Snowden revelations showed how

---

134. Sharon Bradford Franklin, *Left Out of the Party on Cloud Nine: A Response to Jennifer Daskal*, JUST SECURITY, Feb. 13, 2018, https://www.justsecurity.org/52189/left-party-cloud-nine/ [https://perma.cc/6XZE-2CGL].

135. One might wonder how a piece of U.S. legislation could prevent such foreign data localization efforts. This would be through the requirements of the CLOUD Act for an executive agreement. The CLOUD Act sets out the fundamental principles that the executive agreements will incorporate. Executive agreements, thus, would incur obligations for the foreign governments to follow. For instance, under the CLOUD Act, executive agreements cannot create an obligation for a company that receives a surveillance request to be capable of decrypting data. 18 U.S.C. § 2523(b)(3) (2018). That is, a prerequisite for any executive agreement is that the Attorney General determines that the negotiated executive agreement does not include such decrypting obligation. In a similar manner, the CLOUD Act could have imposed a comparable prerequisite for encryption backdoors or data localization efforts. That is, in a rather quid pro quo fashion, if a foreign government wished to enjoy the benefits of an executive agreements, it would have to give up on pursuing data localization laws.

136. Daskal & Swire, *supra* note 121.

137. *See* Yonatan L. Moskowitz, *MLATs and the Trusted Nation Club: The Proper Cost of Membership*, 41 YALE J. INT'L L. ONLINE (forthcoming 2018).

138. *See* Jonathan Katz & Torrey Taussig, *An Inconvenient Truth: Addressing Democratic Backsliding Within NATO*, BROOKINGS (July 10, 2018), https://www.brookings.edu/blog/order-from-chaos/2018/07/10/an-inconvenient-truth-addressing-democratic-backsliding-within-nato/ [https://perma.cc/PXV2-B7CG] (noting illiberal tendencies in Turkey, Hungary, and Poland); *see also* The Democracy Project, *Reversing a Crisis of Confidence* (June 2018), https://www.democracyprojectreport.org/sites/default/files/2018-06/FINAL_POLL_REPORT_Democracy_Project_2018_v5.pdf [https://perma.cc/ZJ4V-U2MA].

139. *See generally* Nancy Bermeo, *On Democratic Backsliding*, 27(1) J. DEMOCRACY 5 (2016); ELLEN LUST & DAVID WALDNER, U.S. AGENCY FOR INT'L DEV., *Unwelcome Change: Understanding, Evaluating, and Extending Theories of Democratic Backsliding* (June 11, 2015), http://pdf.usaid.gov/pdf_docs/PBAAD635.pdf [https://perma.cc/FL88-SPKP].

drastic those measures were in the U.S.[140] The U.S. allegedly no longer engages in such surveillance efforts, but what is to stop other nations from enacting similar measures in the face of national emergencies? In such a case, would the DOJ be able to respond quickly and adequately? Moreover, would the DOJ even be aware of such measures if the qualifying foreign government engages in a clandestine surveillance program like PRISM?[141] That is, how could the CLOUD Act's oversight mechanism work if the U.K. or other countries with an executive agreement begin to engage in undisclosed surveillance efforts?[142] More importantly, would international politics allow the U.S. government to respond? Given the frustration of many countries with the current MLAT system,[143] rescinding the executive agreement and forcing a country to reutilize the MLAT process would be a severe punishment and a major signal that the U.S. lacks trust in the other country's human rights standards. Given the possible political repercussions, would the U.S. be able to take such drastic measures against an ally?[144]

---

140. G. Alex Sinha & Aryeh Neier, Human Rights Watch, With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy (July 28, 2014), https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and [https://perma.cc/G4L2-3BKF] (arguing that mass surveillance methods, such as used by the NSA, stifle journalists, lawyers, and ultimately democracy itself); Elizabeth Stoycheff, *Under Surveillance: Examining Facebook 's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93(2) JOURNALISM & MASS COMM. Q. 296, 307 (2016) ("[T]he government's online surveillance programs may threaten the disclosure of minority views and contribute to the reinforcement of majority opinion."); Jameel Jaffer, Eric Posner & Joshua Foust, *Is the N.S.A. Surveillance Threat Real or Imagined?*, N.Y. TIMES (June 9, 2013), https://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined [https://perma.cc/NE86-AFD4] ("The chilling effect of surveillance makes our public debates narrower and more inhibited and our democracy less vital.").

141. In 2013, the Guardian broke the news that the NSA was carrying out a top-secret program called PRISM, which allowed the NSA officials direct access to the systems of many U.S. based Internet giants such as Google, Facebook, and Apple. With this access, the NSA officials could "collect material including search history, the content of emails, file transfers and live chat." Glenn Greenwald & Ewen MacAskill, *NSA PRISM Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/Y4Q7-FQU9].

142. Assume that Google.co.uk signs a confidentiality agreement with the British government to keep certain data requests secret.

143. *See* Jennifer Daskal, *New Bill Would Moot Microsoft Ireland Case — And Much More!*, JUST SECURITY (Feb. 6, 2018), https://www.justsecurity.org/51886/bill-moot-microsoft-ireland-case-more/ [https://perma.cc/DNM2-8JME] ("The [CLOUD Act] also responds to the growing frustration experienced by foreign governments seeking the communications content of foreigners in the investigation of local crime."); Funk, *supra* note 52, at 23 ("Whether through MLATs, letters rogatory, or informal means, the process of obtaining evidence from abroad in criminal and civil cases can be time-consuming and frustrating to all parties involved, including the courts.").

144. *See* Moskowitz, *supra* note 137, at 8 (arguing decision to terminate executive agreement would depend on "1) whether the cumulative, aggregated foreign violations have undermined domestic individuals' constitutional and statutory protections to such an extent that

The following scenario aims to illustrate a potential conflict between privacy and politics. In the aftermath of the Paris attacks in 2015, France entered into a nationwide state of emergency, which was extended until October 2017.[145] On October 3, 2017, the French Parliament enacted a new anti-terrorism law that allows the police to conduct house raids and searches without a warrant or judicial oversight, even at night.[146] According to some human rights advocates, this new law will harm the rights to liberty, security, freedom of assembly, and freedom of religion across the country.[147] Imagine that after the U.S.-U.K. executive agreement, the U.S. enters into another executive agreement with France, and then the French government amends the anti-terrorism law to add a provision allowing the French government to wiretap every foreign citizen that visits France with mere suspicion. Would the U.S. government suspend the executive agreement in light of this new law? If the U.S. suspends the agreement, it might deteriorate U.S.-French relations. On the other hand, the continuation of the agreement would make many U.S. citizens' communications accessible to the French government. Worryingly, this delicate decision would be made solely by the executive branch, which may have a strong interest in continuing the agreement so as to ensure France's support in its own counter terrorism measures.[148]

B. Privacy Problems with Respect to Non-Qualifying Foreign Governments

In order to obtain data stored in the U.S., those countries that do not enjoy the privileged status of a "qualifying foreign government" would have to either initiate the MLAT process or send a letter rogatory. Unfortunately, both options are slow and cumbersome.[149] Legal scholars Jen-

---

further participation in the scheme would be an endorsement of that unconstitutional process, and 2) whether this harm is sufficient to outweigh the benefits the state is seeking" by an executive agreement).

145. *See* Alissa J. Rubin & Elian Peltier, *French Parliament Advances a Sweeping Counter-terrorism Bill*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/world/europe/france-terrorism-law.html [https://perma.cc/NY2J-MQFC].

146. *Id.*

147. Shereena Qazi, *French Parliament Approves New Anti-Terrorism Law*, AL JAZEERA (Oct. 3, 2017), https://www.aljazeera.com/news/2017/10/anti-terrorism-law-boost-security-france-171002073720302.html [https://perma.cc/YTU4-5WP3].

148. Robyn Greene, *Four Common Sense Fixes to the CLOUD Act that Its Sponsors Should Support*, JUST SECURITY (Mar. 13, 2018), https://www.justsecurity.org/53728/common-sense-fixes-cloud-act-sponsors-support/ [https://perma.cc/26J7-8DJ4] ("Since a decision not to certify a country would inherently incur political and diplomatic costs, an AG may be inclined to err on the side of diplomacy at the cost of human rights, and certify a country that does not adequately meet human rights tests.").

149. *See, e.g.*, Daskal & Swire, *supra* note 121 ("There is broad consensus, however, that the current MLA system is slow, cumbersome and in need of updating to handle the growth of online cloud services and the globalization of criminal evidence.").

nifer Daskal and Peter Swire denounce the current MLAT structure and praise the CLOUD Act by noting:

> Foreign governments have become increasingly frustrated by the MLA[T] system, which they see as an imperialist attempt to insist that foreign governments obtain a warrant issued by a U.S. judge even for data needed in the investigation of local crimes. As a result, these governments are actively seeking ways to bypass the MLA[T] system.[150]

These authors note a very valid concern. However, the CLOUD Act system does not solve the slowness or cumbersomeness of the MLAT process for many foreign countries.[151] If the Attorney General actually considers the factors stated in § 2523(b)(1)(B), only few countries will "qualify".[152] Thus, the CLOUD Act will likely privilege Western democracies and leave the majority of countries in the MLAT world. As Daskal and Swire acknowledge, countries with poor human rights records will have to look for their own paths to access data stored by U.S. based companies.[153] For example, such countries might attempt to adopt data localization laws to convince or coerce ICT companies.[154] Once data is local, the only limit on a government's access will be its own domestic law. Given that the CLOUD Act is silent as to the MLAT world, it would leave countries with poor human rights records on their own.

The CLOUD Act does not include any provision preventing data localization or encryption requirement laws.[155] Therefore once operating in a country, the ICT company must comply with the domestic laws therein, even if they conflict with the U.S. standards. Even if the ICT company

---

150. *Id.*

151. Mailyn Fidler, *MLAT Reform: Some Thoughts From Civil Society*, LAWFARE (Sept. 11, 2015), https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society [https://perma.cc/J2MM-S8KK] ("Swire & Hemmings suggest expedited access for countries with a demonstrated history of meeting U.S. legal standards, akin to qualifying for the U.S. visa waiver program . . . However, many countries that would fit this category already enjoy the fastest processing times."); *see also* WOODS, *supra* note 4, at 6–7.

152. Only those countries whose domestic law "afford[s] robust substantive and procedural protections for privacy and civil liberties" will be eligible to conclude an executive agreement with the U.S. 18 U.S.C. § 2523(b)(1)(B) (2018).

153. Daskal, *supra* note 14 ("Frustrated foreign governments are being incentivized to seek alternative means of accessing such data — via ether [sic] data localization laws that ensure local access or reliance on other surreptitious means of accessing data.").

154. Moskowitz, *supra* note 137, at 7–8 (noting that granting privileged access to certain "Trusted Nations" would not "actually address the MLAT requests that are the most problematic: those issued by states with little familiarity with our legal system, and who might respond to continued MLAT failure by forcing data relocation to their countries").

155. Franklin, *supra* note 134.

values the users' privacy, it might still succumb to the foreign governments' measures that are not in line with human rights standards due to business needs. One example of such submission is Apple's recent concessions to the Chinese government to avoid exclusion from the Chinese market. In 2018, Apple formally transferred its Chinese iCloud operations to a local firm in southern China called Guizhou Cloud Big Data (GCBD), which is known for its close ties to the Chinese government and the Communist Party.[156] Apple began hosting its iCloud encryption keys in China and gave access to GCBD so as to obey the Chinese government's data access requests.[157] This decision was in stark contrast to Apple's actions in 2016 when it refused to build a decryption system requested by the FBI that would help unlock an iPhone by stating:

> Once created, the [backdoor] technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.[158]

Despite its earlier stance, Apple chose to hand over the keys to the Chinese government. As legal scholar Vivek Krishnamurthy wrote, data localization efforts "threaten to fragment cloud computing services — and the global Internet more generally — along national lines, with serious implications for the free exchange of ideas and information, the efficient operation of the Internet, and for human rights, too — especially when the governments doing the localizing are not all that rights-respecting."[159]

Thus, the CLOUD Act seems to offer only two bad scenarios for data privacy. In the first scenario, the Attorney General will certify countries with both good and bad human rights records.[160] China, Turkey, Russia, and the members of the European Union, including Poland and Hungary, would thus all have direct and unlimited access to their citizens' data stored by U.S.-based technology giants. In this scenario, the U.S. would potentially be enabling some countries to persecute political

---

156. Shannon Liao, *Apple Officially Moves Its Chinese iCloud Operations and Encryption Keys to China*, VERGE (Feb. 28, 2018), https://www.theverge.com/2018/2/28/17055088/apple-chinese-icloud-accounts-government-privacy-speed [https://perma.cc/CVF3-QX9R].

157. *Id.*

158. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter/ [https://perma.cc/C6T4-853Q].

159. Krishnamurthy, *supra* note 68, at 9.

160. *See* WOODS, *supra* note 4, at 16.

dissidents. In the second scenario, the Attorney General only certifies countries with strong human rights records, such as those ranked as "Free" in the Freedom House Index. This means most Western democracies and some Commonwealth countries would enjoy the privilege of being a qualified foreign government, while countries like China, Russia, and Turkey would turn to forcing U.S.-based ICTs to localize data. As discussed above, once data is localized, these countries will enjoy direct and unlimited access to their citizen's data. In this scenario, the U.S., the champion of the free Internet and freedom of speech, stands idle while U.S.-based companies succumb to data localization requirements and many people are persecuted for their political opinions.

C. Privacy Problems from Foreign Countries' Perspectives

In the oral arguments of the *Microsoft Ireland* case, Justice Ginsburg asked Microsoft's counsel why Microsoft filed a motion to quash the warrant for this particular case although it was complying with similar orders before 2013.[161] Mr. Rosenkranz, Microsoft's lawyer, argued that their objection was delayed due to the novelty of cloud computing. Allegedly, Microsoft only started using cloud computing in 2010, and it took them a while to understand that there was an extraterritorial component of retrieving data from the cloud.[162] Coincidentally, however, the Snowden revelations took place in 2013, and many U.S. companies faced pressure from foreign governments to limit U.S. access to the data the companies hold.[163]

In the post-Snowden world, U.S. technology companies have been trying various ways to ensure data privacy abroad. For example, Microsoft created a data trustee system, and Apple strengthened its encryption efforts.[164] Many others signed privacy contracts with "foreign customers[,] promising not to share data with other governments."[165] The CLOUD Act not only moots *Microsoft Ireland* but also moots these efforts. Regardless of where data is located, as long as a U.S.-based company owns it, the U.S. government will be able to access it.[166] How-

161. Transcript of Oral Argument at 33, United States v. Microsoft Corporation, 138 S. Ct. 1186 (2018) (No. 17-2).

162. *Id.*

163. *See* Paul M. Schwartz, *Microsoft, Ireland and a Level Playing Field for U.S. Cloud Companies*, BLOOMBERG BNA (Aug. 3, 2016), https://www.bna.com/microsoft-ireland-level-n73014445770/ [https://perma.cc/V45Q-F92P].

164. *See id.*

165. Joseph Marks, *Can the US Demand Emails Stored in Ireland?*, POLITICO (Sept. 8, 2015), https://www.politico.eu/article/can-us-demand-emails-stored-in-ireland-cloud-congress-technology-courts-servers-internet-security/ [https://perma.cc/M9NU-C8KB].

166. One might argue that the CLOUD Act will not increase the U.S. government's access to data stored abroad because the U.S. government will not be able to enforce the law in the

ever, due to post-Snowden global politics, "[t]rust — in both American firms and the U.S. government — is simply too low."[167]

By enacting the CLOUD Act, the U.S. government signaled its disregard for this trust problem. The advantage of the CLOUD Act for the U.S. government is clear: the Act prevents ISPs from hiding data from the U.S. government. This advantage actualizes at the expense of foreign citizens' data privacy and the U.S.'s soft-power in cyber-regulation.

By undermining the bilateral nature of the MLATs and creating U.S. exceptionalism, the CLOUD Act will take away the U.S.'s leverage in setting a global standard for cross-border data access. Given that the U.S. hosts the majority of the big ICT companies, it had important leverage in leading the world in cross-border data access. However, instead of seizing this opportunity, the U.S. has pursued isolation and exceptionalism. That is, unless the U.S. enters into an executive agreement with them, those countries with existing MLATs will be forced to go through the slow and burdensome MLAT process. The U.S., on the other hand, will be able to access any data held by U.S.-based companies, even when the data is stored within an MLAT country, without going through the MLAT process. If the U.S. is not following the MLAT procedure for data stored in Country X, Country X will not want to follow the MLAT procedure to obtain data stored in the U.S. and will be skeptical towards new U.S. efforts in cross-border data access as well. Consequently, data localization efforts will ensue.

Data localization may compromise data privacy of foreign citizens for two reasons. First, pooling of data creates an easy target for hackers.[168] Thus, data localization makes user data more accessible not only

---

first place. One might point to the Securities and Exchange Commission's inability to enforce disclosure rules on foreign companies. However, the CLOUD Act is strikingly different from this example, since it targets U.S.-based companies. With virtually all of their assets in the U.S., it is hard to imagine that U.S. companies will refuse to abide by requests by the U.S. government. Thus, I disagree with the structural criticism that the CLOUD Act will not grant more data access to the U.S. In fact, Microsoft's jubilant support for the CLOUD Act shows how willing the tech giant is to perform its duties under the new law. *See* Brad Smith, *Microsoft Statement on the Inclusion of The CLOUD Act in the Omnibus Funding Bill*, MICROSOFT BLOG (Mar. 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/03/21/microsoft-statement-on-the-inclusion-of-the-cloud-act-in-the-omnibus-funding-bill/ [https://perma.cc/QKN2-H5W5] ("Today is an important day for privacy rights around the world, for international relations and for building trust in the technology we all rely on . . . [T]he CLOUD Act . . . is a critical step forward in resolving an issue that has been the subject of litigation for over four years.").

167. Andrew Keane Woods, *Symposium: Whatever Happens in US v. Microsoft, Three Themes Will Persist*, SCOTUSBLOG (Feb. 8, 2018), http://www.scotusblog.com/2018/02/symposium-whatever-happens-us-v-microsoft-three-themes-will-persist/ [https://perma.cc/L69V-4Q4C].

168. Anupam Chander and Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 719 (2015) ("First, localized data servers reduce the opportunity to distribute information across multiple

to the government but also to other individuals using illegal means. Second, as legal scholar Tatevik Sargsyan argues, with data localization, a government's ability to "manipulate and control" citizens' communications via legal means increases.[169] Sargsyan explains the disadvantages of such "stronger legal claim[s] over data" by noting:

> Overall, centralized management of data will also increase human rights risks, especially in countries that lack strong legal systems. Without data storage and data transfer restrictions, information intermediaries are able to provide important platforms for free expression. However, having local operations will make these companies more vulnerable to censorship and surveillance demands, and will make information accessible to authorities for illegitimate reasons, risking the safety and privacy of minority groups, journalists, and activists.[170]

In addition, the U.S. will have virtually unlimited access to foreign citizens' data. Foreign citizens do not enjoy Fourth Amendment and SCA protections.[171] The CLOUD Act, however, grants the U.S. government access to data held by U.S.-based ICT companies. That is, the U.S. could obtain the emails of two foreign citizens without establishing probable cause or going through the MLAT process.

Following the Snowden revelations, many countries enacted data localization laws in order to prevent this access.[172] However, to the frustration of foreign governments, even data localization will not suffice in

---

servers in different locations. As we have noted above, the information gathered together in one place offers a tempting jackpot, an ideal target for criminals.").

169. *See* Tatevik Sargsyan, *Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security*, 10 INT'L. J. COMM. 2221, 2226 (2016).

170. *Id.* at 2229.

171. The Supreme Court held that the Fourth Amendment does not apply to "the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country." United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990). Thus, United States officials may "undertake illegal measures in foreign countries for the purpose of obtaining evidence, without being required to articulate a probable cause behind their search or seizure." C. Gane & M. Mackarel, *The Admissibility of Evidence Obtained from Abroad into Criminal Proceedings — The Interpretation of Mutual Legal Assistance Treaties and Use of Evidence Irregularly Obtained*, 4 EUR. J. CRIME CRIM. L. & CRIM. JUST. 98, 109 (1996). However, in *United States v. Truong Dinh Hung*, the Fourth Circuit noted that the primary purpose of a warrantless search must be for foreign intelligence. 629 F.2d 908, 913 (4th Cir. 1980).

172. Jonah Force Hill, *The Growth of Data Localization Post-Snowden* (Lawfare Research Paper Series), LAWFARE (July 21, 2014), https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf [https://perma.cc/HPM9-42XF] ("Today, more than a dozen countries, both developed and developing, have introduced or are actively contemplating introducing data localization laws.").

keeping their citizens' data from the U.S. government's reach. Thus, as long as U.S. companies dominate Internet services, there is no way for a country to keep its citizens' data from the U.S. government.

Qualifying foreign governments will also have virtually unlimited access to the data stored by the U.S. government. While the CLOUD Act prohibits access to the data of U.S. citizens, it is silent on other citizenships. Thus, qualifying foreign governments can retrieve data regarding citizens of other countries. As stated before, the only limitation on this access would be the country's own domestic law, which may not amount to much protection.[173]

Not only will the CLOUD Act significantly undermine the digital privacy of foreign citizens, it might also damage the global economy through pressuring the use of cloud computing. Frustration with the MLAT process will most likely accelerate data localization efforts, which have two main negative impacts on global economy. First, data localization prevents companies from reaping the benefits of cloud computing.[174] Data security is much less expensive with cloud computing since data is stored on the cloud rather than the computer's hard-drive.[175]

Moreover, since data is dispersed among several data centers in cloud computing, "if a data center is breached or destroyed in a natural disaster, the information itself is not compromised."[176] Cloud computing also adds an additional layer of data security by "obfuscating" data such that it is impossible to read data.[177] Data localization laws, however, require storing all data within the legislating country. This prevents companies from taking "advantage of the Internet's distributed infrastructure and [using] sharding and obfuscation on a global scale."[178]

Scholars such as Thomas F. Brier, Jr. argue that data localization may be detrimental to technological innovation as well.[179] For instance, according to Brier, technologies that rely on cloud computing, such as internet of things devices, would have to utilize "expensive and cumbersome national infrastructures," a dependence that may "erode[] the

---

173. *See* Fischer, *supra* note 96 ("[B]ecause U.S.-based companies host and carry much of the world's Internet traffic, a foreign country that enters one of these executive agreements with the U.S. to could [sic] potentially wiretap people located anywhere on the globe . . . without the procedural safeguards of U.S. law . . . .").

174. Patrick S. Ryan et al., *When the Cloud Goes Local: The Global Problem with Data Localization*, COMPUTER, Dec. 2013, at 54.

175. *Id.* at 56.

176. *Id.*

177. *Id.*

178. *Id.* at 57.

179. Thomas F. Brier, Jr., *Defining the Limits of Governmental Access to Personal Data Stored in the Cloud: An Analysis and Critique of Microsoft Ireland*, 7 J. INFO. POL'Y. 327, 360 (2017).

promise" of the internet of things.[180] That is, when companies cannot utilize cloud computing due to data localization laws, all other areas that rely on cloud computing to flourish will similarly be harmed.

V. AN ALTERNATIVE ROUTE FOR PRIVACY AND DATA ACCESS: A MULTILATERAL TREATY

The MLAT process is under immense pressure due to the increased number of governmental requests.[181] The CLOUD Act does not solve this problem. Instead, it simply carves out an exception for the U.S. government and potentially a few Western democracies. Moreover, it significantly undermines the privacy of citizens all around the world. While data localization efforts by foreign governments will solve the slowness of the MLAT process, they will create their own privacy problems.

Thus, in the aftermath of the CLOUD Act, the global arena is in dire need of a new framework that would ensure both a quicker process than an MLAT and a less intrusive system than the CLOUD Act. Accordingly, a true global standard that would incorporate not just the U.S.'s, but multiple stakeholders' interests can only be reached through a multilateral treaty.

A multilateral treaty has certain advantages that neither MLATs nor the CLOUD Act offer. By providing a public multi-stakeholder dialogue, a treaty would ensure that data privacy of citizens from different countries will be taken into consideration.[182] Moreover, a multilateral treaty would solve possible conflicts of laws regarding the production of data to foreign governments. ICT companies have to maneuver around a "growing, international patchwork of conflicting legal prohibitions and compulsions relating to surveillance."[183] The CLOUD Act will similarly conflict with foreign domestic legislation that prohibits ICT companies from sharing data with the U.S. In such a scenario, an ICT company finds itself between a rock and a hard place: sharing data with the U.S. might lead to sanctions within the foreign country, while not sharing data with the U.S. will lead to sanctions at home. Thus, a multilateral treaty

---

180. *Id.*

181. Lin & Fidler, *supra* note 5, at 4 ("As the demand for electronic evidence has grown and with an increasing amount of user data being stored remotely on company servers, the number of MLAT requests has burdened the original MLAT architecture, rendering it outdated and inefficient.").

182. *See* WOODS, *supra* note 4, at 16.

183. David Kris, *Preliminary Thoughts on Cross-Border Data Requests*, LAWFARE (Sept. 28, 2015, 9:00 AM), https://www.lawfareblog.com/preliminary-thoughts-cross-border-data-requests [https://perma.cc/FK5W-DJ79]; *see also* Daskal, *supra* note 14 ("The blocking provisions also generate conflicts of laws if a foreign government demands data that US law prohibits companies from turning over; US executives have been detained for failing to turn over data that US law prohibits them from disclosing.").

would ensure that countries overcome these conflicts of laws by adopting a single streamlined process. Another advantage of a treaty for U.S.-based ICT companies would be an increase in their perceived trustworthiness in foreign countries. If all countries, including the U.S., have to go through the same international process to obtain data, foreign customers all around the world would not have to fear that their data is under the U.S. government's surveillance.[184]

A multilateral treaty might also better distribute the burden of processing data requests. The majority of government requests are processed by a few countries, and mostly by the U.S.[185] While foreign countries would benefit from a better-resourced DOJ, which would shorten the MLAT process, the U.S. would bear the cost. However, a treaty could create an efficient system to alleviate the burden on the U.S. by requiring member states to contribute to a common fund. This common fund would be an additional resource for those countries that are most burdened by MLAT requests. Outsourcing the cost of processing MLAT requests would benefit the U.S., while a more efficient DOJ that processes requests in a shorter time period would benefit other countries.

Although a treaty would protect and promote the interests of all parties within the MLAT system, treaty-making is costly and time consuming.[186] Moreover, some countries are content with the status quo. If a country is not concerned about the U.S. government's access to its citizens' data, the CLOUD Act does not pose a great concern to them. In fact, data localization might be easier for many countries since these governments would not have to abide by international standards or respond to global criticism. Thus, many countries will not show the political will to enter into a treaty that would require them to create and abide by an international standard.[187] Yet, when the need for a streamlined

184. Kris, *supra* note 183 ("For the U.S. providers, international agreements . . . could also reduce the perception, among European customers, that data stored with U.S. providers is especially vulnerable to governmental surveillance.").

185. WOODS, *supra* note 4, at 16 ("This is especially important because of the nature of today's Internet services: the majority of government requests for users data are processed by a few countries that struggle to meet the demand.").

186. *See id.*

187. The absence of treaties on cybersecurity, non-proliferation of weapons of mass destruction, or state recognition illustrates the difficulty of adopting a treaty when countries have countervailing interests. *See* Andrew Keane Woods, *Procedural Options for Improving Cross-Border Requests for Data*, LAWFARE (Oct. 13, 2015, 7:58 AM), https://www.lawfareblog.com/procedural-options-improving-cross-border-requests-data [https://perma.cc/HN5K-2MVC] ("Forging an international agreement that satisfies India, China, Brazil, Russia, and the US will likely be so watered down, it would have little utility; in fact, there is a serious risk that the resulting agreement would lead to an erosion of privacy rights, not an enhancement.").

process is dire, countries with divergent interests have successfully drafted and implemented treaties.[188]

With these caveats in mind, by setting a uniform procedural and/or substantive system, a multilateral treaty is the best alternative to solve the current cross-border data access crisis without undermining citizens' digital privacy. Importantly, such a treaty might require certain countries to expand their working force for processing data requests and divide the resulting cost for such expansion. Doubling up the number of workers and resources of the DOJ's Office of International Affairs, the body responsible for processing data access requests, would certainly expedite the cross-border data access process and simplify the process by setting a uniform request process applicable to all member states.189 Due to the gatekeeping functions of the judges, such a treaty would also protect the privacy of both U.S. and foreign citizens.

In this regard, the Council of Europe's Cybercrime Convention is both a success story and a cautionary tale. The Convention on Cybercrime (also referred as the Budapest Convention) is a multilateral treaty with 61 states parties, including the United States, Canada, and Japan.[190] Among other provisions, the Convention requires states parties to criminalize certain conducts such as illegal access and interception, data and system interference, misuse of devices, forgery, fraud, child pornography, and intellectual property offenses and adopt laws that would facilitate international cooperation on cybercrime and electronic evidence.[191] However, the vague terms of the Convention and the lack of limitations on states parties' reservation allowed some states parties not to take on

188. With 159 parties, the New York Convention has been described as the most successful international document so far in unified international sales law. *See* BRUNO ZELLER, CISG AND THE UNIFICATION OF INT'L TRADE LAW 94 (1st ed. 2007). As for substantive law, The Convention on the International Sale of Goods created a uniform substantive law that applies to transactions between parties from different countries. *See* Anthony S. Winer, *The CISG Convention and Thomas Franck's Theory of Legitimacy*, 19 NW. J. INT'L L. & BUS. 1, 2 (1998).

189. Commentators agree that more funding to the DOJ would solve the slowness of the MLAT process. *See, e.g.*, Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SEC. J. ONLINE (Jan. 28, 2015, 1:05 PM), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/ [https://perma.cc/R2DZ-C7KT]; Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687, 689 (2017); WOODS, *supra* note 4, at 10.

190. *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/185/signatures [https://perma.cc/YK4L-FZVN].

191. JACK GOLDSMITH, HOOVER INST., CYBERSECURITY TREATIES: A SKEPTICAL VIEW 3 (2011), http://media.hoover.org/sites/default/files/documents/FutureChallengesGoldsmith.pdf [https://perma.cc/CBB9-8PKZ].

new obligations under the treaty.[192] Moreover, despite a few exceptions, the Convention is predominantly European.[193] Yet, many commentators also praise the Convention, as it is a functioning treaty with increasing membership and a common international framework.[194]

Aspiring to further this success, the parties to the Budapest Convention agreed to adopt a protocol to "help law enforcement secure evidence on servers in foreign, multiple or unknown jurisdictions."[195] However, the fact that the Council of Europe is considering adopting a protocol that would bypass the existing MLATs and grant greater direct access to the countries party to the Convention of Cybercrime is worrisome.[196] This would not solve but rather exacerbate problems that would result from the CLOUD Act. Moreover, despite the increasing membership to the Convention, only half of those states agreed to adopt the first Additional Protocol to the Convention.[197] Thus, it is unclear whether the new Additional Protocol could rise to become an internationally accepted treaty. However, the contents and exact contours of a multilateral treaty that can achieve this goal are beyond the scope of this Note.

---

192. *Id.* ("The Cybercrime Convention is widely viewed as unsuccessful. It achieved "consensus" on computer crimes only by adopting vague definitions that are subject to different interpretations by different states.").

193. Kristen E. Eichensehr, *Data Extraterritoriality*, 95 TEX. L. REV. 145, 157 (2017) ("Although its membership is open to States beyond the Council of Europe, its 53 states parties are overwhelmingly European and Western, with a few outliers like Japan, Israel, Senegal, and Sri Lanka.").

194. Alexander Seger, *Enhanced Cooperation on Cybercrime: a Case for a Protocol to the Budapest Convention*, ISPI (July 16, 2018), https://www.ispionline.it/en/pubblicazione/enhanced-cooperation-cybercrime-case-protocol-budapest-convention-20964 [https://perma.cc/6PCP-XNBE] ("[Cybercrime Convention] has become the global standard in this field . . . More than 160 States had cooperated with the Council of Europe in capacity building activities on the basis of the Budapest Convention, and many of them are likely to join this treaty sooner or later.").

195. T-CY News, *Cybercrime: Towards a Protocol on Evidence in the Cloud* (June 8, 2017), https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud [https://perma.cc/SA4C-7A65].

196. ACCESS NOW, ACCESS NOW KEY RECOMMENDATIONS ON THE COMMISSION'S TECHNICAL DOCUMENT MEASURES TO IMPROVE CROSS-BORDER CCCESS TO ELECTRONIC EVIDENCE FOR CRIMINAL INVESTIGATIONS FOLLOWING THE CONCLUSIONS OF THE COUNCIL OF THE EUROPEAN UNION ON IMPROVING CRIMINAL JUSTICE IN CYBERSPACE 4 (2017), https://www.accessnow.org/cms/assets/uploads/2017/06/AN_response_to_Commission_on_e-evidence_June2017.pdf [https://perma.cc/JW2J-HC7Q] ("Access Now is seeing governments look to non-MLAT bilateral or multilateral options to bypass the MLAT process. For instance, the Council of Europe is in the early stages of negotiations to grant greater direct access to the countries party to the Convention of Cybercrime.").

197. CCDCOE, *Council of Europe Ponders a New Treaty on Cloud Evidence*, (June 28, 2017), https://ccdcoe.org/council-europe-ponders-new-treaty-cloud-evidence.html [https://perma.cc/EP9M-G46G] ("The Convention, which was originally drafted by the Council of Europe member states and the US and Canada, currently has a total of 55 ratifications and accessions worldwide, while the 1st Additional Protocol has only 29.").

VI. CONCLUSION

The U.S. has always championed the ideas of "Internet freedom" and free speech. The CLOUD Act threatens both. This system not only risks the privacy of U.S. citizens by allowing unlimited access to qualifying foreign governments, but also threatens the privacy of foreign citizens since the U.S., their own country, and qualifying foreign governments will gain access to their data. As long as the data is stored by a U.S.-based company, the U.S. government can obtain the data through a § 2703(d) order or a warrant. However, the U.S. government loses its negotiating power in the international arena and lets other states reign free. This system thus puts national barriers on the Internet and free speech. Put differently, the U.S. gains access to data held by U.S.-based companies but loses a great deal of soft power and risks the privacy of many. To prevent such a gloomy scenario, governments around the world should enter into negotiations regarding a multilateral treaty that sets a global standard for cross-border data access. This new multilateral treaty would not only overcome the slowness of the MLAT system, but would also limit the overbroad access of the CLOUD Act.