LEGAL ACCESS TO THE GLOBAL CLOUD

*Paul M. Schwartz**

Increased use of the cloud and its international scope raise significant challenges to traditional legal authorities that permit access to data stored outside the United States. The resulting stakes are high. This area of law affects a wide range of important matters concerning law enforcement, national security, and civil litigation.

Up until now, however, policymakers in this area have failed to fully appreciate the technological distinctions between different types of data clouds. This Article develops and distinguishes between three models of cloud computing to provide greater clarity for courts when evaluating international data access requests. These models are the Data Shard, Data Localization, and Data Trust clouds. This new typology reveals how the same legal authority will lead to notably different results in data access cases depending on the technical architecture of the cloud network. To illustrate, this Article assesses the likely results for each type of cloud under the full range of American legal authorities that permit parties to seek digital information held abroad—namely, the Fourth Amendment, the Stored Communications Act, Mutual Legal Assistance Treaties, administrative or grand jury subpoenas, and the Foreign Intelligence Surveillance Act.

This Article's analysis of cloud models also points to the profound instability of current American data access rules. The writing is on the wall. Companies and individuals outside of the United States now have multiple ways, including changing their cloud management models, to shelter data beyond the exclusive reach of U.S. law, which will increase the importance of non-U.S. access rules. This trend will spell the end of unilateral decisionmaking by U.S. courts concerning the legal process to be applied when the government or civil litigants seek data stored extraterritorially.

In response, this Article advances two principles for a world of omnipresent global cloud computing. First, U.S. law should treat extraterritorial data requests equally, regardless of the location of the cloud provider's headquarters. This legal approach would foster a level playing field for global cloud companies and encourage innovation, rather than further balkanization of the internet. Second, there is a need for

---

* Jefferson E. Peyser Professor of Law at University of California, Berkeley School of Law; Co-Director, Berkeley Center for Law & Technology. I would like to thank James X. Dempsey, Stavros Gadinis, Mark Gergen, Brittany Johnson, Sonya Katyal, Orin Kerr, Annie Lee, Katerina Linos, William M. Treanor, Karl-Nikolaus Peifer, Tory D. Roberts, Peter Swire, and Ian Waldron for their helpful comments and suggestions on earlier drafts. I also thank the Berkeley Center for Law & Technology, Microsoft, and the Fritz Thyssen Foundation for their research support.

international cooperation to create reciprocity. The "Pax Americana" of unilateral U.S. governance in this area is ending, and the wisest course for U.S. policy is to establish new international agreements for global data access. As this Article details, the CLOUD Act of 2018 takes a major step toward incorporation of these principles in an effort to preserve the internet as a global space. But the Act also encourages a know-your-customer regime, where the ultimate cost may be paid in users' privacy.

INTRODUCTION

Cloud computing is one of the fastest-growing areas of information technology. Data are moving from our personal devices, such as laptops and phones, and onto different configurations of remotely managed servers. These servers can be networked throughout the world. The increased use of the cloud and its international scope raise significant challenges to

traditional legal authorities that permit access to data stored outside the United States.

The resulting stakes are high. This area of law concerns the legal process to be applied when the U.S. government or civil litigants seek the world's cloud data. It affects a wide range of important matters concerning law enforcement, national security, and civil litigation. U.S. law enforcement is worried about the risk of "going dark," a condition in which it cannot obtain access to stored and transmitted information.[1] International privacy advocates are concerned that U.S. laws may permit excessive access to global cloud data services provided by U.S.-based companies.[2] Internet scholars are raising the alarm about a balkanization of the web due to country-by-country data localization instead of a globally networked internet.[3] Finally, leading American tech companies are afraid that U.S. law will cause foreign customers to abandon their cloud services and products.[4]

Unfortunately, policymakers in this area have long proceeded with a double form of tunnel vision. The first shortcoming is that much legal analysis in this area is siloed; it looks at only one U.S. access authority at a time. Currently, much attention is devoted to the Stored Communications Act (SCA).[5] This statute requires the government to obtain a warrant or court order to access specified customer data held by internet service providers.[6] In a dramatic turn of events regarding this statute, the highly contested case of *United States v. Microsoft Corp.* reached the Supreme Court,[7] only to be mooted when Congress swiftly enacted the CLOUD

---

1. Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary, 115th Cong. 5–6 (2017) (statement of Christopher A. Wray, Director, FBI).

2. For a discussion, see Paul M. Schwartz & Karl-Nikolaus Peifer, Transatlantic Data Privacy Law, 106 Geo. L.J. 115, 118–19 (2017) [hereinafter Schwartz & Peifer, Transatlantic Data Privacy].

3. See Jennifer Daskal, Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues, 8 J. Nat'l Sec. L. & Pol'y 473, 474–75 (2016) [hereinafter Daskal, Law Enforcement Access]; Peter Swire & DeBrae Kennedy-Mayo, How Both the EU and the U.S. Are "Stricter" than Each Other for the Privacy of Government Requests for Information, 66 Emory L.J. 617, 662 (2017); Andrew Keane Woods, Against Data Exceptionalism, 68 Stan. L. Rev. 729, 752–53 (2016).

4. For different perspectives on this concern, see Clint Boulton, NSA's Prism Could Cost IT Service Market $180 Billion, Wall St. J.: CIO Journal (Aug. 16, 2013), https://blogs.wsj.com/cio/2013/08/16/nsas-prism-could-cost-it-service-market-180-billion/ (on file with the *Columbia Law Review*); Ian Traynor, European Firms 'Could Quit US Internet Providers over NSA Scandal,' Guardian (July 4, 2013), https://www.theguardian.com/world/2013/jul/04/european-us-internet-providers-nsa [https://perma.cc/T9QP-BZ3R].

5. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).

6. See id. § 2703.

7. 138 S. Ct. 356 (2017), granting cert. to In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. (*Microsoft Ireland*), 829 F.3d 197 (2d Cir. 2016).

Act of 2018.[8] This Act settled the question of the international reach of a single U.S. legal statute: It makes clear that SCA warrants have an extraterritorial reach. At the same time, however, the CLOUD Act represents a potential decisive break with the past siloed approach—at least regarding law enforcement access to the cloud. It opens the door to the establishment of new rules for government-to-government access to data. Once adopted, these new executive agreements will allow foreign governments to make direct data requests to U.S. cloud providers. This major turn can only be understood, however, as part of an assessment of the full range of extraterritorial access rules. This Article carries out this task.

The second form of tunnel vision is that much legal analysis ignores the kind of cloud in which data are stored. This shortcoming is highly problematic because different types of clouds raise distinct legal issues.[9] Sound legal policy in this area depends on an awareness of the underlying management model of a cloud network. All clouds are not created equal, especially when it comes to where and how they store information, and how they permit access to it.[10]

This Article corrects the law's tunnel vision about cloud computing. This correction leads to a weighty conclusion: The long-standing "Pax Americana" for data access rules is ending.[11] The old system was one of unilateral reliance by the United States on its own rules for extraterritorial access. Today, there are efficient technological end-runs available for the rest of the world that permit non-U.S. cloud customers to avoid U.S. rules for data stored outside the United States.[12] This Article demonstrates the grounds for the weakening and future collapse of the current Pax Americana for data access rules.

The Article then develops two primary principles for constructing a new legal order for a world of omnipresent cloud computing and assesses the CLOUD Act in light of these policy propositions. First, the United States should treat extraterritorial clouds equally, regardless of the nationality of the corporate provider.[13] Any other approach would hasten internet balkanization and encourage non-U.S. customers to favor cloud providers that are not headquartered in the United States. Such a development would be counterproductive; it would reduce access to global clouds by U.S. law enforcement, national security agencies, and civil litigants. Second, U.S. access rules should be supplemented by development

8. CLOUD Act, H.R. 1625, 115th Cong. div. V (2018).

9. See infra Part II.

10. See infra Part II.

11. On the past reliance on U.S. decisionmaking for internet governance, which this Article calls "Pax Americana" for the internet, see Jack Goldsmith & Tim Wu, Who Controls the Internet? 13–46 (2006).

12. See infra Part II.

13. See infra section III.B.1.

of new international agreements concerning extraterritorial data access.[14] These agreements should first be negotiated with individual nations whose legal rules concerning access to cloud information are closest to those of the United States.

This Article proceeds in three parts. It first explores the siloed and fragmented nature of current legal analysis in this area. It does so through analysis of two cases concerning the global reach of warrants under the SCA. The pedagogical value of these cases remains undiminished by the CLOUD Act. The first case, *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.* (*Microsoft Ireland*), is the Second Circuit decision that upheld territorial limits to SCA warrants but was ultimately dismissed by the Supreme Court.[15] The second case, *In re Search Warrant No. 16-960-M-01 to Google* (*Google Pennsylvania*), came to a result contrary to the circuit decision of *Microsoft Ireland*.[16] *Google Pennsylvania* is one of a series of important judicial decisions reaching the same conclusion for clouds run by Google; these judgments found that the SCA extends to extraterritorial clouds.[17] While *Microsoft Ireland* and *Google Pennsylvania* have polar opposite outcomes, they reflect the same basic limitation: Both cases are based on a flawed understanding of the critical technology before the courts. *Microsoft Ireland* and *Google Pennsylvania* concern different underlying cloud models, which raise distinct legal and policy issues. Yet, these cases and the leading scholarship concerning global access to networked data fail to engage with important distinctions among cloud technologies.[18]

---

14. See infra section III.B.2.

15. See United States v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018) (per curiam) (vacating and remanding *Microsoft Ireland* with instructions to dismiss as moot). For the path to the Supreme Court for this case, see *Microsoft Ireland*, 829 F.3d 197 (2d Cir. 2016), reh'g denied, 855 F.3d 53 (2d Cir. 2017); see also In re Info. Associated with One Yahoo Email Address that Is Stored at Premises Controlled by Yahoo, Nos. 17-M-1234, 17-M-1235, 2017 WL 706307, at *2–3 (E.D. Wis. Feb. 21, 2017) (adopting the reasoning of the four judges who dissented from the Second Circuit's denial of rehearing en banc, such that it would be a permissible domestic application of the SCA to enforce the warrants at issue).

16. See 232 F. Supp. 3d 708, 719–25 (E.D. Pa. 2017) (holding that warrants issued pursuant to the SCA seeking data stored abroad did not violate the presumption against extraterritoriality because any invasion of privacy would occur at the time of the disclosure in the United States).

17. Other cases analyzing the Google cloud have reached the same result as *Google Pennsylvania*. See, e.g., In re Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); In re Search of Info. Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757 (GMH), 2017 WL 2480752, at *11 (D.D.C. June 2, 2017); In re Search of Content that Is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, 2017 WL 1487625, at *4 (N.D. Cal. Apr. 25, 2017).

18. The relevant scholarship engages around issues concerning the future meaning of territoriality for cloud data. Compare Jennifer Daskal, The Un-Territoriality of Data, 125 Yale L.J. 326, 365–78 (2015) [hereinafter Daskal, The Un-Territoriality of Data] (arguing that global telecommunications make territoriality a meaningless concept for deciding data access questions for cloud information), with Woods, supra note 3, at 735

This Article argues for a new approach. Legal decisionmaking about access to global clouds must be grounded in knowledge of how existing clouds differ from one another. Initially, cloud services were U.S.-centric: U.S.-headquartered companies provided cloud services on a global basis but stored data on servers in the United States.[19] U.S. companies quickly moved beyond this U.S.-centric approach, however, and developed globally distributed cloud networks.[20] In reflection of this reality, this Article develops a new taxonomy of cloud services. Defined from the perspective of a U.S.-headquartered company, the three essential models are Data Shard, Data Localization, and Data Trust clouds.[21]

("Contrary to prevailing wisdom, jurisdiction over cloud-based data has nearly everything to do with territoriality—it requires an inquiry into the location of the data, the domicile of the data controller, the location of the crime, the citizenship of the victim, and/or the citizenship of the perpetrator."). For other scholarship that examines the issue of territoriality in the internet age and other issues related to global data access, see generally Damon C. Andrews & John M. Newman, Personal Jurisdiction and Choice of Law in the Cloud, 73 Md. L. Rev. 313, 351–83 (2013) (explaining why the internet model for personal jurisdiction and choice of law does not perfectly address the unique jurisdictional issues posed by cloud computing and advancing workable approaches); David Cole & Federico Fabbrini, Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders, 14 Int'l J. Const. L. 220, 233–37 (2016) (advocating for a transatlantic privacy agreement between the United States and the European Union to safeguard citizens' privacy against overinvasive surveillance across borders); Orin S. Kerr, The Fourth Amendment and the Global Internet, 67 Stan. L. Rev. 285, 285–86 (2015) [hereinafter Kerr, The Fourth Amendment] (noting the territorial nature of Fourth Amendment application and the goal of "adapt[ing] existing principles for the transition from a domestic, physical environment to a global, networked world"); Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 374 (2014) [hereinafter Kerr, Next Generation] (proposing the contours of a "next generation privacy act" in the United States to better address modern low storage costs and delocalized networks); Ned Schultheis, Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry, 9 Brook. J. Corp. Fin. & Com. L. 661, 682–87 (2015) (describing tensions between the European Union, its Member States, and the United States regarding the extraterritorial use of SCA warrants and the need for a system more streamlined than the Mutual Legal Assistance Treaty (MLAT) process); Recent Case, In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014), 128 Harv. L. Rev. 1019, 1026 (2015) (arguing that in the context of SCA warrants, "the location that matters is that of the service provider and not the requested data").

19. Anthony T. Velte et al., Cloud Computing 117 (2010).

20. See Arne Josefsberg, Dublin Data Center Celebrates Grand Opening, Microsoft: TechNet (Sept. 23, 2009), https://blogs.technet.microsoft.com/msdatacenters/2009/09/23/dublin-data-center-celebrates-grand-opening [https://perma.cc/2ZQL-6EJW] (describing the grand opening of Microsoft's first international cloud center in Dublin, Ireland, in 2009); AWS Global Infrastructure, Amazon Web Services, https://aws.amazon.com/about-aws/global-infrastructure [https://perma.cc/QV77-MZT4] (last visited July 26, 2018) (noting that the first U.S. location of Amazon Web Services launched in 2006 with locations following in Ireland in 2007 and Singapore in 2010).

21. See infra section I.B.

To shift the grounds for legal analysis and policy debate, this Article identifies these three models of cloud computing and explores how different judicial results follow once the law understands their implications. A Data Shard cloud is one in which information is "sharded"; it splits data up in a globally dispersed network and keeps them in constant motion among different data centers.[22] A Data Localization cloud stores data outside the United States. It is also typically marketed to customers outside the United States. This approach permits customers to isolate data outside the geographical boundaries of the United States.[23] Finally, a Data Trust cloud is one in which a non-U.S. entity manages the cloud as a trustee for a U.S.-headquartered provider.[24] Through encryption and the law of trusts, the trustee effectively brings such cloud data under its domestic, non-U.S. law.

In Part II, this Article goes beyond the SCA to explore the full range of American legal authorities that permit parties to seek digital information held abroad. Looking at requests by government authorities and private parties, the Article assesses the likely results when information is held in Data Shard, Data Localization, or Data Trust clouds. Using this taxonomy, Part II identifies notable and meaningful differences in likely outcomes when the legal authority is the same, but different cloud management models are involved. This analysis notably pinpoints the grounds for the profound instability of the current U.S. approach. The writing is on the wall; the rest of the world can and will increasingly "route around" U.S. legal access rules by shifting to clouds that increase the importance of non-U.S. law. This trend will spell the end of unilateral decisionmaking by U.S. courts concerning the legal process to be applied when the government or civil litigants seek data stored extraterritorially.

Finally, in its third Part, this Article presents two principles for a new U.S. approach. As a first principle, this Article argues that U.S. law should treat extraterritorial data requests equally, regardless of the location of the cloud provider's headquarters.[25] One benefit of this approach is that it would avoid putting U.S.-based companies in a position in which they have to choose between obeying one but not both sets of legal demands. One legal system may forbid a transfer of data, and the United States may require it. In short, U.S. companies can face conflicting obligations with regard to a single item of data.[26] U.S. law should not create stricter legal standards for the extraterritorial customer data of U.S.-based cloud companies. A legal approach that fosters a level playing field for global cloud

22. See infra section I.B.

23. See infra section I.B.

24. See infra section I.B.

25. See infra section III.B.1.

26. For a discussion of this conflict, see Volkswagen, A.G. v. Valdez, 909 S.W.2d 900, 902 (Tex. 1995) ("[W]hen the laws of the foreign sovereign protect relevant information from discovery, the interests of the domestic court or agency must be balanced with those of the foreign sovereign.").

companies would reward the development of technical expertise, permit the market to select the superior cloud technology, promote the scalability of technology, and help prevent the balkanization of the internet into competing national or regional fiefdoms. The CLOUD Act makes a decisive move in this direction for the SCA, although much depends on how courts will apply the required comity analysis.

The second principle concerns the need for international cooperation around the concept of reciprocity.[27] The United States should develop a series of international agreements on access to global cloud data; the first step should be negotiations with countries that most closely share American values. In a path-breaking step for cooperation in international law enforcement, the CLOUD Act goes far beyond its amendments of the SCA. This law also supplements the current landscape of legal access rules by opening the door for the United States to negotiate separate executive agreements with other nations. The United States and United Kingdom are now developing such a bilateral agreement.[28] Much is open, however, regarding this new statute's impact on global privacy, law enforcement access to cloud data, and a global and interoperable internet. One looming problem is the likely collision between the CLOUD Act and the data protection laws of the European Union, in particular the General Data Protection Regulation (GDPR), which took effect in May 2018. A further conflict will follow from the European Union's preference for a coordinated E.U.–U.S. response concerning international data access, as opposed to the CLOUD Act's approach of authorizing bilateral accords with individual countries.

A final aspect of the law's regulation of the cloud is worth noting: the shift underway to a know-your-customer global regime for the internet. The CLOUD Act creates incentives for providers to be aware of and be able to document the nationality and location of their users. The benefit to the provider will be to make the location of their servers less important. In so doing, this law reduces the significance of data localization for data access requests and thereby promotes the maintenance of a globally interoperable internet. But in encouraging this documentation of the nationality and location of cloud customers, the CLOUD Act moves providers closer to the paradigm in place for U.S. banks and financial service entities, which collect detailed identification information about customers and are even legally required to file reports proactively when their customers engage in suspicious activities.[29]

---

27. See infra section III.B.2.

28. International Conflicts of Law and Their Implications for Cross Border Data Requests by Law Enforcement: Hearing Before the H. Comm. on the Judiciary, 114th Cong. 2–3 (2016) [hereinafter Statement of Rep. Goodlatte] (statement of Rep. Goodlatte, Chairman, H. Comm. on the Judiciary).

29. See 31 C.F.R. § 1020.220 (2017) (requiring banks and other financial institutions to maintain Customer Identification Programs).

I. MODELS OF CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction."[30] To expand on this concise definition, one would begin by noting how the cloud locates computing resources on the internet to make them dynamic and scalable.[31] Such distributed computing permits rapid expansion of data processing to handle a greater load or take on new tasks.[32] Cloud computing also transfers computing responsibilities from one party to another and achieves new efficiencies in computing management.[33] Today, the cloud is ubiquitous. A Pew Foundation poll already predicts a future in which all of us access software and share information through cloud servers rather than personal computers.[34]

Beyond this description, courts in extraterritorial access cases tend to look at other aspects of the cloud. In particular, these courts have focused on where cloud data are *stored*, and how and where companies *access* them. These cases, however, typically examine only a single management model at a time and in incomplete fashion, which has helped to obscure the important variations that exist among cloud networks.

Building on case law and drawing on marketplace developments in global data storage services, this Part develops a three-part model of cloud management. It first demonstrates the need for this model by contrasting two recent cases, *Microsoft Ireland* and *Google Pennsylvania*. In these cases, U.S. law enforcement sought information stored in global clouds. The information demands were made pursuant to the same statute, the SCA, but the two courts reached divergent outcomes. Post–CLOUD Act, these cases remain highly useful as a pedagogical matter. First, these cases reveal how U.S. courts ignore technical differences among different kinds of extraterritorial clouds. These technical differences continue to exist after enactment of the CLOUD Act and they remain highly significant for the kinds of comity analyses that this new statute requires for certain law enforcement requests for extraterritorial

30. NIST Cloud Computing Program—NCCP, Nat'l Inst. of Standards & Tech., https://www.nist.gov/programs-projects/cloud-computing [https://perma.cc/P52N-NGQ3] (last updated Apr. 12, 2018).

31. For an introduction, see Velte et al., supra note 19, at 3–4.

32. See Paul M. Schwartz, Information Privacy in the Cloud, 161 U. Pa. L. Rev. 1623, 1628–32 (2013) (describing the recent "shift in global data access and processing" attending the growth of cloud computing).

33. See id. at 1632–34; see also Velte et al., supra note 19, at 77–78.

34. See Janna Anderson & Lee Rainie, Pew Research Ctr., The Future of Cloud Computing 8 (June 11, 2010), http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing [https://perma.cc/9GEM-6Z29].

data. Second, the technical differences in types of clouds remain important for the many legal authorities beyond the SCA. Hence, *Microsoft Ireland* and *Google Pennsylvania* allow the exploration of legal and technical issues that the enactment of the CLOUD Act leaves unresolved.

This Part then sets out its three cloud models: the Data Shard, Data Localization, and Data Trust clouds. It analyzes how they differ from each other regarding the issues of *location* of cloud data and *access* to the information. Finally, this Part examines the lack of consensus in leading scholarship regarding the meaning and importance of territoriality in cases involving access to networked data.

In light of these three models, this Article builds upon this scholarship to derive a set of four initial lessons. First, the legal significance of where cloud data is accessed versus where it is located—the source of much scholarly debate—cannot be answered without reference to specific cloud models. Beyond *Microsoft Ireland* and *Google Pennsylvania*, however, it is striking how other courts have futilely tried to resolve questions of extraterritorial access to cloud data equipped only with the concepts of access and location. Second, the Data Trust cloud shows how it is possible to divide management of networked information from the ability to access it. This difference has important implications for certain kinds of U.S. access requests. Third, internet balkanization is already occurring and is a trend that has continued post–CLOUD Act. Fourth, cloud technology allows parties outside of the United States to shelter their data in distinct ways, which calls for policymakers to consider the full range of legal authorities and the interaction of law and cloud technology.

A. *Case Law:* Microsoft Ireland *and* Google Pennsylvania

Federal electronic surveillance law for domestic law enforcement consists of three statutes: the Wiretap Act, the Stored Communications Act, and the Pen Register Act.[35] Of these, the SCA is the most relevant to access to cloud information.[36] There are many open questions regarding this statute's applicability to information stored in a cloud located outside the United States. To begin exploring these uncertainties, this Article considers two recent decisions.

In *Microsoft Ireland*, the Second Circuit held that the SCA did not obligate Microsoft to give the government information stored in an extraterritorial data center.[37] After accepting the government's appeal from this decision, the Supreme Court ultimately declared it mooted by the enactment of the CLOUD Act, which, given its extraterritorial reach,

35. For an overview, see Daniel Solove & Paul M. Schwartz, Information Privacy Law 344–53 (6th ed. 2017) [hereinafter Solove & Schwartz, Information Privacy Law].

36. See Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).

37. See 829 F.3d 197, 201 (2d Cir. 2016).

would have obligated Microsoft to give the government that information.[38] Unlike the Second Circuit in *Microsoft Ireland*, the Eastern District of Pennsylvania in *Google Pennsylvania* held that the SCA required a cloud provider to supply the government with information distributed in its global network.[39]

Two cases, two results. There is far more here, however, than this initial snapshot indicates. Beyond the narrow question regarding the extraterritorial reach of the SCA, which the CLOUD Act resolved, there are significant underlying dissimilarities between the clouds involved in these two cases, and those dissimilarities warrant distinct legal consideration.

All clouds are not created equal, and technical differences among them raise legal issues that will persist for future discovery requests post–CLOUD Act, both for the CLOUD Act itself and for other legal authorities beyond that statute. Before examining these differences, it will be valuable to understand two further aspects of cloud computing. First, the cloud represents an extremely lucrative area for U.S. companies to offer services, and second, it raises major concerns for U.S. security agencies and law enforcement agencies. Regarding the importance of this area for business, a multibillion-dollar market exists for the international clouds of U.S. companies. In addition, U.S. law regarding access to personal data strongly affects this market. There has also been a relevant watershed moment in this regard. June 2013 marked the beginning of the revelations from former National Security Agency (NSA) employee Edward Snowden about NSA surveillance and the secret cooperation of many U.S. companies with the government's clandestine activities.[40] In response, many customers of cloud services outside the United States developed newfound interest in using clouds that avoided the territory of the United States. Post-Snowden, Forrester Research estimated that U.S. businesses lost up to $180 billion due to the distrust in some countries toward U.S. tech companies.[41]

In a similarly high-profile fashion, national security agencies and law enforcement in the United States consider this area of law to be one of paramount significance. The storage of information in bits and pieces in cloud networks has the potential to limit their ability to access cloud data,

---

38. See United States v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018) (per curiam) (vacating and remanding *Microsoft Ireland* with instructions to dismiss as moot).

39. See 232 F. Supp. 3d 708, 709 (E.D. Pa. 2017).

40. For a discussion by the European Court of Justice of the Snowden leaks, see Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650. For the Guardian's archive relating to the leaked NSA files, see James Ball et. al, Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security, Guardian (Sept. 6, 2013), https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [https://perma.cc/7535-49VM]; 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/1 [https://perma.cc/9S8E-3WGK].

41. Boulton, supra note 4.

posing a possible catch-22. As Magistrate Judge Thomas J. Rueter observed in *Google Pennsylvania* regarding the kind of cloud at issue in that case: "[N]o one knows which country to ask, and even if specific servers could be identified, the data may no longer be there by the time its location has been identified."[42] In a sense, this issue is a variation of the going dark problem raised by national security and law enforcement agencies in the debate about strong encryption and "back doors." New devices, including iPhones, increasingly rely on encryption, which makes the data unreadable and can preempt these agencies from accessing communications they otherwise have the legal authority to access.[43] Similarly, cloud data stored extraterritorially may evade the ability of governmental officials to use legal authorities to view targeted communications. From their viewpoint, the network has "gone dark."

At this point, a discussion of the hidden dissimilarities between *Google Pennsylvania* and *Microsoft Ireland* is necessary. In particular, these cases illuminate how different models of cloud management can encourage different conclusions regarding the scope of the same legal authority. The lesson is one that extends beyond the SCA and the CLOUD Act. In *Google Pennsylvania*, Magistrate Judge Rueter held that a warrant compelling Google to disclose information was not an extraterritorial application of the SCA.[44] His analysis of the question of extraterritoriality turned on where the *access* to the information would take place.[45] Google argued that the warrants at issue could not compel it to produce records that were stored outside the United States.[46] Functionally, however, Google could only access the extraterritorially stored information through its Legal Investigations Support Team in the United States.[47] Google would then turn the information over to the FBI pursuant to its warrant request, and the agency would review the copies of the data in Pennsylvania.[48] Under the facts of the case, therefore, the judge found

---

42. 232 F. Supp. 3d at 725.

43. See In re Search of an Apple iPhone Seized During Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016) (noting the government's difficulty in accessing data on an iPhone due to the device's encryption). However, the FBI has come under fire for "grossly inflat[ing]" statistics it cited as the most compelling evidence for the need to address going dark: It "claim[ed] investigators were locked out of nearly 7,800 devices connected to crimes last year when the correct number was much smaller, probably between 1,000 and 2,000." Devlin Barrett, FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public, Wash. Post (May 22, 2018), https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html [https://perma.cc/EY7J-AWAB].

44. See 232 F. Supp. 3d at 725.

45. See id.

46. See id. at 710.

47. Id. at 712–13.

48. Id. at 722.

that access depended on the location of the search and the review. He determined that "the searches of the electronic data . . . will occur in the United States when the FBI reviews the copies of the requested data in Pennsylvania."[49] Magistrate Judge Rueter focused on (1) where the data would be retrieved by the cloud provider pursuant to a warrant, and (2) where the data would be given to U.S. law enforcement.[50] The answer to both questions was the same: These activities would take place within the United States.

Conversely, in *Microsoft Ireland*, the Second Circuit focused on the *location* of the sought-after data and held that the SCA did not require Microsoft to give the government information stored in its non-U.S. data center.[51] Writing for the court, Judge Susan L. Carney emphasized that "even messages stored in the 'cloud' have a discernible physical location,"[52] and in Microsoft's case, the relevant information was located at its data center in Dublin, Ireland.[53] In its interpretation of the underlying statute, the appellate court ruled that Congress did not intend for SCA warrants to have a global reach.[54] The matter might not have been clear when the SCA was enacted in 1986, but in enacting the CLOUD Act in 2018, Congress made explicit its wish for these warrants to have such an exterritorial reach.[55]

These cases used different tests: One looked to the issue of data access, the other to data location. The cases cannot be understood, however, without attention to the different underlying cloud management models. *Google Pennsylvania* involved a Data Shard cloud, a type of cloud in which the cloud provider stores information both globally and domestically.[56] It breaks data into small components, or shards, which the system routes around the globe, with different bits shifted between various locations.[57] In contrast, *Microsoft Ireland* involved a Data Localization cloud, a type of cloud in which information is stored extraterritorially.[58] As noted above and discussed further below, a pure Data Localization cloud is one in which the information can be accessed only in the same geographic location as where the data are stored.[59] Yet, the Second Circuit

49. Id.

50. See id. at 721–22.

51. See 829 F.3d 197, 216 (2d Cir. 2016).

52. Id. at 220 n.28.

53. Id. at 209, 220 n.28.

54. See id.

55. See CLOUD Act, H.R. 1625, 115th Cong. div. V, § 102(1)–(2) (2018).

56. See 232 F. Supp. 3d 708, 723 (E.D. Pa. 2017).

57. Id.

58. See 829 F.3d at 220.

59. There is a twist in *Microsoft Ireland*, which is that the precise model at stake was a partial or incomplete one. See id. at 230 (Lynch, J., concurring) (noting that Microsoft stores emails on local servers in Ireland, but that it can also access them from Redmond,

in *Microsoft Ireland* did not consider whether pure Data Localization would raise different issues, or whether and how to assess the partial localization in that case.

A final distinction exists between these two cases. It concerns the practical consequences of a finding of "no access" under the SCA—as constituted pre–CLOUD Act—in *Microsoft Ireland* (the Data Localization cloud), or *Google Pennsylvania* (the Data Shard cloud). In *Microsoft Ireland*, the U.S. government had an important alternative beyond the SCA to access the sought-after information: It could draw on the Mutual Legal Assistance Treaty (MLAT) process.[60] As this Article discusses below,[61] under an MLAT, a public authority can ask for the assistance of the country in which the sought-after data are held, and the request will be processed in the foreign country consistent with the domestic law of that country.[62] In *Google Pennsylvania*, however, Magistrate Judge Rueter was concerned about the absence of any such mechanism.[63] In his opinion, Data Shard clouds emerged as a new dimension of the going dark problem.[64] As discussed below, the CLOUD Act now provides built-in mechanisms, through its comity provisions, that the SCA did not originally allow and that might mitigate some of the need for MLATs.[65] Nonetheless, and as also discussed below, MLATs are likely to remain important.

B. *Data Shards, Data Localization, and Data Trusts*

As discussed above, different technical models for cloud computing are present in the *Google Pennsylvania* and *Microsoft Ireland* cases. Building on these two examples and others, this Article now develops a taxonomy of cloud types. Drawing on existing deployment patterns, it identifies three approaches to cloud management: the Data Shard, Data Localization, and Data Trust models. Each of these technical approaches—which are not typically distinguished under current legal analysis—has distinct implications for how the law should govern access to international cloud data.

Washington). This Article explores the issue of storage of data versus where the data can be accessed below. See infra section I.C.

60. See *Microsoft Ireland*, 829 F.3d at 221.

61. See infra section II.A.3.

62. See generally Peter Swire & Justin D. Hemmings, Mutual Legal Assistance in an Era of Globalized Communications, 71 N.Y.U. Ann. Surv. Am. L. 687 (2016) [hereinafter Swire & Hemmings, Mutual Legal Assistance] (presenting an excellent overview of the MLAT process); World Map, Mutual Legal Assistance Treaties, https://mlat.info [https://perma.cc/R36T-QK74] (last visited July 26, 2018) (providing a graphical representation of, and further details on, the extensive global network of MLATs).

63. See 232 F. Supp. 3d 708, 724 (E.D. Pa. 2017).

64. See id. at 724–25.

65. See infra section III.B.

In the Data Shard cloud, a company stores information in the cloud in multiple international locations.[66] In this dynamic approach, the network itself distributes data to domestic and international servers. A single file can be broken into components and stored in different countries, and intelligence embedded in the network decides where to send and store the data. The network harnesses its own intelligence to create operational efficiencies.[67] As Anupam Chander and Uyên P. Lê observe, "rows of a database are held separately in servers across the world—making each partition a 'shard' that provides enough data for operation."[68] Because data are inherently scattered under this approach, national boundaries are largely irrelevant. The data are sharded according to the logic of the system, and not according to venerable historical lines drawn on a map of the world.[69] Like Richard Wagner's Flying Dutchman, the information located in a Data Shard cloud is constantly in motion. Its only rest occurs when summoned by a company's legal team.

The Google cloud provides a leading example of the Data Shard approach. As the court in *Google Pennsylvania* noted, Google operates a cloud network that "automatically moves data from one location on Google's network to another . . . to optimize for performance, reliability, and other efficiencies."[70] More specifically, the *Google Pennsylvania* court observed that "Google user data . . . is not stored as one single, cohesive digital file; instead, Google stores individual data files in multiple data 'shards,' each separate shard being stored in separate locations around the world."[71] A user's information might be found in the United States as well as on Google servers throughout the world.[72] Moreover, under its Data Shard model, Google can only access information in its cloud from the United States.[73] Hence, it *locates* cloud information in shifting locations throughout the world but *accesses* cloud information exclusively from the United States.[74]

---

66. For a discussion of data sharding, see generally Sikha Bagui & Loi Tang Nguyen, Database Sharding: To Provide Fault Tolerance and Scalability of Big Data on the Cloud, 5 Int'l J. Cloud Applications & Computing 36 (2015); Patrick Ryan & Sarah Falvey, Trust in the Clouds, 28 Computer L. & Security Rev. 513, 520 (2012).

67. Cory Isaacson, Database Sharding: The Key to Database Scalability, Database Trends and Applications (Aug. 14, 2009), http://www.dbta.com/Editorial/Trends-and-Applications/Database-Sharding–The-Key-to-Database-Scalability-55615.aspx [http://perma.cc/9BBH-N4XJ].

68. Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677, 719 (2015).

69. Ryan & Falvey, supra note 66, at 520.

70. 232 F. Supp. 3d 708, 723 (E.D. Pa. 2017).

71. Id. at 724.

72. Id. at 712–13.

73. Id.

74. Id.

In Data Localization, the second model, a company stores information in a cloud that is restricted to a single country or region.[75] A number of U.S. cloud providers, including Amazon Web Services (AWS) and Microsoft, take this approach. For example, AWS now has fifty-five "availability zones" around the world.[76] It most recently opened a European region in France.[77] German telecommunication companies have also developed clouds that store data exclusively in Germany.[78] As one trade publication explains, "The main selling points for cloud operators in Germany are location, location[,] and location."[79] An important distinction should be made, however, between data localization as a technical matter and as a legal one. This Article uses the concept of the Data Localization model to point to *technical localization*, that is, a network configuration that stores digital information exclusively in one or more locations and excludes it from other geographic locations. In contrast, *legal localization* refers to a statute or other binding legal mandate that requires such local data storage. Chander and Lê have documented a notable trend throughout the world of legal data localization.[80]

A Data Localization model was at the center of the *Microsoft Ireland* litigation.[81] The case concerned a web-based email service run from a data center in Dublin, Ireland. A wholly owned Microsoft subsidiary operated this Irish data center, and U.S. law enforcement authorities had subpoenaed Microsoft for records in this cloud space.[82] Thus far, this Article has discussed only the idea of a pure Data Localization model. The twist in the *Microsoft Ireland* case, however, is that the precise model at stake was a partial or incomplete one.[83] In that case, Microsoft technicians and attorneys in both Dublin and Redmond, Washington, could access the sought-after information.[84] In *Microsoft Ireland*, the *location* of the data was

---

75. For a critical account of the "push for data localization," see Patrick Ryan et al., When the Cloud Goes Local: The Global Problem with Data Localization, Computer, Dec. 2013, at 54, 57.

76. AWS Global Infrastructure, supra note 20.

77. Sam Clark, AWS Opens New Region in Paris to Widen Reach, Stack (Dec. 19, 2017), https://thestack.com/cloud/2017/12/19/aws-opens-new-region-in-paris-to-widen-reach [https://perma.cc/5T96-6V3R].

78. Peter Sayer, For Germany's Cloud Providers, It's Location, Location, Location, Network World (Mar. 14, 2016), http://www.networkworld.com/article/3043951/for-germanys-cloud-providers-its-location-location-location.html [https://perma.cc/UK9J-LTJZ].

79. Id.

80. See Chander & Lê, supra note 68, at 708–13. For an argument that laws requiring local data localization are driven by "[n]ation-states who perceive themselves to be at a comparative disadvantage in the efficiency of their Internet signals intelligence," see John Selby, Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?, 25 Int'l J.L. & Info. Tech. 213, 232 (2017).

81. See 829 F.3d 197, 202–03 (2d Cir. 2016).

82. Id. at 203.

83. See id.

84. As Judge Gerard Lynch noted in his concurrence in *Microsoft Ireland*, Microsoft employees located domestically were capable of reviewing the records in question "and

Ireland, but *access* to the information could take place either from Dublin or Redmond.[85] Unlike the cloud model at issue in *Microsoft Ireland*, many other Data Localization clouds are complete. For example, cloud services offered by AWS and Microsoft's regional European Union cloud are not accessible from the United States.[86]

Finally, the Data Trust model, the third approach, builds on and further refines the Data Localization approach.[87] As in the Data Localization model, a Data Trust cloud can be located within one country or a single region. But the further step here is to separate network management from the ability to access data.[88] In the Data Trust approach, one entity—the Data Manager—oversees the network hardware and software. A separate party, the Data Trustee, has the exclusive ability to access the data. Here, we reach the opposite pole from the Data Shard model, which relies on networked intelligence and ignores national boundaries. The Data Trust model depends on legal and technical constructs—national boundaries and trust instruments—and shapes technology to fit the selected legal categories. This approach can be used to establish both an extraterritorial *location* of information and an extraterritorial *access* to it. Moreover, the Data Trust model bifurcates the issue of management of the cloud network from that of access to data. This Article terms this quality the "divisibility of control" and explores its significance below.

---

provid[ing] the relevant materials to the demanding government agency, without ever leaving their desks in the United States." Id. at 229–30 (Lynch, J., concurring).

85. See id.

86. See Amazon Web Services, Choosing a Cloud Platform, AWS, https://aws.amazon.com/choosing-a-cloud-platform/ [https://perma.cc/97WA-QTFM] (last visited July 26, 2018); Microsoft, Microsoft Azure Germany, Microsoft Azure, https://azure.microsoft.com/en-us/overview/clouds/germany [https://perma.cc/A3K9-HYM8] [hereinafter Microsoft Azure] (last visited July 26, 2018).

87. One early discussion of cloud computing pointed to a "Cloud Cube Model" in which one element concerned "technology ownership." Barrie Sosinsky, Cloud Computing Bible 6–7 (2011). The Data Trust can be seen as building on this aspect of cloud computing. A different theoretical approach speaks of a concept of "data sovereignty," which is also somewhat similar to the idea of the Data Trust. Nayan B. Ruparelia, Cloud Computing 119 (2016).

88. One Data Trust model, the Microsoft Cloud Germany, has been the subject of legal analysis in the German legal literature concerning cloud privacy. See Michael Rath et al., Die neue Microsoft Cloud in Deutschland mit Datentreuhand als Schutzschild gegen NSA & Co.? [The New Microsoft Cloud in Germany: A Data Fiduciary as Protective Shield Against the NSA and Company?], 32 Computer und Recht 98, 103 (2016) (emphasizing the contractual and technical protections in the Data Trust model as developed by Microsoft Germany); Paul M. Schwartz & Karl-Nikolaus Peifer, Datentreuhändermodelle—Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte? [Data Fiduciary Model—Protection from Data Requests of U.S. Governmental Authorities and Courts?], 33 Computer und Recht 165, 174 (2017) [hereinafter Schwartz & Peifer, Data Fiduciary Model] (concluding that the use of a Data Trust model in Germany increases the protection of stored information from requests by foreign law enforcement by making it subject to German data protection law).

At present, only Microsoft makes use of the Data Trust model.[89] It offers a "Microsoft Cloud Germany" to customers in the European Union and European Economic Area.[90] The Microsoft Data Trust stores customer data exclusively within Germany, in data centers located in Frankfurt and Magdeburg.[91] Most significantly, T-Systems is the trustee for the stored information, which means it alone controls the ability to access the network.[92] T-Systems is an independent German corporation. The trust arrangement, which is a contractual obligation under German law between the two parties, significantly restricts the access of Microsoft Germany to the information in its cloud.[93] Beyond law, moreover, customer data in the Microsoft German cloud are encrypted, and only T-Systems holds the keys to the data.[94] As a result, Microsoft is unable, as a technical matter, to gain access to the data in clear text.

As the trust is set up, T-Systems—not Microsoft Germany—is responsible for handling all outside data requests, whether from government or private third parties.[95] As a legal matter, under the German law of trusts and pursuant to its agreement with T-Systems, Microsoft is generally forbidden from accessing the information in its cloud without the permission of T-Systems.[96] Moreover, Microsoft can access the information only for a limited number of specified reasons, such as for network maintenance, and can do so only under the supervision of T-

89. See Microsoft, Microsoft Cloud Germany Datasheet 1–2 (2016) [hereinafter Microsoft Cloud Germany Datasheet], https://go.microsoft.com/fwlink/?LinkId=839380&clcid=0x409 (on file with the *Columbia Law Review*).

90. Id.

91. Id.

92. Id.

93. See Microsoft Azure, supra note 86 ("An independent data trustee controls access to all customer data in the Azure Germany datacenters. T-Systems International . . . serves as trustee, protecting disclosure of data to third parties . . . . Even Microsoft does not have access to customer data or the datacenters without approval from and supervision by the German data trustee.").

94. See Microsoft Cloud Germany Datasheet, supra note 89, at 1 ("[T-Systems] controls physical and logical access to customer data."); Microsoft, Encryption, Microsoft Trust Center, https://www.microsoft.com/en-us/trustcenter/security/encryption (on file with the *Columbia Law Review*) (last visited July 26, 2018) ("Microsoft business cloud services and products use encryption to safeguard customer data . . . . [O]nly someone with the decryption key can access it.").

95. Frank Simorjay, Microsoft, Microsoft Cloud Germany: Compliance in the Cloud for Organizations in EU/EFTA 9 (2016), https://gallery.technet.microsoft.com/Cloud-Germany-Compliance-4161d8df/file/159647/4/Microsoft%20Trustee%20Compliance%20model.pdf (on file with the *Columbia Law Review*) ("Because Microsoft does not have custody of or access to Microsoft Cloud Germany customer data, Microsoft is unable to comply with requests from governments or other parties for access to customer data . . . .").

96. Id. at 6 ("Under normal operating conditions . . . Microsoft has no access to German customer data."). For an analysis of these provisions, see Schwartz & Peifer, Data Fiduciary Model, supra note 88, at 170–71.

Systems.[97] The agreement between T-Systems and customers of the German cloud contractually obliges the Data Trustee, T-Systems, to perform its role of managing data in strict accordance with terms of the trust.[98] Finally, as noted earlier, the data in the system are encrypted with the Data Trustee in control of the keys. It is the Data Trustee who performs or supervises any operational tasks that require access to customer data or the infrastructure on which customer data resides.[99]

Thus, Microsoft Cloud Germany takes decisive steps to separate construction and management of the cloud data from control of access to it. Microsoft is doubly restricted—legally and technically—from accessing customer data by German law (the trust arrangement) and existing technical restrictions (the encryption keys). Microsoft built the network and its software runs on it, but T-Systems controls the physical and "logical" systems that process customer data. The technology of this network solidifies the divisibility of control also established by the trust agreement.

C. *The Scholarly Debate and Initial Lessons*

These three models show a rich variety of approaches to cloud computing services. They demonstrate that one size *doesn't* fit all in litigation that evaluates *access* to data and *location* of data in the cloud. Different clouds lead to different answers to questions about ability to access data and the location of data. Leading legal scholarship is wrestling with the meaning of territoriality in regulating access to cloud data but has not engaged in the consideration of different types of cloud services.

1. *The Scholarly Debate.* — Just as the case law is uncertain about questions regarding access and location, an important debate in the legal academy concerns the extent to which clouds necessitate a new approach in this area. The leading voices in this discussion are Professors Andrew Woods and Jennifer Daskal. The scholarship is divided on the question of the relevance of territoriality with respect to international access to cloud data. Woods can be seen as representing the "business as usual" camp, and Daskal can be viewed as leading the "data exceptionalists."[100] As we

97. Simorjay, supra note 95, at 6 (outlining a four-step process for Microsoft to access customer data: (1) Microsoft's request for access; (2) verification of the request; (3) grant of supervised access "scoped to a specific service and only for the time necessary"; and (4) access termination upon completion of the task).

98. Id. at 9 ("The relationships between Microsoft and the data trustee, Microsoft and its customers, and the data trustee and customers are enforced by binding contracts among all three parties.").

99. See supra notes 92–94 and accompanying text.

100. For scholars other than Woods in the business-as-usual camp, see Kerr, The Fourth Amendment, supra note 18, at 291; Swire & Hemmings, Mutual Legal Assistance, supra note 62, at 715–16. For voices other than Daskal regarding data exceptionalism, see Andrews & Newman, supra note 18, at 388; Zachary D. Clopton, Territoriality, Technology, and National Security, 83 U. Chi. L. Rev. 45, 62–63 (2016); Cole & Fabbrini, supra note 18, at 234; Ahmed Ghappour, Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, 69 Stan. L. Rev. 1075, 1086 (2017).

will also see in the next section, members of the judiciary have adopted positions reflecting one or the other point of view.

On one side in the debate, Woods views data as a physical object. As he puts it: "[T]he 'cloud' is actually a network of storage drives bolted to a particular territory . . . ."[101] Regarding law enforcement access to data in the criminal law context, Woods notes that "[c]ontrary to prevailing wisdom, jurisdiction over cloud-based data has nearly everything to do with territoriality—it requires an inquiry into the location of the data, the domicile of the data controller, the location of the crime, the citizenship of the victim, and/or the citizenship of the perpetrator."[102] In his view, some scholars in this area mistakenly begin from a starting point of data exceptionalism.[103] For Woods, academics with this perspective consider information to be radically different. In particular, the data exceptionalists believe existing legal paradigms fail to provide a framework for access to cloud-based data.[104]

This perspective is unconvincing for Woods, who points to other assets, such as money in a bank account, that are similarly mobile and divisible.[105] International wire transfers of money are a daily event and, crucially, in his view, courts have developed rules for "determining the location of money for the purposes of asserting jurisdiction over the asset."[106] Indeed, Woods would go so far as to argue that while cloud data can be "cop[ied] and store[d] in multiple locations" more easily than "debt, money, or other assets," the "core of the territoriality analysis" remains unchanged.[107] Unlike a variety of intangible assets, cloud data have a physical presence; they reside on "physical drives that can be seized."[108]

Woods proposes that a standard comity test be applied to data in the global cloud. Comity is a long-standing concept of reciprocity in international law; it is the principle that one jurisdiction will extend the courtesy to a foreign jurisdiction by recognizing the validity of its law. In this context, a comity analysis considers whether the nation seeking the information stored in the cloud "has an interest in [the] data that outweighs competing state interests."[109] In the established approach, courts decide whether or not another jurisdiction's interests weigh against the transfer of the sought-after evidence.[110] Although such a test can be unpredictable, Woods finds any possible uncertainty to be "a small price to pay for

101. Woods, supra note 3, at 729.
102. Id. at 735.
103. See id. at 788.
104. See id. at 788–89.
105. See id. at 729.
106. Id. at 758.
107. Id.
108. Id. at 761.
109. Id. at 774.
110. Id. at 778.

an approach to resolving conflicts that takes into account the concerns of other states and solves jurisdictional disputes in a decentralized, case-by-case manner."[111] Woods does not explain, however, if decentralization is merely the best likely solution, a second-best solution, or a solution with merits of its own in this context.

In addition, Woods sees a need for reciprocity among foreign legal authorities in recognizing and enforcing foreign judgments.[112] In particular, he notes that "American courts could agree to respond to foreign law enforcement requests for data on an expedited basis if and only if the request comes from a country that processes American government requests for data expeditiously."[113] Like his judicial comity analysis, the policy solution here would also be decentralized.

Finally, Woods argues that such "a decentralized, state-by-state approach to state access to data in the cloud" is preferable to a "push for an international treaty forged out of pixie dust."[114] As the mention of "pixie dust" indicates, Woods is skeptical of the merits of a global treaty for access to international cloud data.[115] In his judgment, it is unnecessary and undesirable to develop such a broad multilateral agreement because comity rules are already in place to handle these matters.[116] Additionally, a treaty regime would likely reach only the lowest common denominator to ensure that all parties sign on to the agreement.[117] Such a low threshold of protection for the purposes of gaining consensus would likely threaten due process and other individual rights. The many undemocratic states throughout the world would demand weak treaty provisions to permit them to inundate American cloud providers with demands for access to information of their nationals stored in the United States.[118]

In contrast to Woods, Jennifer Daskal views the "un-territoriality of data" as raising fundamentally new challenges.[119] She argues that "data undermines longstanding assumptions about the link between data location and the rights and obligations that should apply."[120] Digital information is different because data now flow across international borders with "ease, speed, and unpredictability."[121] Moreover, there is a physical

111. Id.

112. Id.

113. Id.

114. Id. at 781.

115. See id.

116. See id. at 788.

117. Id.

118. See Daskal, Law Enforcement Access, supra note 3, at 490 (warning of a "free-for-all" which would harm privacy rights).

119. Daskal, The Un-Territoriality of Data, supra note 18, at 326.

120. Id.

121. Id. at 329.

disconnect between the location of the data and the location of the user.[122] Indeed, cloud users may not even know where their information is located.[123] As Daskal states, "Whereas territoriality depends on the ability to define the relevant 'here' and 'there,' data is everywhere and anywhere and calls into question which 'here' and 'there' matter."[124] In sum, "[d]ata is shaking territoriality at its core."[125]

Daskal warns of new risks in a world where territoriality lacks its former normative significance. In particular, her chief message is to caution against "the kind of unilateral, extraterritorial law enforcement that electronic data encourages—in which nations compel the production of data located anywhere around the globe, without regard to the sovereign interests of other nations."[126] Daskal further argues that this result would impose another set of costs, including "the balkanization of the Internet into multiple, closed-off systems."[127] Her policy solution is to call for "a series of bilateral or multilateral agreements among a handful of like-minded nations."[128] As this Article discusses below, the CLOUD Act creates a process for reaching such agreements for the international law enforcement community and permits these accords to reach beyond the relatively limited authorities found in the SCA.[129] As for Daskal, her proposed solutions depend on jurisdictional tests that apply to both regulatory and compulsory process goals.[130] In shaping these solutions, Congress and the executive branch should both be involved.[131]

Daskal also rejects data location as the sole determinant of the rules that should apply.[132] She points to a need for better alternative approaches. Jurisdiction could be based on the nature of the crime and the requesting government's interest in prosecution.[133] Daskal suggests that such factors might supplement or substitute for other factors. Another possible jurisdictional approach would look to "the place where the

---

122. Id.

123. Kim Lindros & Ed Tittel, How to Explain the Cloud to End Users, CIO (Aug. 27, 2014), https://www.cio.com/article/2598057/cloud-security/how-to-explain-the-cloud-to-end-users.html [https://perma.cc/4LWA-YUT6].

124. Daskal, The Un-Territoriality of Data, supra note 18, at 397.

125. Id.

126. Id. at 326.

127. Id. at 333–34.

128. Id. at 395. Daskal also has a normative prescription concerning the Fourth Amendment. She calls for a presumption of applicability of this constitutional protection "regardless of whether the collection [of data] takes place inside or outside of the United States, and regardless of whether the target is a U.S. person or not." Id. at 383. The government can rebut this "presumptive Fourth Amendment" only by establishing that none of the parties to the communication is a U.S. person. Id.

129. See infra section III.B.2.b.

130. Daskal, The Un-Territoriality of Data, supra note 18, at 395–96.

131. Id.

132. See Daskal, Law Enforcement Access, supra note 3, at 498–99.

133. Daskal, The Un-Territoriality of Data, supra note 18, at 395.

company controlling the data operates or maintains its headquarters; user nationality; or user location."[134] Under such a framework, many jurisdictional flowers would bloom in place of the current approach of "unilateral, extraterritorial law enforcement."[135] In time, the hope is that a series of tailored, superior approaches would emerge to the "un-territoriality" of data.[136]

2. *Initial Lessons.* — Four preliminary conclusions can be reached at this juncture. First, regarding the extent to which the cloud raises new legal issues, the best answer is "it depends." Data servers are certainly bolted to a particular geographical territory, but they are also networked globally. For data in clouds, there is a new kind of malleability concerning data location, service provider location, and accessing party location.[137] Moreover, the information at stake is not just another form of intangible property. Unlike the kinds of assets that Woods points to, such as debts or stocks,[138] the issue of propertization of personal information is highly contested.[139] There is also no agreement in the United States as to the extent that personal information should be viewed as the property of an individual, and, even more to the point, it is unclear how propertization would clarify questions relating to access to global cloud data.[140]

At the same time, data in the cloud raise different issues than, for example, data in a filing cabinet. Most crucially, one size does not fit all when current law assesses legal access to global clouds. Analysis must consider the precise kind of cloud model that is at issue. Hence, to Daskal's point about the "un-territoriality of data," some clouds do not call into question the "here" and "there."[141] For example, one can consider a cloud located in a single country as roughly analogous to the lockers of a self-storage company located in a single jurisdiction.[142] Such data operations, which this Article terms complete Data Localization clouds, are not "shaking territoriality at its core."[143] Hence, there is no special paradigmatic value in the viewpoint of either the data exceptionalists (Daskal) or the camp arguing for business as usual (Woods).

---

134. Id.

135. Id. at 333.

136. Id. at 333–34.

137. See supra text accompanying notes 19–24.

138. See Woods, supra note 3, at 756.

139. For a window into the debate about personal data propertization, see generally Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2056 (2004).

140. See id. at 2057–58.

141. Daskal, The Un-Territoriality of Data, supra note 18, at 326.

142. A storage locker or similar metaphor is frequently used in the context of cases involving law enforcement access to stored digital data. See, e.g., United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) (likening a search of a computer to a search of a locked footlocker).

143. Daskal, The Un-Territoriality of Data, supra note 18, at 397.

The key requirement is to consider how different cloud models function and the implications for global data access. Yet, as the brief survey above of *Microsoft Ireland* and *Google Pennsylvania* demonstrates, judicial awareness of the implications of the different network models appears scant. Judges in cloud access cases are divided among the data exceptionalists or the business-as-usual proponents for data access issues. These different perspectives still lead to different results in judging data access requests post–CLOUD Act.

This Article already discussed Judge Susan Carney's insistence that "even messages stored in the 'cloud' have a discernible physical location."[144] Thus, there is ultimately nothing new concerning this request in her view, and Judge Carney can be said to belong to the business-as-usual camp. For a Data Shard cloud, however, such a location is evanescent, and this categorization is not helpful.[145]

The Second Circuit's denial of a petition for rehearing en banc in *Microsoft Ireland* further illustrates the judicial struggle to understand different cloud models.[146] The dissenting judges in the rehearing grappled with the question of the nature of different cloud networks and, at times, conflated different cloud models. In his dissent, for example, Judge Dennis Jacobs adopted the business-as-usual perspective.[147] For him, the only question was where Microsoft had access to the data. Thus, the physical location of information mattered, but only for deciding the question of where Microsoft could access it. As Judge Jacobs noted, "It need only touch some keys in Redmond, Washington."[148] All other questions about territoriality were unhelpful in his view, and in a *cri de coeur*, he warned against those who would promote "reifying the notional."[149] In his view, "Localizing the data in Ireland is not marginally more useful than thinking of Santa Claus as a denizen of the North Pole."[150] To him, it does not matter where Santa Claus lives, and it does not matter where data are stored; data in the cloud do not raise new issues. In case anyone missed the point, Judge Jacobs provided a final dramatic flourish: "Where are the snows of yesteryear?"[151]

---

144. *Microsoft Ireland*, 829 F.3d 197, 220 n.28 (2d Cir. 2016).

145. See supra text accompanying note 22.

146. 855 F.3d 53, 54 (2d Cir. 2017) (denying en banc review).

147. See id. at 61 (Jacobs, J., dissenting).

148. Id.

149. Id. at 62.

150. Id.

151. Id. As comparative literature majors and fans of medieval French literature will recognize, Judge Jacobs is quoting François Villon's Ballade des Dames du Temps Jadis: "*Mais où sont les neiges d'antan.*" François Villon, Ballade des Dames du Temps Jadis [Ballade of the Ladies of Times Past] (15th c.).

In his dissent to the denial of the petition for rehearing, however, Judge Christopher Droney raised the issue of the nationality of the cloud provider. He wrote: "If the emails sought by the Government in this case were maintained by a foreign-based internet service

At the oral hearing in *Microsoft Ireland*, the Supreme Court similarly struggled to understand differences in cloud models and the relative significance of where one accessed data versus where one stored it.[152] The Justices strove to develop analogies and metaphors that would allow them to grasp the nature of cloud computers and whether there was something new under the sun that existing law did not capture. For Justice Ruth Bader Ginsburg, the Microsoft computers were located in Ireland, and "something ha[d] to happen to those computers in order to get these e-mails back to the United States."[153] This would be a business-as-usual perspective.[154] In contrast, Justice Anthony Kennedy wondered if a Microsoft employee present in Ireland had to act on the computer on which the data was stored.[155] Did "some person have to be there?" he asked.[156] This line of questioning might have opened the door to adoption of a data exceptionalism viewpoint.[157] In response and perhaps pointing in this direction, Joshua Rosenkranz, Microsoft's attorney, came up with the idea of a "robot" being sent "into a foreign land to seize evidence," which "would certainly implicate foreign interests."[158]

This attempt to explain cloud computing through robot messengers proved to have limited appeal for the high court. At that junction, Justice Sonia Sotomayor stated, "I'm sorry . . . I guess my imagination is running wild," and asked, "[W]ho tells the robot what to do and what does the robot do?"[159] The answer from Rosenkranz: The cloud provider would send the robot instructions to execute in the foreign land.[160] This explanation did not appear to gain traction.[161] Finally, Justice Ginsburg wondered whether "in this brave new world," it might "be wiser just to say let's leave things as they are" and let Congress regulate if it wants.[162] In sum, and in line with the first point, data in the cloud can raise different and new legal questions, but no simple perspective—whether location of data, territoriality, or access—will be sufficient.

---

provider, the situation would be quite different." *Microsoft Ireland*, 855 F.3d at 76 (Droney, J., dissenting).

152. See Transcript of Oral Argument at 35–39, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2).

153. Id. at 8.

154. See supra section I.C.1.

155. Transcript of Oral Argument, supra note 152, at 44.

156. Id.

157. See supra section I.C.1.

158. Transcript of Oral Argument, supra note 152, at 44–45.

159. Id. at 45.

160. Id.

161. At any rate, Justice Neil Gorsuch chose not to focus on mechanical messengers and instead asked why the government could not just obtain a warrant in Redmond and "[p]ush . . . aside" someone from Microsoft to seize the data there in the United States. Id. at 46–47.

162. Id. at 6.

Second, Data Trust clouds point to an additional lesson previously mentioned—namely divisibility. It is now possible to separate management of networked information from the ability to access it.[163] This division can be achieved through technology (software that places access controls in the hands of a Data Trustee).[164] It can be further bolstered through domestic law (through the creation of a formal Data Trust).[165] This aspect of cloud services is likely to increase in importance in the future; as this Article explores below, an increase in governmental requests through the subpoena process will heighten the attractiveness of Data Trust networks. This result follows because divisibility of control in this kind of cloud network heightens the insulation of such non-U.S. clouds from subpoenas.[166] The law must now take divisibility into account in its rules for access to global data.

Third, Daskal's prediction about internet balkanization has already been validated. There are several causes for this phenomenon: technical localization, consumer demand, and legal data localization. This Article has distinguished between technical data localization, in which network management structures the localization, and legal data localization, in which a statute or other kind of legal mechanism mandates the localization. In part, technical data localization is being driven on the demand side. International privacy advocates are skeptical of U.S. tech companies in general and their global clouds in particular; their call is for a homegrown digital infrastructure. Thus, in warning against U.S. clouds, German investigative reporters Stefan Aust and Thomas Ammann advocate development of "a stronger European data protection" as part of a "self-conscious development" of an independent European digital infrastructure.[167] One benefit will be to end the "tacit transmission of our information to U.S. intelligence services."[168] Moreover, just as green technology can be a factor for economic growth, Aust and Ammann believe strong data protection laws will stimulate a native digital industry in Germany and the European Union.[169]

Customers in many countries also want to keep their data within their own country, and the market for cloud services has responded with a new set of services. As Professor Peter Swire and Justin Hemmings write, "[C]ompanies have sought ways to show global customers their careful

---

163. See supra section I.B.

164. See supra section I.B.

165. See supra section I.B.

166. The basic point is that a powerful argument can be made that information in Data Trust clouds is a record of the user and not of the service provider or the Data Trustee. See infra section III.A.

167. Stefan Aust & Thomas Ammann, Digitale Diktatur [Digital Dictatorship] 341 (2014).

168. Id.

169. Id.

stewardship of private data."[170] U.S. tech companies have experienced monetary losses from the decisions made post-Snowden in the global marketplace and are now responding by offering localized services.[171] In a joint amicus brief before the Second Circuit in *Microsoft Ireland*, Verizon, Cisco, Salesforce, and other corporations cautioned about the counterproductive impact of extending extraterritorial effect to the SCA.[172] The tech companies warned: "Foreign customers will respond by moving their business to foreign companies without a presence in the United States, ultimately frustrating the interests of the U.S. government in general . . . ."[173] To some extent, the CLOUD Act speaks to this concern by leveling the differences between U.S. and non-U.S. cloud providers for non-U.S. customers.[174] At the same time, and as will be discussed below, some differences still remain that make non-U.S. clouds attractive for customers outside the United States. These customers' ability to route around the law, at least to some extent, by using non-U.S. clouds will persist post–CLOUD Act given the sweep of other U.S. statutory authorities for extraterritorial data access.

Data localization is also being driven by legal requirements. European law already contains occasional mandates for legal data localization. For example, a recent German law requires providers of publicly available telecommunications services to store certain traffic data within Germany.[175] Outside the European Union, nondemocratic countries, such as Russia, have enacted different kinds of legal data localization requirements.[176] There are multiple reasons for these laws, including protectionism for native tech companies and making surveillance easier for domestic intelligence agencies and law enforcement agencies.[177] The perverse result, as Chander and Lê argue, is that the centralizing of user information can also lighten the surveillance burden for outside intelligence agencies.[178]

---

170. Swire & Hemmings, Mutual Legal Assistance, supra note 62, at 714.

171. See Claire Cain Miller, Revelations of N.S.A. Spying Cost U.S. Tech Companies, N.Y. Times (Mar. 21, 2014), https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html (on file with the *Columbia Law Review*).

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

173. Id.

174. See CLOUD Act, H.R. 1625, 115th Cong. div. V, § 103(a)(1) (2018) (adding 18 U.S.C. § 2713(h)(2), which establishes a mechanism for a U.S. cloud provider to file a motion to quash if the customer "is not a United States person and does not reside in the United States").

175. Lothar Determann & Michaela Weigl, Data Residency Requirements Creeping into German Law, 3 World Data Protection Rep. (BNA) (Mar. 24, 2016).

176. Chander & Lê, supra note 68, at 717–19.

177. Swire & Hemmings, Mutual Legal Assistance, supra note 62, at 712.

178. Chander & Lê, supra note 68, at 717.

Fourth, and most critically, policy in this area must be based on a dynamic analysis of the interaction of legal rules and cloud technology. The technology of the cloud now provides a way to route around law. The development of Data Localization clouds as well as Data Trust clouds shows that more companies and individuals outside of the United States have ways to shelter their data beyond the SCA's reach. Sound policymaking requires anticipation of the likely interplay of the resulting cycles of interaction between technology and law. This dynamic extends beyond the SCA, as amended by the CLOUD Act; policymakers must consider the full range of legal authorities and how law and technology interact to affect the scope of these different means for gaining access to cloud data. This Article will now carry out this task and examine the law permitting government and private parties extraterritorial access to data held in non-U.S. clouds.

II. EVALUATING LEGAL AUTHORITIES FOR EXTRATERRITORIAL ACCESS TO DATA

This Article argues that different cloud management models raise distinct issues concerning extraterritorial requests for information. In section I.A, this Article looked at the assessment by two courts of a law enforcement data request made pursuant to the SCA. In addition to the SCA, U.S. law provides other ways for parties to seek access to information held abroad. This Article now explores these legal authorities. It distinguishes between the means available to the U.S. government and to private parties. For each legal authority, this Part assesses the likely results when the information is part of a Data Shard, Data Localization, or Data Trust cloud model. It finds notable differences in the likely outcomes following from the same legal authority being applied to different cloud management models.

This Part finds a likely shift to law enforcement use of subpoena power rather than warrant power. It also points to a rising significance of MLATs, which will incorporate foreign law into data access questions. Additionally, there will be increased incentives for non-U.S. customers who are concerned about U.S. access to their data to select Data Localization and Data Trust clouds. In seeking to cover the applicable legal authorities in a concise and clear fashion, this Part concludes each section with a summary of the legal authority in question. Finally, an Appendix to this Article summarizes the findings of this Part. A single chart can sometimes be worth a thousand words—or even several thousand words.

A. *Extraterritorial Access by the U.S. Government*

In assessing the U.S. government's access to cloud information, one threshold question is the reach of the Fourth Amendment. Other legal authorities open to the U.S. government are the MLAT process, the SCA,

administrative and grand jury subpoenas, and regulations and statutes concerning foreign intelligence surveillance.

1. *The Fourth Amendment.* — The Fourth Amendment protects individuals against certain kinds of collection of personal information by the government. It safeguards a right of "the people" to be secure against "unreasonable searches and seizures" of "persons, houses, papers, and effects."[179] The Fourth Amendment also contains a provision stating that no warrants shall be issued except "upon probable cause."[180] But in their role of restricting governmental activities, these interests are limited in their ability to safeguard data privacy rights against extraterritorial surveillance.

The Fourth Amendment is a restriction on governmental power, not a grant of power.[181] Accordingly, the authority to execute search warrants on foreign soils must be located elsewhere.[182] For example, *Microsoft Ireland* examined whether the SCA could provide such authority to compel a company to disclose data stored outside the United States.[183] But for the U.S. government to carry out a search or seizure on foreign soil without the cooperation of the local government would probably constitute a crime under local law, something U.S. government agents would be reluctant to do.[184] This reluctance reflects, in part, the "well-established international law axiom that one state may not unilaterally exercise its law enforcement functions in the territory of another state."[185] This axiom is reflected in the Restatement (Third) of Foreign Relations Law. It observes, "A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officers of that state."[186]

If the U.S. government were to convince non-U.S. authorities to carry out a search and seizure of data stored in their country on behalf of the United States, or to look the other way when U.S. agents committed the search and seizure themselves, however, the Fourth Amendment might limit this application. In *United States v. Verdugo-Urquidez*, the Supreme Court held that Fourth Amendment search and seizure

179. U.S. Const. amend. IV.

180. Id.

181. See id.

182. See Fed. R. Crim. P. 41(b)(5) (permitting warrants for searches on property outside the United States, owned or leased by the United States for diplomatic or consular purposes).

183. 829 F.3d 197, 200–01 (2d Cir. 2016).

184. There have been rare cases in which the U.S. government, in criminal investigations, obtained access to data stored on foreign computers without the cooperation of either the local government or the service provider. Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace 136–39 (2010); see also United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *1 (W.D. Wash. May 23, 2001) (describing how FBI agents in the United States accessed a criminal suspect's server in Russia).

185. Ghappour, supra note 100, at 1082–83.

186. Restatement (Third) of the Foreign Relations Law of the United States § 432(2) (Am. Law Inst. 1987).

restrictions do not apply extraterritorially to people without "significant voluntary connection[s]" to the United States.[187] While a warrant is not required for searches outside the United States, *Verdugo-Urquidez* has also been interpreted to mean that the Amendment's reasonableness requirement applies to searches outside the United States, but only if they involve a U.S. person or a person with significant contacts with the United States.[188] In this reading, the Fourth Amendment demands "reasonableness," but not a warrant for certain searches outside the United States.

The applicable circuit precedent is split, however, on what "reasonableness" requires in this context. The Ninth Circuit has found that the Fourth Amendment reasonableness test requires that the U.S. government, when conducting a search abroad, comply with the foreign law in the jurisdiction where the search occurs.[189] In contrast, the Second and Seventh Circuits have held that Fourth Amendment reasonableness for extraterritorial searches requires a balancing of the government's need for the information and the privacy interest at stake.[190] Most crucially, the extent of Fourth Amendment protection will vary depending on whether a cloud is organized as a Data Shard, Data Localization, or Data Trust network.

Finally, there is the issue of the Third-Party Doctrine. It dictates that people who voluntarily give information to so-called third parties have no "reasonable expectation of privacy" under the Fourth Amendment.[191] Among other kinds of information, the Supreme Court has applied the Third-Party Doctrine to bank records and telephone numbers dialed from, or received by, a device.[192]

Three key decisions have developed the doctrine thus far. First was *United States v. Miller*, a 1976 Supreme Court decision that, for purposes

---

187. 494 U.S. 259, 261, 271 (1990).

188. See id. at 274–75.

189. See United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987) (holding that when the United States is involved in investigations abroad, "the law of the foreign country must be consulted at the outset as part of the determination whether or not the search was reasonable").

190. See United States v. Stokes, 726 F.3d 880, 893 (7th Cir. 2013) ("Whether a search is reasonable under the Fourth Amendment . . . requires the court to weigh the intrusion on individual privacy against the government's need for information and evidence."); United States v. Maturo, 982 F.2d 57, 61 (2d Cir. 1992) (balancing the appellant's Fourth Amendment rights against the alleged unreasonable cooperation between the U.S. Drug Enforcement Administration and the Turkish National Police).

191. See Solove & Schwartz, Information Privacy Law, supra note 35, at 288–95.

192. See Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding under the Third-Party Doctrine that Fourth Amendment protections do not apply to telephone numbers dialed from a device); Solove & Schwartz, Information Privacy Law, supra note 35, at 288–95 (discussing applications and critiques of the Third-Party Doctrine). For a recent argument concerning the need to narrow the current understanding of the Third-Party Doctrine, see Neil Richards, The Third Party Doctrine and the Future of the Cloud, 94 Wash. U. L. Rev. 1441, 1489 (2017).

of its Fourth Amendment analysis, found that checks were the bank's "business records" and not the "private papers" of the depositors.[193] Building on *Miller*, the Court then held in *Smith v. Maryland* in 1979 that law enforcement's use of a pen register, a device that recorded numbers dialed, did not implicate Fourth Amendment rights.[194] When Smith placed a call, he "voluntarily conveyed" the telephone numbers to the phone company.[195] In June 2018, however, in *Carpenter v. United States*, the Court placed a significant new limitation on the Third-Party Doctrine.[196]

The *Carpenter* opinion concerned cell-site location information (CSLI). For the Supreme Court, government acquisition of CSLI was a Fourth Amendment search that generally required a warrant. It declared that there was "a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."[197] The Court emphasized the "unique nature of cell phone location information," which provided a unique set of locational data derived, in part, from the tendency of individuals to "compulsively carry cell phones with them all the time."[198]

It is, therefore, an open question whether the Fourth Amendment applies to information stored in a cloud, either extraterritorially or domestically. Cloud information may be seen as akin to what Justice Kennedy called "the modern-day equivalents of an individual's own 'papers' or 'effects.'"[199] Such information does seem distinguishable from a mere telephone number or a negotiable instrument, such as a check. For example, the format of that information is decided by a telephone company or financial institution respectively and not by the party who generates it. On the other hand, a future court may try to distinguish cloud information from the "increasingly precise CSLI" to which the *Carpenter* Court extended the Fourth Amendment.[200]

a. *Data Shards.* — We begin with an analysis of a governmental request for information located outside the United States and stored in a

193. 425 U.S. 435, 440–41 (1976).

194. *Smith*, 442 U.S. at 745–46 (citing *Miller*, 425 U.S. at 442).

195. Id. at 744.

196. 138 S. Ct. 2206, 2220 (2018).

197. Id. at 2219.

198. Id. at 2218–20.

199. Id. at 2230 (Kennedy, J., dissenting) (citing United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010)).

200. Id. at 2212. Existing case law on this point is limited. See *Warshak*, 631 F.3d at 288 (finding that Fourth Amendment rights exist in remotely stored email); United States v. Bach, 310 F.3d 1063, 1066 n.1 (8th Cir. 2002) (applying the search warrant standard in a case involving remotely stored email). For a discussion, see Orin Kerr, Does Carpenter Revolutionize the Law of Subpoenas?, Lawfare (June 26, 2018), https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas [https://perma.cc/TU9D-S3QG].

Data Shard cloud. As a threshold matter, the Fourth Amendment is only applicable when a search or seizure occurs. As an example of an activity that does not reach this threshold, a police officer that observes illegal behavior carried out in "plain view" is not considered to be conducting a search and, hence, does not implicate the Fourth Amendment.[201]

For Fourth Amendment purposes, however, courts are likely to consider the government's collection of information from a Data Shard cloud to be a "search." Indeed, the *Google Pennsylvania* court reached this conclusion.[202] Similarly, Orin Kerr, the leading scholar of electronic criminal procedure, has long argued that a Fourth Amendment search occurs when "information from or about the data is exposed to possible human observation, such as when it appears on a [computer] screen."[203]

If retrieval is considered a "search" under the Fourth Amendment, the next question under *Verdugo-Urquidez* is whether the information in question belongs to a U.S. person or an entity that otherwise has significant contacts with the United States.[204] If the answer is yes, the Fourth Amendment safeguards such information because a search conducted within the United States triggers its probable cause requirement. Accordingly, U.S. customers of Data Shard services will likely receive Fourth Amendment protection, while foreign users of these clouds will not.

b. *Data Localization and Data Trusts.* — The Fourth Amendment analysis can be combined for these two network variants, as this constitutional provision is likely to prove of limited applicability for both clouds due to the same factors. An extraterritorial search of data belonging to a non-U.S. person generally does not implicate the Fourth Amendment.[205] In other words, these constitutional protections do not apply to searches of property held in a location outside the United States and owned by a foreign party. Many clients of Data Localization or Data Trust clouds are likely to be non-U.S. persons and, therefore, receive no Fourth Amendment protections.

If a non-U.S. person can meet the *Verdugo-Urquidez* test, however, there may be Fourth Amendment protections for information stored in a Data Localization or Data Trust cloud and searched outside the United States. The *Verdugo-Urquidez* test does not require a warrant, with its heightened requirement of probable cause, for searches outside the United States, but only "reasonableness."[206] Under the Ninth Circuit's approach, which looks to compliance with foreign law in the jurisdiction where the search

---

201. See Minnesota v. Dickerson, 508 U.S. 366, 375 (1993).

202. 232 F. Supp. 3d 708, 721 (E.D. Pa. 2017).

203. Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 551 (2005).

204. United States v. Verdugo-Urquidez, 494 U.S. 259, 270–71 (1990).

205. See id. at 274–75.

206. Id. at 264–65.

occurs, the Data Trustee will only be obliged to comply with search requests that fulfill the requirements of foreign domestic law.[207] As for the Data Manager, like the Data Trustee, it would not reasonably be expected to violate the respective foreign law of trusts to comply with this request. Should this analysis be applied to Microsoft Cloud Germany, U.S. courts that follow the Ninth Circuit are likely to honor the validity of the Data Trust model.

There is less certainty regarding the test shared by the Second and Seventh Circuits.[208] These appellate courts have held that Fourth Amendment reasonableness for extraterritorial searches requires balancing the government's need for the information with the privacy interest at stake.[209] Restricting the analysis to the European Union, the requirements of E.U. and Member States' "data protection" laws demonstrate a strong interest in privacy.[210] E.U. data protection law has a strong anchoring in the constitutional law of the European Union as well as of Member States.[211] For example, there are at least three important foundational expressions of a constitutional right of privacy in the European Union: the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights, and the Treaty on the Functioning of the European Union.[212] There is also important case law regarding information privacy from the European Court of Human Rights and the European Court of Justice.[213]

As a final caution, the analysis here must necessarily be fact specific. If a non-U.S. person or company has sufficient contacts with the United States to be considered part of the U.S. "national community," the Fourth Amendment might apply even to information stored overseas.[214] Such a relationship might be created through physical contacts with the United States or a legal relationship, such as being a resident alien.[215]

c. *Fourth Amendment Summary*. Information stored in a Data Shard cloud will receive Fourth Amendment protections when the data belongs to a U.S. person or a person with significant contacts with the United

207. See United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987).

208. See United States v. Stokes, 726 F.3d 880, 893 (7th Cir. 2013); United States v. Maturo, 982 F.2d 57, 61 (2d Cir. 1992).

209. See *Stokes*, 726 F.3d at 893; *Maturo*, 982 F.2d at 61.

210. The European Union, like most of the rest of the world, refers to its information privacy law as "data protection law." Daniel Solove & Paul M. Schwartz, Privacy Law Fundamentals 31 (4th ed. 2017) [hereinafter Solove & Schwartz, Privacy Law Fundamentals].

211. Schwartz & Peifer, Transatlantic Data Privacy, supra note 2, at 122–27.

212. Consolidated Version of the Treaty on the Functioning of the European Union art. 16, May 9, 2008, 2008 O.J. (C 115) 47; Charter of Fundamental Rights of the European Union art. 8(1), Dec. 18, 2000, 2000 O.J. (C 364) 1; Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter the European Convention on Human Rights].

213. See Schwartz & Peifer, Transatlantic Data Privacy, supra note 2, at 122–29.

214. United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990).

215. See id. at 270–71.

States. In contrast, non-U.S. users of such clouds will not receive Fourth Amendment protection. Information stored in extraterritorial Data Localization and Data Trust clouds is likely to fall outside the reach of the Fourth Amendment, though the required analysis must be fact specific.

2. *The SCA*. — This Article has already examined how judges interpreted the (old) SCA in *Microsoft Ireland* and *Google Pennsylvania*.[216] The SCA forms part of the Electronic Communication Privacy Act (ECPA), which supplies the current framework for federal surveillance law.[217] Enacted in 1986, the SCA is the most important part of ECPA for international clouds; it regulates access to certain kinds of communication, namely "stored wire and electronic communications and transactional records," when in "electronic storage," which is where cloud data spends most of its life cycle.[218] With *Microsoft Ireland* before the Supreme Court, however, Congress acted "in this brave new world" and amended the statute, as Justice Ginsburg had recommended.[219]

The relevant architecture of the SCA, both pre– and post–CLOUD Act, can be quickly summarized. Section 2702 limits the disclosure of stored communications by service providers except for certain listed exceptions.[220] Section 2703 establishes the conditions under which the government may require a service provider to disclose the content of communications covered by the SCA.[221] Finally, the SCA requires warrants to be issued under Rule 41 of the Federal Rules of Criminal Procedure.[222]

What changed with the enactment of the CLOUD Act? Primarily, this statute largely flattens the potential for disparate treatment of different kinds of clouds.[223] Some subtle differences do still remain, however, and the necessary judicial analysis for contested data requests will be highly fact specific. Three initial points demonstrate how the CLOUD Act has changed the SCA.

First, the CLOUD Act makes clear that the reach of the SCA is international.[224] As discussed earlier, the Second Circuit in *Microsoft Ireland*

---

216. See supra section I.A.

217. For an overview, see Solove & Schwartz, Privacy Law Fundamentals, supra note 210, at 69–74.

218. See Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012). For an overview of this statute, see Orin S. Kerr, Computer Crime Law 675–83 (4th ed. 2017).

219. Transcript of Oral Argument, supra note 152, at 6; see also CLOUD Act, H.R. 1625, 115th Cong. div. V (2018).

220. See 18 U.S.C. § 2702.

221. See id. § 2703.

222. See id.

223. See H.R. 1625 div. V, § 103(a)(1) (mandating that service providers comply with the SCA regardless of where their information is stored).

224. See id.

answered this previously open issue about SCA warrants in the negative,[225] and the magistrate judge in *Google Pennsylvania*—as well as judges in a few other courts—answered it in the affirmative.[226] The CLOUD Act then amended the SCA by requiring electronic communication service providers to comply with its provisions "regardless of whether such communication, record, or other information is located within or outside of the United States."[227] The critical test is whether the covered information is "within such provider's possession, custody, or control."[228] The language of "possession, custody, or control" echoes that required, of course, for a subpoena pursuant to the Federal Rules of Civil Procedure's Rule 45.[229] In short, Congress has made it clear that SCA warrants have an international reach. This part of the statute can be viewed as Step One; it takes effect immediately.

Second, the CLOUD Act includes two comity provisions, one general and one specific, which are both of great importance to cloud providers. The general one, discussed in section 103(c), takes effect as part of the statute's Step One.[230] As for the specific comity clause, it creates a new process for executive agreements with "qualifying foreign governments," along with accompanying new safeguards for cloud providers.[231] This is the statute's Step Two, and it only takes effect once there are such executive agreements.[232] No such agreements are in place, but relevant negotiations are underway between the United States and the United Kingdom.[233] These amendments to the SCA regarding comity break important new ground; their importance for future legal access to the global cloud cannot be overstated. As Daskal noted, "no comity claim [had] ever been invoked in connection with an SCA warrant" prior to the CLOUD Act.[234] That state of affairs is now destined to change.

To qualify for an executive agreement, a foreign nation must provide protections to their cloud providers that are similar to those speci-

225. See 829 F.3d 197, 201 (2d Cir. 2016) ("Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas.").

226. See 232 F. Supp. 3d 708, 717 (E.D. Pa. 2017) (holding that SCA warrants can request information stored internationally); see also supra note 17.

227. H.R. 1625 div. V, § 103(a)(1) (adding 18 U.S.C. § 2713).

228. Id.

229. See Fed. R. Civ. P. 45. For a discussion of the scope of a subpoena served pursuant to Rule 45, see Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 147 (S.D.N.Y. 2011).

230. See H.R. 1625 div. V, § 103(c).

231. Id. § 103(b) (adding 18 U.S.C. § 2713(h)).

232. See id. (defining a "qualifying foreign government" as one "with which the United States has an executive agreement").

233. See Statement of Rep. Goodlatte, supra note 28, at 2–3.

234. Jennifer Daskal, *Microsoft Ireland*, the CLOUD Act, and International Lawmaking 2.0, 71 Stan. L. Rev. Online 9, 12 (2018), https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/04/71-Stan.-L.-Rev.-Online-9-Daskal.pdf [https://perma.cc/C8PQ-HA9D] [hereinafter Daskal, International Lawmaking 2.0].

fied under the CLOUD Act. Once a nation qualifies under this statutory provision, a cloud provider may seek to quash a disclosure request for a customer who is not a U.S. person or a U.S. resident and for whom the disclosure of data "would create a material risk that the provider would violate the laws of a qualifying foreign government."[235] The CLOUD Act then spells out a detailed blueprint for the ensuing comity analysis.[236]

Beyond the specific comity clause, and as noted above, the SCA also has a general comity provision for countries without an executive agreement.[237] This provision is tucked away in a short subsection of the statute labeled "Rule of Construction."[238] Presciently, the authors of the CLOUD Act seemed to realize that an international extension of the SCA would bring more cloud providers into conflict with national law. Hence, the statute makes it clear that "comity analysis" pursuant to "common law standards" is available for SCA orders issued extraterritorially in instances in which no executive agreement exists with the target country.[239] The Restatement (Third) of Foreign Relations has the most influential expression of these common law standards.[240]

As an illustration, consider a foreign cloud provider in Freedonia, a fictional country, faced with a data request about a Freedonian citizen but without a qualifying agreement with the United States.[241] Indeed, to develop the hypothetical further, Freedonian law limits these kinds of data transfers to the United States due to privacy considerations and imposes strong penalties on domestic providers that violate its law. The result? Through a motion in a U.S. court, a cloud provider in Freedonia could seek to quash the SCA warrant by raising the issue of comity.[242] In the Congressional Research Service's reading of this venerable doctrine, it notes,

> Common law comity principles generally dictate that U.S. legal obligations can be avoided as a result of foreign law only when the person or entity in question acted in good faith to avoid the conflict, but there remains a likelihood of severe sanctions in the foreign nation for failure to comply with foreign law.[243]

---

235. H.R. 1625 div. V, § 103(b) (adding 18 U.S.C. § 2713(h)(2)(A)(ii)).

236. Id. (adding 18 U.S.C. § 2713(h)(2)(B)–(5)).

237. Id. § 103(c).

238. Id.

239. Id.

240. See Restatement (Third) of the Foreign Relations Law of the United States § 442(1) (Am. Law Inst. 1987).

241. See Duck Soup (Paramount Pictures 1933) (referencing the national song of "Freedonia": "Hail, hail Freedonia").

242. See H.R. 1625 div. V, § 103(c).

243. Stephen P. Mulligan, Cong. Research Serv., R45173, Cross-Border Data Sharing Under the CLOUD Act 10 (2018), https://fas.org/sgp/crs/misc/R45173.pdf [https://perma.cc/8T6T-BA9N].

As will be discussed below, some companies in the European Union have met this test in resisting discovery requests in the context of U.S. civil litigation.[244] Thus, the CLOUD Act both extends extraterritoriality to the SCA and gives foreign providers new paths for contesting SCA warrants.

Finally, the CLOUD Act lifts ECPA's blocking provisions for U.S. cloud providers. Prior to amendment, the SCA's § 2702 prevented foreign governments from directly acquiring the contents of electronic communications.[245] This aspect of the law meant foreign governments used MLATs or letters rogatory when seeking the U.S. government's assistance in obtaining disclosure.[246] The new law amends § 2702 by adding language that permits disclosure to a qualifying foreign government, which is, as noted above, one that signs an executive agreement with the United States.[247] In addition to dropping ECPA's previous prohibition on disclosure to foreign governments, the CLOUD Act immunizes cloud providers who comply with such foreign governmental requests from civil or criminal penalties in the United States.[248]

a. *Data Shards.* — With the enactment of the CLOUD Act, an SCA warrant can be used to compel a request for information stored extraterritorially but accessed within the United States. At least in this context, the Data Shard model no longer raises the danger of law enforcement going dark. Location of data outside the United States does not place a cloud provider and its servers outside the reach of the SCA.

At the same time, however, the amended SCA now provides Data Shard clouds with explicit protections for their foreign customers. First, under the specific comity provision of the CLOUD Act, a Data Shard cloud can contest requests for data of non-U.S. persons if compliance with the SCA warrant would violate the law of a "qualifying foreign government."[249] Second, in the absence of such a qualifying executive agreement, a Data Shard cloud can make use of the general comity provisions when compliance with an SCA request would similarly violate foreign law.[250]

Under the resulting comity analysis, a Data Shard cloud accessed in the United States may receive somewhat less protection than other kinds

244. See infra section III.B.

245. See 18 U.S.C. § 2702(a)(3) (2012) ("[A] provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity.").

246. See Swire & Hemmings, Mutual Legal Assistance, supra note 62, at 694–96 (discussing how sovereign nations seek evidence using MLATs or letters rogatory).

247. See H.R. 1625 div. V, § 104(2)(A)(i)(II) (adding 18 U.S.C. § 2702(b)(9)).

248. See id. § 104(3)(B)(i)–(ii) (amending 18 U.S.C. § 3124(d)–(e)).

249. Id. § 103(b) (adding 18 U.S.C. § 2713(h)).

250. Id. § 103(c) (stating that common law continues to apply when there is no executive agreement).

of clouds that are extraterritorial. This result follows both under general and specific comity analyses.[251] For a non-U.S. person in a country with a qualifying agreement, one factor in the CLOUD Act calls for assessment of "the nature and extent of the provider's ties to and presence in the United States."[252] A Data Shard cloud run by a U.S. provider who accesses stored data in the United States arguably has strong ties to this country; this factor would weigh in favor of upholding an SCA warrant for the cloud data of the non-U.S. person. A similar comity factor exists under the common law test established by the Restatement (Third) of Foreign Relations.[253] A provider's connection to the United States, however, is only one of eight factors (under the CLOUD Act's specific provision)[254] or five (under the Restatement),[255] respectively.

Moreover, as the Congressional Research Service notes, the comity analysis "is likely to be a highly fact-specific evaluation that depends on the specific circumstances of a demand for data stored overseas."[256] For example, in addition to ties to and presence in the United States, other factors assess the importance of the sought-after information to the investigation as well as the "interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure."[257] A court may well order compliance with an SCA warrant for any of the three kinds of clouds in cases in which timely and effective access to the information bears on a matter of great significance.[258]

b. *Data Localization.* — The CLOUD Act makes it clear that the SCA now extends to both complete and partial Data Localization clouds. Similar to the law's treatment of Data Shard clouds, the law also provides these clouds with a path to quash SCA warrants. In the resulting comity analysis, a critical factor concerns a provider's "ties to and presence in" the United States.[259] Under this factor, the law grants a complete Data Localization cloud some level of increased protection compared to a partial Data Localization cloud, like the one involved in the *Microsoft Ireland* case. In that latter cloud model, the information is located abroad, but a service provider can access it from within the United States.[260] The partial

---

251. See id. § 103(b)–(c).

252. Id. § 103(b) (adding 18 U.S.C. § 2713(h)(3)(E)).

253. The third factor in this test looks to "whether the information originated in the United States." Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c) (Am. Law Inst. 1987).

254. See H.R. 1625 div. V, § 103(b) (adding 18 U.S.C. § 2713(h)(3)(A)–(H)).

255. See Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c).

256. Mulligan, supra note 243, at 10.

257. H.R. 1625 div. V, § 103(b) (adding 18 U.S.C. § 2713(h)(3)(A)).

258. See id. (adding 18 U.S.C. § 2713(h)(3)(G)).

259. Id. (adding 18 U.S.C. § 2713(h)(3)(E)).

260. See supra notes 83–85 and accompanying text for a discussion of the partial Data Localization cloud at issue in *Microsoft Ireland*.

Data Localization cloud has stronger ties to and presence in the United States than does a complete Data Localization cloud located outside this country.[261]

c. *Data Trusts.* — Like Data Shard and Data Localization clouds, Data Trusts are now subject to SCA requests. After all, the law now applies regardless of whether sought-after information "is located within or outside of the United States."[262] But cloud providers involved with a Data Trust are afforded a new kind of insulation from U.S. data requests. This result follows because Data Trust clouds split access to customer data from the management of it.[263]

Because the CLOUD Act covers only data within a provider's "possession, custody, or control,"[264] Data Trust cloud providers can leverage their split access-management structure for their benefit. A party running a Data Trust cloud will have a strong defense under this standard, whether as a legal or as a technical matter. Its argument will be that it may have "possession, custody, or control"[265] of encrypted 1s and 0s, but not of the underlying information that these encoded data represent.[266] Moreover, this party has entered into a trust agreement under which it has promised not to seek access to the information. By separating access to the data from management of the servers, this service model permits U.S. cloud providers to run non-U.S. clouds while avoiding the entangling statutory question as to whether they possess, have custody of, or control the information. Thus, the cloud provider will likely be on solid ground in referring SCA requests to the Data Trustee. In turn, the Data Trustee will be governed, in the first instance, by the law of the non-U.S. jurisdiction of the cloud in question.[267] In the United States, the law will then evaluate a Data Trustee's refusal to comply under the same comity analysis as for the provider who runs a complete Data Localization cloud.

d. *SCA Summary.* — All three cloud models now fall within the scope of the SCA. To a large extent, moreover, the CLOUD Act ensures that the law treats different kinds of clouds in a generally similar fashion. All three cloud models are now subject to SCA requests. In addition, a foreign customer of a Data Shard cloud or partial Data Localization cloud no longer faces weaker rights under the SCA because of the cloud provider's ability to access her data from within the United States.

Nonetheless, the CLOUD Act creates an opening for a comity analysis that treats these cloud models differently. If a Data Shard cloud is

---

261. See H.R. 1625 div. V, § 103(b) (adding 18 U.S.C. § 2713(h)(3)(E)).

262. Id. § 103(a)(1) (adding 18 U.S.C. § 2713).

263. See supra notes 89–99 and accompanying text (discussing how the Microsoft Data Trust model operates in Germany).

264. H.R. 1625 div. V, § 103(a)(1) (adding 18 U.S.C. § 2713).

265. Id.

266. See supra notes 89–99 and accompanying text.

267. See H.R. 1625 div. V, § 103(c).

located within the United States, its "ties to and presence in" this country will be a factor weighing in favor of compliance with an SCA warrant.[268] As for Data Localization clouds, comity analysis will favor upholding an SCA warrant for a complete Data Localization cloud, one in which the data are located *outside* the United States and are accessible only *outside* this country. In that case, the provider's "ties to and presence in" the United States are weaker.[269]

Finally, of the three models, a Data Trust cloud has a different kind of insulation from extraterritorial use of the SCA. The provider can argue that it does not meet the statutory threshold of being a party with "possession, custody, or control."[270] Under the Data Trust model, the cloud provider will likely be able to direct such requests to the Data Trustee, who will reference the non-U.S. law of the jurisdiction where the respective cloud is located when responding to the request. Under the resulting comity analysis, a U.S. court is likely to treat the Data Trustee in a similar fashion to a provider running a complete Data Localization cloud. As a final caveat, one should note that comity analysis, whether general or specific, looks to other factors, such as the penalties following in a foreign jurisdiction for compliance with the order and the importance of the sought-after data to an investigation or litigation.[271]

3. *MLATs.* — A long-established way for the U.S. government to access private information held abroad is through Mutual Legal Assistance Treaties. These agreements permit a public authority seeking data to ask for the assistance of the country in which the data is held and require that country to cooperate in processing such requests under its domestic law.[272] MLATs establish legal mechanisms for cooperation between signatory nations in criminal matters and proceedings, including the exchange of evidence and information during criminal proceedings.[273]

Even with enactment of the CLOUD Act, the MLAT process remains relevant. First, the data requests of U.S. law enforcement may fall outside the SCA, which regulates access to "stored wire and electronic communications and transactional records" when in "electronic storage."[274] Thus, *Microsoft Ireland* concerned the U.S. government's attempt to obtain access to emails.[275] The SCA also covers information that is uploaded to and stored with cloud providers, who will generally fall under

---

268. See id. § 103(b) (adding 18 U.S.C. § 2713(h)(3)(E)).

269. See id.

270. See id. § 103(a)(1) (adding 18 U.S.C. § 2713).

271. See id. § 103(b) (adding 18 U.S.C. § 2713(h)(3)(A)–(H)); Restatement (Third) of the Foreign Relations Law of the United States 442(1)(c) (Am. Law Inst. 1987).

272. See Mutual Legal Assistance Treaties, supra note 62.

273. For an overview, see Swire & Hemmings, Mutual Legal Assistance, supra note 62, at 696–700.

274. 18 U.S.C. § 2701.

275. See 829 F.3d 197, 200–01 (2d Cir. 2016).

its two idiosyncratic legislative terms of art, "electronic communication service" (ECS) or "remote computing service" (RCS), and hence will be covered by this statute.[276] Yet, post–CLOUD Act amendment, the SCA still does not cover a variety of information that a business has gathered for its own purposes about its customers.

It is now common for companies to track and create profiles of their customers, clients, or users. In doing so, these entities are not acting as an ECS or RCS and do not fall within the SCA. MLATs do reach such data; as one summary noted, "MLATs generally obligate nations to summon witnesses, compel the production of documents and other evidence, issue warrants, and serve process."[277]

Second, while this law foresees development of a new system of international data sharing around executive agreements, there are no such arrangements currently in place. Hence, foreign governments are still obligated to use the MLAT process when they seek data from the United States. Indeed, there has been a dramatic increase in the number of requests from foreign countries to the Department of Justice for assistance in obtaining data and other evidence in the United States.[278] In short, MLATs remain important—and they also come in many different forms.

MLATs can be bilateral, multilateral, regional, and country-to-regional. According to one estimate, "[t]here are hundreds of bilateral MLATs" throughout the world.[279] For example, the United States has MLATs in place with numerous E.U. Member States and with the European Union itself.[280] Building on the E.U.–U.S. MLAT, these two entities also signed an Umbrella Agreement in June 2016 to increase law enforcement cooperation while setting "high standards for the protection of personal data transferred by law-enforcement authorities."[281]

The use of MLATs has been widely criticized, however, as time-consuming and inefficient. The district court in *Microsoft Ireland* singled it out as impractical.[282] Woods also speaks of the "extremely long time" that an MLAT request typically takes to complete.[283] He notes: "The entire

276. 18 U.S.C. § 2711(2), (3)(A)(ii).

277. Mulligan, supra note 243, at 13.

278. Id. at 15.

279. Woods, supra note 3, at 748.

280. See Country Profile: United States, Mutual Legal Assistance Treaties, https://mlat.info/country-profile/united-states [https://perma.cc/V5YL-KKDJ] (last visited July 26, 2018).

281. European Commission Press Release STATEMENT/16/2040, Joint EU–U.S. Press Statement Following the EU–U.S. Justice and Home Affairs Ministerial Meeting (June 2, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-2040_en.htm [https://perma.cc/PN5B-DJJM].

282. See In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 474–75 (S.D.N.Y. 2014).

283. Woods, supra note 3, at 749.

process has been estimated to take an average of ten months, and in some cases can take much longer."[284] In testimony before Congress, Christopher Kelly, Assistant Attorney General of Massachusetts, flatly stated that the "MLAT process . . . is not a viable solution" to the problem of law enforcement access to international cloud data.[285]

a. *Data Shards.* — Analysis regarding the Data Shard cloud is clear: The MLAT process is irrelevant because courts will consider the locus of the search to be domestic in nature. In fact, the MLAT process is also likely to be considered irrelevant for another reason. As Magistrate Judge Rueter noted in *Google Pennsylvania*, information in this cloud model is constantly shifting from country to country.[286] Hence, in language regarding going dark that this Article has already cited, Magistrate Judge Rueter noted that "no one knows which country to ask, and even if specific servers could be identified, the data may no longer be there by the time its location has been identified."[287] While the CLOUD Act makes it clear that the SCA extends extraterritorially, the statute does not cover all possible requests for information.[288] Hence, the problem of going dark might still arise: A request to a Data Shard cloud pursuant to the MLAT process, as opposed to the domestic U.S. process, would be stymied due to an inability to identify the foreign government to which a data request should be made.

b. *Data Localization.* — Information requests to a Data Localization cloud under the MLAT process would proceed under specific national and regional agreements. For Europe, moreover, the 2016 Umbrella Agreement between the European Union and the United States establishes additional protections before E.U. law enforcement agencies can give data to U.S. law enforcement agencies.[289] This Agreement does not provide a new substantive basis for such exchanges, which would continue to be governed by the law of the E.U. Member State to which

---

284. Id.

285. See Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation & Protecting Rights: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary, 115th Cong. 5 (2017) (statement of Christopher W. Kelly, Assistant Att'y Gen., Office of the Mass. Att'y Gen.). On a more positive note, a Review Group under the Obama Administration proposed important ways to improve the MLAT process, including by increasing resources to the office in the Department of Justice that is responsible for MLAT requests. See President's Review Grp. on Intelligence & Commc'ns Techs., Liberty and Security in a Changing World 226–28 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [https://perma.cc/Q42J-NMFP].

286. See 232 F. Supp. 3d 708, 724–25 (E.D. Pa. 2017).

287. Id. at 725.

288. See supra text accompanying notes 249–250.

289. See Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, E.U.-U.S., June 2, 2016, T.I.A.S. No. 17-201 (entered into force Feb. 1, 2017) [hereinafter Umbrella Agreement].

the information request is directed. Rather, it makes such transfers subject to an overarching set of principles, which are also found in that same year's Privacy Shield agreement with the United States.[290] Specifically, the principles include limitations on data use, a right to access and rectification of information, and judicial redress before U.S. courts should U.S. authorities fail to comply with its requirements for access or rectification.[291]

c. *Data Trusts.* — Under the Data Trust model, an MLAT request would be directed to the Data Trustee, not the service provider. Only the former would have the technical ability to access the information as well as the legal authority to do so under the binding local trust arrangement. Significantly, the Data Trust arrangement would reduce any ambiguity as to whether an information request by U.S. law enforcement was occurring extraterritorially. It would make it clear that the *location* of the data was outside the United States and the *search* of the data was also extraterritorial in nature.

To explore how such MLAT access would proceed, we can consider the Microsoft Cloud Germany. Were U.S. law enforcement to seek data in Germany stored in this network that was not covered by the SCA, it would turn to T-Systems, the Data Trustee, pursuant to the U.S.–Germany treaty on Mutual Legal Assistance in Criminal Matters.[292] Article 12(1) of the U.S.–Germany MLAT foresees the use of "surveillance of telecommunications" as a justification for an extraterritorial data request.[293] At the same time, however, the law of the "Requested State"—namely, Germany—"governing criminal investigations or proceedings" would apply to such a request.[294] This language means that a request by U.S. law enforcement for information stored in the German cloud would be judged according to German Criminal Procedure Law (StPO).[295] Between the protections of E.U. Member State law and those of the Umbrella Agreement, the MLAT process provides strong safeguards for users of E.U.-stored data.

d. *MLAT Summary.* — Under the three cloud management models, different results occur when data requests are made pursuant to MLATs. First, Data Shard clouds are not likely to implicate MLATs as the data request will be considered purely domestic. Second, Data Localization

---

290. See id. The Umbrella Agreement's protections generally track those of the Privacy Shield. For an overview of the Privacy Shield, see Solove & Schwartz, Information Privacy Law, supra note 35, at 1187–97.

291. Umbrella Agreement, supra note 289, arts. 5(2), 6.

292. See Treaty Between the United States of America and the Federal Republic of Germany on Mutual Legal Assistance in Criminal Matters, Ger.-U.S., Oct. 14, 2003, art. 1(1), T.I.A.S. No. 09-1018; Microsoft Cloud Germany Datasheet, supra note 89, at 1.

293. Treaty Between the United States of America and the Federal Republic of Germany on Mutual Legal Assistance in Criminal Matters, supra note 292, art. 12(1).

294. Id. art. 19(1).

295. For a discussion, see Schwartz & Peifer, Data Fiduciary Model, supra note 88, at 165.

clouds in the European Union will have strong protections against U.S. data requests under the Umbrella Agreement and E.U. Member State law. Third, MLATs are likely to remain relevant to foreign governments in the absence of executive agreements pursuant to the CLOUD Act. Finally, MLAT requests for information in a Data Trust model will be made to a Data Trustee, the party with the sole ability to control access to the information.

4. *Administrative or Grand Jury Subpoenas.* — U.S. law permits the government to issue a subpoena to a company that engages in business *inside* the United States for property under its control that is located *outside* the United States.[296] Unlike a warrant, a governmental subpoena is issued without judicial involvement. For example, the Eleventh Circuit in its *Bank of Nova Scotia* decision upheld a subpoena authorizing disclosure of the banking records of U.S. citizens that a Canadian bank with U.S. branches had maintained in the Bahamas.[297] The Eleventh Circuit held that the bank had to release the records, even though disclosure would violate Bahamian law.[298] Thus far, no case has applied the *Bank of Nova Scotia* rule to data stored by cloud providers on behalf of third parties.

Regarding such extraterritorial subpoena requests, case law distinguishes between (1) records that a party to litigation holds and (2) records that an entity holds on behalf of another party. In some cases, a subpoena recipient is "asked to turn over records in which only *they* have a protectable privacy interest."[299] For example, in *Marc Rich & Co.*, the Second Circuit "permitted a grand jury subpoena issued in a tax evasion investigation to reach the overseas business records of a defendant['s] Swiss commodities trading corporation."[300] The subpoena in *Marc Rich & Co.* was directed to a corporation for its own overseas records. The *Marc Rich & Co.* court found that the grand jury had jurisdiction over the corporation under the "territorial principle"; this concept permits governments to punish individuals or entities for acts outside their boundaries when such acts are "intended to produce and do produce detrimental effects within it."[301]

In contrast, a foreign-based entity that holds records on behalf of another party is generally considered to have a stronger interest against

---

296. See In re Grand Jury Subpoena to Marc Rich & Co., A.G., 707 F.2d 663, 667 (2d Cir. 1983) (articulating the long-standing rule that if the recipient of a grand jury subpoena is within the court's personal jurisdiction, responsive materials within the subpoena recipient's control must be produced regardless of where they are kept).

297. See In re Grand Jury Proceedings Bank of N.S., 740 F.2d 817, 818 (11th Cir. 1984). For a similar holding, see United States v. Vetco, Inc., 691 F.2d 1281, 1287–91 (9th Cir. 1981) (enforcing Internal Revenue Service summonses against Swiss subsidiaries of American firms).

298. See *In re Bank of N.S.*, 740 F.2d at 826–28.

299. *Microsoft Ireland*, 829 F.3d 197, 221 (2d Cir. 2016).

300. Id. at 215 (discussing *In re Marc Rich & Co.*, 707 F.2d 663).

301. *In re Marc Rich & Co.*, 707 F.2d at 666.

extraterritorial subpoenas than a non-U.S. entity that is a party to the underlying litigation in the United States. This distinction is generally supported by a Department of Justice policy expressed in a December 2017 memorandum concerning data requests to an entity that stores data in the cloud. The Computer Crime and Intellectual Property Section summarized the relevant policy as follows: "[P]rosecutors should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation."[302]

When a subpoena is contested by a non-U.S. party, a U.S. court will evaluate the merits of the matter through a comity analysis. The U.S. Supreme Court has defined comity as the "spirit of cooperation in which a domestic tribunal approaches the resolution of cases touching the laws and interests of other sovereign states."[303] It is a concept of "judicial self-restraint in furtherance of policy considerations which transcend individual lawsuits."[304] As this Article has already noted in regards to the CLOUD Act's introduction of comity into ECPA, the resulting analysis will be highly fact specific.[305] For example, as the Texas Supreme Court stated in recognizing the importance of this principle, comity requires careful examination of "[t]he circumstances of each situation."[306]

The leading test for comity is found in the Restatement (Third) of Foreign Relations Law.[307] It contains a five-factor analysis, which looks to:

> [1] [T]he importance to the investigation or litigation of the documents or other information requested; [2] the degree of specificity of the request; [3] whether the information originated in the United States; [4] the availability of alternative means of securing the information; and [5] the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.[308]

---

302. Comput. Crime & Intellectual Prop. Section, Criminal Div., U.S. Dep't of Justice, Seeking Enterprise Customer Data Held by Cloud Service Providers 1 (2017), https://www.justice.gov/criminal-ccips/file/1017511/download [https://perma.cc/L38Z-838B].

303. Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court, 482 U.S. 522, 543 n.27 (1987); see also id. at 555 (Blackmun, J., concurring in part and dissenting in part) ("Comity is . . . a principle under which judicial decisions reflect the systemic value of reciprocal tolerance and goodwill.").

304. Volkswagenwerk Aktiengesellschaft v. Superior Court, 176 Cal. Rptr. 874, 884 (Cal. Ct. App. 1981).

305. See supra section II.A.2.

306. Gannon v. Payne, 706 S.W.2d 304, 307 (Tex. 1986).

307. See Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c) (Am. Law Inst. 1987).

308. Id.

Some courts, such as the Ninth Circuit, have expanded the required analysis by adding additional factors.[309] A comity analysis is also common when private parties seek information as part of litigation in the United States. This point is discussed in more detail below in section II.B.2.

a. *Data Shards.* — When a subpoena is presented to a company managing a Data Shard cloud, the result is likely to be straightforward. For a U.S. court, a foreign jurisdiction is likely to lack a justifiable foreign relations interest in the information request to a Data Shard cloud.[310] Hence, a comity analysis is likely to be unnecessary, and a subpoena issued to a Data Shard cloud would be considered domestic in nature. After all, the locus of storage of information is unknown to the user and can shift by the time a data request is made and the information is to be retrieved.[311]

b. *Data Localization.* — A cloud provider generally holds information on behalf of a third party. In *Microsoft Ireland*, a case about the reach of the SCA's *warrant* power, the Second Circuit indicated in dicta that it did not think that a *subpoena* should be used to order such information when held outside the United States. The court noted it had "never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item."[312]

Other circuits have ruled differently regarding custodial records found overseas when the holding entity was a bank.[313] As the Restatement (Third) of Foreign Relations concisely summarizes, "United States courts have disagreed on the obligations of non-party custodians, such as banks and brokers, with offices in the United States and foreign states."[314] After acknowledging such decisions in other circuits upholding subpoenas for

---

309. See Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992) (listing other relevant factors as "the extent and the nature of the hardship that inconsistent enforcement would impose upon the person, . . . [and] the extent to which enforcement by action of either state can be reasonably expected to achieve compliance with the rule prescribed by that state" (alterations in original) (internal quotation marks omitted) (quoting United States v. Vetco, Inc., 691 F.2d 1281, 1288 (9th Cir. 1981))).

310. See *Google Pennsylvania*, 232 F. Supp. 3d 708, 722–25 (E.D. Pa. 2017) (stating that "[n]o foreign nation's sovereignty will be interfered with in any ascertainable way" when a search pursuant to an SCA warrant will be conducted in the United States); see also In re Search of Info. Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757 (GMH), 2017 WL 2480752, at *6–11 (D.D.C. June 2, 2017) (holding that in light of international comity, an SCA warrant for information in Google's Data Shard cloud is a permissible domestic application of the SCA).

311. See supra notes 66–69 and accompanying text.

312. *Microsoft Ireland*, 829 F.3d 197, 215 (2d Cir. 2016).

313. See id. at 216 & n.26 (collecting cases).

314. Restatement (Third) of the Foreign Relations Law of the United States § 442 cmt. h (Am. Law Inst. 1987).

overseas bank records, the *Microsoft Ireland* court drew a distinction between banks and cloud providers.[315] For the Second Circuit, it had been long established that bank customers do not have a privacy interest in their records that blocks subpoenas.[316] It pointed to *United States v. Miller*, a 1976 Supreme Court decision that found such records, for purposes of Fourth Amendment analysis, to be the bank's "business records" and not the "private papers" of the depositors.[317]

In 2018, however, the Supreme Court in *Carpenter v. United States* left *Miller* intact but created a new rule for "the rare case where the suspect has a legitimate privacy interest in records held by a third party."[318] The Court found such an interest existed in "a detailed log of a person's movements over several years" and, in particular, in cell-site records.[319] In the future, courts, like the Second Circuit in *Microsoft Ireland*, are likely to explore the distinction between banks-as-custodians and cloud-providers-as-custodians.[320] Accordingly, much here will depend on how U.S. courts carry out their comity analysis.

c. *Data Trusts.* — Compared to a Data Localization cloud, a Data Trust cloud provides greater protection from subpoena requests. Pursuant to the law of the relevant jurisdiction, only the Data Trustee will be authorized to access data stored in this kind of cloud. Here, the question of control becomes important. Under applicable U.S. law, the sought-after information must be "subject to the recipient's custody or control."[321] To give a concrete example, Microsoft Germany will be able to make a strong argument that information in its German cloud is not under its "custody or control." Under the terms of its trust, only the Data Trustee (a third party) can access the information necessary to respond to subpoena requests.[322]

Moreover, as a technical matter, the Data Trustee controls the actual access to the data, which means that Microsoft Germany, as the cloud provider, cannot even view customer data in its cloud. In deciding this issue of control, courts have looked to the question of whether an entity

315. See 829 F.3d at 216.

316. Some restrictions on the access to and use of bank records are provided by statutory law, such as the federal Bank Secrecy Act, 31 U.S.C. §§ 5311–5332 (2012).

317. See *Microsoft Ireland*, 829 F.3d at 216 (citing United States v. Miller, 425 U.S. 435, 440–41 (1976)).

318. 138 S. Ct. 2206, 2222 (2018).

319. Id.

320. On the continuing validity of the Third-Party Doctrine in garden-variety warrants for bank records, see Presley v. United States, 895 F.3d 1284, 1291 (11th Cir. 2018) (noting that *Miller* precludes finding a "reasonable expectation of privacy" in business records held by a bank).

321. *Microsoft Ireland*, 829 F.3d at 201.

322. See supra note 88 and accompanying text.

has the "practical ability" to obtain a document.[323] Microsoft Germany has a strong argument that because it lacks such capacity, the subpoena cannot compel it to act.

A subpoena issued to T-Systems, the Data Trustee, raises different issues. Here, there is a party with "custody or control." A U.S. court might consider whether such a Data Trustee is similar to or distinguishable from an overseas bank holding U.S. customer records. Arguably, notable distinctions can be drawn between this entity and a bank. A bank manages the financial transactions of an individual according to standard processes that render this information as much the business records of the bank as that of the individual.[324] In contrast, a Data Trustee does not carry out business on behalf of its customer in the fashion that a bank does. For example, it does not impose standard formatting requirements on items like checks or wire transfers, and it does not interact with other entities on the customer's behalf, as when a bank executes a wire transfer.[325] The amount and kind of data collected vary greatly based on the customer. And finally, the Data Trustee may even lack knowledge of or ability to access the underlying information if the customer uses her own encryption tools.[326]

At the same time, however, the Third-Party Doctrine provides a plausible counterargument. Under this doctrine, as this Article has discussed, people who voluntarily give information to so-called third parties have no "reasonable expectation of privacy" under the Fourth Amendment.[327] Additionally, the Second Circuit in *Microsoft Ireland* neglected to mention that the Third-Party Doctrine has been applied by the Supreme Court beyond bank records to include—among other kinds of information—telephone records.[328] That said, a Data Trustee is clearly a non-U.S. based entity that holds records on behalf of another party. Hence, it may not

---

323. See, e.g., Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 147–48 (S.D.N.Y. 2011); In re NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007) (discussing how parties are considered to be in control of documents when they can access them).

324. See supra note 317 and accompanying text.

325. See Frank Simorjay, Microsoft, supra note 95, at 6–8 (explaining Microsoft's Data Trustee model in Germany as one in which the trustee's primary role is to control access to customer data by only granting Microsoft access "scoped to a specific service and only for the time necessary to accomplish the permitted purpose" in response to a verified request).

326. In addition to controlling access to customer data, the trustee's other roles and responsibilities in Microsoft's Data Trustee model include incident management, network management, datacenter management, and risk management—none of which involve dictating any parameters of the customer's data. See id. at 8–9.

327. See Solove & Schwartz, Information Privacy Law, supra note 35, at 288–95.

328. See Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that individuals have no expectation of privacy in the numbers they dial because they voluntarily give those numbers to the phone company); Solove & Schwartz, Information Privacy Law, supra note 35, at 288–95 (discussing applications and critiques of the Third-Party Doctrine). For a recent argument concerning the need to narrow the current understanding of the Third-Party Doctrine, see Richards, supra note 192, at 1489.

seem like a classic third party for a U.S. court.[329] Rather, it may fall into another category—one that typically triggers the stronger protections of comity analysis.

d. *Subpoena Authority Summary.* — In the case of a Data Shard cloud, a subpoena will be considered domestic in nature. For a Data Localization cloud, in contrast, precedents about international subpoenas are not conclusive. To further muddy the waters, a cloud holding information for a customer can be distinguished in meaningful ways from a bank or other financial institution. Finally, the Data Trust cloud splits the ability to access information in a network from the ability to manage the cloud server itself. As a result, the party managing the cloud (the cloud service provider) has a strong argument against surrendering data pursuant to a subpoena. And, in turn, the Data Trustee has a strong, but different, argument that it is a mere caretaker of the information.

5. *Statutory Authority for Foreign Surveillance.* — The main statute that governs the U.S. government's foreign intelligence gathering authority is the Foreign Intelligence Surveillance Act (FISA).[330] This statute requires the government to obtain an order from a special court, the Foreign Intelligence Surveillance Court (FISC), when it wishes to gather "foreign intelligence."[331] The government is to make a showing of probable cause that the party to be monitored is a "foreign power" or an "agent of a foreign power."[332] In a roughly analogous structure to the SCA, FISA's Title I and Title III permit court-ordered access to stored content.[333] Laura Donohue refers to these aspects of the statute's pre-9/11 orientation as "traditional FISA."[334]

After 9/11, there were many changes in the government's data collection and analysis in this area. In response, Congress sought both to amend the law to reflect the new practices and to force alterations in some of these operations.[335] Regarding international cloud computing, the most important legal changes are found in provisions of the FISA Amendments Act of 2008 (FAA).[336] The FAA permits the U.S. government to compel service providers in the United States to assist in the

329. The Supreme Court revisited the Third-Party Doctrine in Carpenter v. United States, 138 S. Ct. 2206 (2018). It declared that "[t]he Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations." Id. at 2222.

330. 50 U.S.C. §§ 1801–1885c (2012). One provision of the FISA Amendments Act regulates surveillance outside the United States that targets U.S. persons. See id. § 1881a(b).

331. See id. § 1802(b).

332. Id. §§ 1802, 1805.

333. Id. §§ 1805, 1824.

334. Laura K. Donohue, The Future of Foreign Intelligence 13–15 (2016).

335. For a highly negative account of these practices, see Owen Fiss, A War Like No Other 225–61 (2015).

336. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. §§ 1881–1885c).

"targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[337] If the target is a non-U.S. person, probable cause is not required. Rather, the government must have a reasonable belief that the target's location is outside the United States.[338] Moreover, the activity must be to "acquire foreign intelligence information," which includes information necessary to protect against foreign threats to the national security of the United States.[339]

The acquisition of foreign intelligence information is also subject to significant limits. These include the use of "targeting procedures," which are to be "reasonably designed" to "ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States."[340] The acquisition must also be "conducted only in accordance with" some kind of "minimization procedures" to limit the acquisition, retention, and dissemination of nonrelevant information.[341] Cases under the FAA are rare, and there is no case discussing whether the Act can be used to compel U.S.-based service providers to disclose information stored outside the United States.[342]

The FAA is, in fact, mainly focused on surveillance *inside* the United States. The FAA requires U.S.-based service providers to turn over data on persons *outside* the United States, but it mainly contemplates the disclosure of data stored or otherwise accessible inside the United States. It leaves open the question that *Microsoft Ireland* answered regarding the SCA: Does a statute that is otherwise silent on the issue require U.S.-based service providers to take action with respect to data stored outside the United States? While the Second Circuit resolved that issue for the SCA,[343] there is no public case about its resolution under the FAA.

Beyond FISA and the FAA, Executive Order 12,333 defines—at a high level of generality—the authority of the U.S. government to obtain access to data stored on computers outside the United States.[344] Issued by President Ronald Reagan, this Executive Order establishes the overall framework for U.S. gathering of foreign intelligence. It grants broad authority for the U.S. intelligence community to engage in data collec-

337. 50 U.S.C. § 1881a(a).

338. Id. § 1881a(a)–(b).

339. Id. § 1881a(a), (c)(2). For a discussion, see David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 17:3 (2d ed. 2016).

340. 50 U.S.C. § 1881a(d)(1).

341. See id. § 1881a(c)(1).

342. The USA Freedom Act does require publication of significant FISC opinions. See 50 U.S.C. § 1872. Public opinions of the FISC, as well as public filings before it, are available online at Foreign Intelligence Surveillance Court, Public Filings, http://www.fisc.uscourts.gov/public-filings [https://perma.cc/RX9Y-B538] (last visited Aug. 14, 2018). For an in-depth analysis of the court, see Kris & Wilson, supra note 339, at §§ 5.1–5.7.

343. See *Microsoft Ireland*, 829 F.3d 197, 201 (2d Cir. 2016).

344. Exec. Order No. 12,333, 3 C.F.R. § 200 (1981).

tion.[345] Part 2.3 of the Order permits the collection, retention, and dissemination of the following types of data: "[i]nformation obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation" as well as "incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws."[346]

a. *Data Shards*. — The Data Shard cloud is accessed in the United States, and, hence, will be subject to provisions of FISA and the FAA regarding searches of stored content in the United States. A Data Shard provider will be subject to the same requirements as any other "electronic service provider" under these statutes.

b. *Data Localization*. — FISA and the FAA do not extend to the capture of communications that lack some geographic connection with the United States.[347] Thus, the issue of necessary connection to the United States will be a critical question regarding a Data Localization cloud accessible within the United States. FISA applies only to the acquisition of communications that occur within the United States or when the government is targeting a known U.S. person outside the United States. It appears, therefore, that a Data Localization cloud whose content can be accessed from the United States will fall under FISA. There is no publicly available FISC opinion, however, regarding this issue.

c. *Data Trusts*. — If U.S. intelligence seeks to compel cooperation from a non-U.S. Data Trust cloud under the FAA, it is unlikely to succeed. In such a situation, neither the cloud provider nor the Data Trustee has accessed communications in the United States. Additionally, these parties do not fall within the definition of "an electronic communication service provider" under the Act.[348] Both parties would be considered non-U.S. service providers that are outside the Act's jurisdiction. The U.S. intelligence community also has power to engage in surveillance of information stored electronically pursuant to Executive Order 12,333.[349] Its ability to effectively do so, as under the FAA, will turn on its ability to overcome data security measures, including any use of encryption, provided in a Data Trust cloud.[350]

d. *Foreign Intelligence Summary*. — A Data Shard cloud will be subject to provisions of foreign intelligence surveillance law for searches of stored content within the territory of the United States. Its status is the same as any U.S.-based "electronic service provider." In contrast, a Data

345. Kris & Wilson, supra note 339, at § 17:19.

346. 3 C.F.R. § 200, at pt. 2.3.

347. 2 James G. Carr et al., Law of Electronic Surveillance § 9.13 (2018).

348. See 50 U.S.C. § 1885(6) (2012).

349. See 3 C.F.R. § 200, at pt. 2.3 (listing the types of information that the intelligence community is allowed to collect, retain, or disseminate).

350. Whether the data security will be breakable will turn on a range of security and nonsecurity issues. For a discussion, see Bruce Schneier, Beyond Fear 264–66 (2003).

Localization cloud will be subject to FISA and the FAA only so long as there is a geographic connection with the United States. A Data Localization cloud accessible from the United States will likely fall under the applicable foreign intelligence surveillance statutes. Finally, a Data Trust cloud located outside the United States is not an "electronic service provider" under relevant statutory provisions.

B. *Extraterritorial Discovery by Private Parties*

Thus far, this Article has examined legal authorities enabling governmental demands for data stored in non-U.S. clouds. There are also paths for requests that are made by civil litigants in the United States for such information. In comparison to other jurisdictions, the U.S. discovery process is far-reaching. As the Sedona Conference explains, "U.S. discovery is widely considered to be the broadest and most permissive in the world."[351] Unlike in civil law countries, discovery in the United States is not managed by a judge but is instead largely self-executing by parties to the litigation.[352] As Gil Keteltas observes, "[D]iscovery in U.S. litigation is a right, and key information must be provided to an opponent even without a request from the opponent."[353]

When private parties seek extraterritorial discovery, U.S. discovery law provides two paths: U.S. litigants can seek discovery pursuant to the Hague Convention or through the Federal Rules of Civil Procedure. This Article considers each authority in turn.

1. *The Hague Convention.* — The United States is a signatory to the Hague Evidence Convention, which provides a nonexclusive means of taking evidence in civil and commercial matters.[354] According to the helpful summary of European data protection commissioners, the Hague Convention "provides a standard procedure for issuing 'letters of request' or 'letters rogatory' which are petitions from the court of one country to the designated central authority of another requesting assistance from that authority in obtaining relevant information located within its borders."[355] From the perspective of U.S. litigants, however, the Hague Convention proves to be a flawed method for gathering evidence.

---

351. Sedona Conference, International Overview of Discovery, Data Privacy & Disclosure Requirements 198 (2009), https://thesedonaconference.org/publication/sedona-conference%C2%AE-international-overview-discovery-data-privacy-and-disclosure (on file with the *Columbia Law Review*).

352. Gil Keteltas, US E-discovery, *in* E-discovery and Data Privacy: A Practical Guide 3, 3–6 (Catrien Noorda & Stefan Hanloser eds., 2011).

353. Id. at 6.

354. Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, 847 U.N.T.S. 231.

355. Article 29 Data Protection Working Party, No. 00339/09/EN, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation 6 (Working Paper No. 158, 2009), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf (on file with the *Columbia Law Review*). For a

First, not all E.U. Members are parties to the Hague Convention.[356] Second, many E.U. signatory states filed reservations at the time of ratification that essentially prevent its use as part of pre-trial discovery.[357] These countries include France, Germany, Spain, and the Netherlands.[358] It should be noted, however, that a letters rogatory can also be submitted to countries outside of the Hague Convention and would be subject to general principles of comity.[359]

a. *Data Shards*. — The letters rogatory process, pursuant to the Hague Convention, is not relevant to the Data Shard cloud. After all, access to information in such a cloud is provided exclusively from the United States. As a consequence, courts are likely to consider this information to be located in the United States. In such cases, normal domestic discovery pursuant to the Federal Rules of Civil Procedure will occur.

b. *Data Localization and Data Trusts*. — In the case of Data Localization and Data Trust clouds, a letter requesting evidence will be served from a U.S. court to a judicial authority in the country where the cloud is located. Both Data Localization and Data Trust clouds can be served with these letters. A litigant in the United States seeking discovery might argue, however, that gathering evidence from the U.S. provider running a Data Localization cloud should not require use of the Hague Convention because the provider is directly subject to the Federal Rules of Civil Procedure. This case would be bolstered if the Data Localization cloud was an incomplete one, as in *Microsoft Ireland*, where the non-U.S. data were also technically accessible for the cloud provider from within the United States.[360] A different result is likely if a Data Trust arrangement is at stake. Here, a litigant in the United States would be more likely to use the Hague Convention process and to direct requests solely to the Data Trustee rather than to the cloud provider, who is restricted from accessing the data in the network.

c. *The Hague Convention Summary*. — A Data Shard cloud does not implicate the need for use of letters rogatory. Both Data Localization and Data Trust clouds, in contrast, can fall under the Hague Convention. Moreover, a Data Trust will provide additional protection to its users; it insulates the cloud provider from these data requests and shifts them to the local, non-U.S. Data Trustee.

2. *Federal Rules of Civil Procedure*. — The Federal Rules of Civil Procedure permit discovery of all nonprivileged information relevant to a claim or

---

useful, concise analysis of the letters rogatory process, see Swire & Hemmings, Mutual Legal Assistance, supra note 62, at 702–04.

356. Article 29 Data Protection Working Party, supra note 355, at 6.

357. Id.

358. Id.

359. Swire & Hemmings, Mutual Legal Assistance, supra note 62, at 702.

360. See supra text accompanying note 83.

defense.[361] These rules define "relevancy" broadly.[362] In 2006, Amendments to the Federal Rules included "electronically stored information" as being among the information covered by the "duty to disclose."[363] These amendments also added an explicit balancing test that requires, among other factors, an assessment of "whether the burden or expense of the proposed discovery outweighs its likely benefit."[364]

A distinction must be drawn between discovery directed against a party in litigation and discovery directed at a nonparty that holds data that may be considered relevant (a so-called third party). Generally, a plaintiff or defendant must comply with a discovery request for its own data, regardless of where the data is stored. However, U.S. law also permits discovery directed at third parties. Here, the picture becomes more complicated, as those third parties, such as cloud providers, may be prohibited from disclosing data stored by their users. ECPA flatly prohibits cloud providers from complying with civil discovery requests to disclose the content of data held on behalf of users. Such requests must be served directly on the creator of the records.[365] ECPA does, however, permit cloud providers to disclose customer-identifying information and other metadata in response to civil discovery requests.[366]

As noted above, under *Microsoft Ireland*, the provisions of ECPA prohibiting disclosure of content in response to civil subpoenas do not apply to content stored outside the United States.[367] When parties in the United States seek information located in a foreign country for production as part of civil litigation, courts look to the applicable rules regarding comity. The most influential test for comity in the United States is the Restatement (Third) of Foreign Relations Law. The Restatement sets up a multipart test concerning the necessary comity analysis.[368] This test helps to define limits of a U.S. court's "power to order foreign discovery in the face of objections by foreign states."[369] When parties in the United States seek information located in a foreign country for production in civil litigation, courts invoke the five-factor comity analysis, which includes a balancing of the U.S. court's interest in complying with the discovery request and the risk of undermining "important interests of

361. See Fed. R. Civ. P. 26(b)(1).

362. See Fed. R. Civ. P. 26(b) advisory committee's note to 1970 amendment.

363. See Fed. R. Civ. P. 26(a).

364. Fed. R. Civ. P. 26(b)(1).

365. 18 U.S.C. § 2702 (2012).

366. Id. § 2702(c).

367. See supra section II.A.4.

368. Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c) (Am. Law Inst. 1987).

369. Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court, 482 U.S. 522, 544 n.28 (1987).

the state where the [requested] information is located."[370] Depending on the type of global cloud storing the information and where that information is stored, results for discovery requests can vary drastically.

a. *Data Shards.* — As seen with letters rogatory, a U.S. court is not likely to view a Data Shard cloud—where data is searchable from the United States—as involving a foreign data request. Similarly, a civil litigation request to a Data Shard provider may be treated as subject to the same rules as garden-variety domestic requests. If so, the normal rule of "relevancy" for civil discovery in the United States will apply and not a multifactor comity test.

b. *Data Localization and Data Trusts.* — E.U. data protection law will be important to the comity analysis for Data Localization and Data Trust clouds. In cases in which such discovery requests are contested, litigants from E.U. Member States will typically present U.S. courts with evidence of the fundamental importance of data protection in their legal order.[371] Information privacy in the United States does not have a similar status anchored in fundamental rights, which means a U.S. court may struggle to understand its international relation, namely, data protection law.[372]

In addition to the data protection law of the non-U.S. trustee, a Data Trust outside the United States is safeguarded by the relevant jurisdiction's law of trusts. Such fiduciary relationships, as present between T-Systems and its Microsoft cloud customers, represent an additional, substantive national interest when a court carries out a comity analysis and assesses the balance of interests present in the matter before it. In such cases, a Data Trust cloud will be able to claim that a foreign discovery request would harm "important interests of the state."[373]

A final issue regards the distinction between a discovery request made to a party to the underlying litigation and one made to a third party with control over that information. This distinction is important for international discovery requests made pursuant to subpoenas.[374] The use of a Data Trust cloud creates additional protection from foreign discovery requests beyond those of a Data Localization cloud. Information in such clouds is held by a party with a role more akin to a storage locker company than a bank holding customer records.

c. *Federal Rules of Civil Procedure Summary.* — Discovery requests to a Data Shard cloud are likely to be viewed as similar to a domestic discovery request. In contrast, a U.S. court will analyze a contested request to Data Localization and Data Trust clouds under a comity analysis. Of these

---

370. For all five factors, see Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c).

371. See Volkswagen, A.G. v. Valdez, 909 S.W.2d 900, 902 (Tex. 1995).

372. Schwartz & Peifer, Transatlantic Data Privacy, supra note 2, at 122–37.

373. See Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c).

374. See supra section II.A.4.

two network models, Data Trust clouds are most likely to have success in resisting U.S. litigants' requests for data in the cloud. Companies managing this kind of cloud will be able to demonstrate "important interests of the state" threatened by the foreign discovery request.[375] Moreover, the information in such a cloud will be subject to the legal requirements of data protection law and domestic trust law. Under a comity analysis, a U.S. court would assign significant weight to these factors against granting a discovery request to cloud data stored extraterritorially.

III. PRINCIPLES FOR LEGAL ACCESS TO THE GLOBAL CLOUD

This Article now revisits its four initial lessons with reference to the preceding analysis of existing legal authorities for extraterritorial data access. Its main conclusion will be that the old status quo, a unilateral approach primarily controlled by the United States, is breaking down. The Pax Americana for the internet is not what it used to be; or more precisely, the ability of the United States to go it alone concerning requests for extraterritorial data is diminishing. The key factors in this decline are the growth of the internet outside the United States, the increased trend toward localization of data (both legal and technical), and the international skepticism toward U.S. privacy protections.

In place of the unilateral approach, this Article advocates for new international agreements regarding extraterritorial data access. These are to be based, first, on a level playing field—to meet the need for equal treatment of global clouds, regardless of the location of the provider's headquarters. As a second principle, this Article calls for the development of rules for data access to global clouds based on reciprocal interests among nations. To a great extent, the CLOUD Act acknowledges these policy concerns and breaks important new ground.

A. *Initial Lessons Revisited*

Section I.C.2 drew four preliminary lessons. The first is that Data Shard, Data Localization, and Data Trust clouds raise distinct legal issues. A one-size-fits-all analysis is not suitable for evaluating legal questions regarding access to information stored in these different kinds of clouds, and the preceding analysis of U.S. legal authorities for extraterritorial data access confirms this point. In particular, Data Shard and Data Trust clouds remain at different ends of the spectrum with respect to such data requests. And while the CLOUD Act has largely flattened the distinction among different types of clouds for SCA requests,[376] differences in treatment persist under other legal authorities.

---

375. Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c).

376. See supra note 223 and accompanying text.

Under a variety of laws, U.S. courts are likely to treat a Data Shard cloud in the same fashion as any garden-variety, U.S.-based cloud. As far as governmental data requests are concerned, for example, courts will reach this outcome for subpoena requests.[377] Regarding discovery requests by private parties, courts are similarly likely to assimilate their analysis of Data Shard clouds to that of U.S.-based clouds.[378] Over time, these outcomes may make Data Shard networks relatively less attractive for non-U.S. clients who are concerned about data access requests from the United States and skeptical of U.S. privacy law. This result may be altered, however, by the CLOUD Act—especially once the United States reaches executive agreements with foreign governments pursuant to the Act.

The second lesson regards the divisibility of control—that is, the ability to separate cloud access from other aspects of network management. This dimension is found in Data Trust clouds, which—under the current state of play—offer additional protections from U.S. extraterritorial requests for localized cloud information. The CLOUD Act extends the SCA to these clouds, but access requests under the Act will be directed to the Data Trustee, not the cloud provider. In this fashion, the divisibility of control serves to equalize treatment of a U.S. provider of a Data Trust cloud with a non-U.S. provider of a foreign localized cloud.[379] On the civil side, requests for information in a Data Trust cloud will be analyzed according to a comity analysis, which is typically that of the Restatement (Third) of Foreign Relations. Data Trustees will be able to draw on the protections of both their domestic information protection law and domestic law of trusts, resulting in strong interests against disclosure of cloud data.[380]

The third lesson concerns the growth of data localization, both of the technical and legal kind. Professors Jack Goldsmith and Tim Wu have identified the important role of intermediaries in assisting governments to control internet behavior.[381] In their explanation, law does not function like the Ten Commandments—that is, as "a series of direct, individualized directives (thou shall not kill, steal or bear false witness)."[382] Rather, governments exercise extraterritorial control over the internet by controlling the behavior of intermediaries.[383] This process is demonstrated by the localization requirements for global clouds. Through legal mandates, governments have acted to require their potential surveillance "targets" to store data domestically with regulated

377. See supra section II.A.4.
378. See supra section II.B.
379. See supra section II.A.3.
380. See supra section II.A.3.
381. Goldsmith & Wu, supra note 11, at 67–68.
382. Id. at 68.
383. Id.

"intermediaries," namely cloud companies. Moreover, non-U.S. customers who do not fall under such a legal requirement may seek such services for their own reasons, including doubts about U.S. privacy protections. The development of ready-made cloud technology that permits localization has lowered the costs of using Data Localization or Data Trust clouds.

The fourth lesson is that policies in this area must be based on a dynamic analysis of the interplay between legal rules and cloud technology. The myriad parties involved in the process include those who seek data, cloud customers, cloud providers, and nation-states that contemplate data localization laws. In response to legal and technological developments, these parties will, in turn, strategically alter their behavior. When it comes to extraterritorial access to data held in non-U.S. clouds, such strategic behavior will predictably seek out clouds that are more rather than less insulated from data requests originating from the United States.

With these four lessons in mind, what are the big-picture takeaways? First, the CLOUD Act has weakened a past pattern of U.S. law, which was to subsume Data Shard clouds entirely within its existing rules for domestic clouds. The CLOUD Act makes Data Localization and Data Shard clouds equally subject to SCA requests. As a consequence, certain non-U.S. customers of networked computing may be more willing to use Data Shard clouds. Put differently, non-U.S. customers who are skeptical of U.S. law, or would prefer to have data requests for their information handled under their own legal system, gain somewhat less of a benefit from using Data Localization and Data Trust clouds. Like Data Shard clouds, these latter models are now also subject to U.S. SCA requests.

Second, it is also clear that MLATs will remain important. The process of developing executive agreements under the CLOUD Act will take many years; in contrast, there are now sixty countries that have MLATs with the United States.[384] MLATs will also be of continuing importance if a foreign government seeks information about a U.S. person or non-U.S. person located in the United States. Perhaps most importantly post–CLOUD Act, the SCA leaves unaltered the inapplicability of the SCA to a wide range of records that a business may have about its customers, clients, and users.

Finally, the regime of Pax Americana for the internet is in decline. As a historical matter, the United States developed the internet and subsequently exercised great power over its rules.[385] Due to this historical development, the internet's "origin story"—as Hollywood says in superhero films—led the world's data traffic to pass through the territory of

384. See supra note 280 and accompanying text.

385. For one of the best histories of this development, see generally Katie Hafner & Matthew Lyon, Where Wizards Stay Up Late: The Origins of the Internet (1996).

the United States.[386] The result was a bonanza for U.S. national security agencies and law enforcement. Today, however, the dominance of the United States over the internet is under assault in many areas of policy, including global access to extraterritorial data. Legal data localization is one of the ways that many countries are now threatening the open internet. The next section considers the erosion of the Pax Americana, specifically as it affects extraterritorial data access. It also identifies two core principles to guide the future of data access laws in light of the shifting balance of power in global internet policy.

B. *International Cooperation and Equal Treatment of Extraterritorial Clouds*

As cloud technologies continue to evolve, the past unilateral approach of the United States is no longer tenable. Moving forward, the United States cannot expect to be the sole decisionmaker regarding the applicable legal process when the U.S. government or civil litigants seek data stored extraterritorially.[387] This result follows for a number of factors, including a likely future that is one of increased Data Localization and Data Trust clouds, which will limit the reach of extraterritorial data requests.

There has also been a dramatic growth of the internet outside the United States. The International Telecommunication Union estimates that approximately 3.2 billion people were online in 2015.[388] Of these, approximately two billion were from developing countries.[389] According to one estimate, fewer than ten percent of internet users are located in the United States.[390] As the center of gravity of internet usage shifts, more countries will resist exclusivity status for U.S. data access rules. At the same time, U.S. cloud companies will continue to face data requests from parties outside the United States.

In both governmental and civil litigation, foreign litigants will seek to shield data under a comity analysis by emphasizing the importance of their constitutional and statutory interests in data protection and privacy.[391] Both civil litigation discovery and governmental data demands

386. Bernard E. Harcourt, Exposed: Desire and Disobedience in the Digital Age 76–79 (2015).

387. For an insightful definition of "the unitary approach," see Swire & Kennedy-Mayo, supra note 3, at 663–64.

388. Int'l Telecomm. Union, Facts and Figures: The World in 2015 (2015), https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf [https://perma.cc/9Y6E-BJE2].

389. Id.

390. Internet Users in the World by Regions—Dec. 31, 2017, Internet World Stats, http://www.internetworldstats.com/stats.htm [https://perma.cc/3KTD-S7CZ] (last updated June 2, 2018); Statista, Internet Usage Worldwide 14 (2018), https://www.statista.com/study/12322/global-internet-usage-statista-dossier/ (on file with the *Columbia Law Review*).

391. See, e.g., In re Xarelto (Rivaroxaban) Prods. Liab. Litig., MDL NO. 2592, 2016 WL 2855221, at *3–6 (E.D. La. May 11, 2016) (noting the importance of conducting a

will therefore be complicated by the constitutional status of information privacy in important foreign jurisdictions, most notably the European Union.[392] Indeed, in the relevant academic literature in the United States, scholars have either noted a trend toward U.S. courts giving greater weight to foreign privacy law in their comity verdicts or argued that such a result is necessary.[393]

Finally, in the absence of some mechanism for global data access rules, there is risk of a free-for-all among conflicting rules. Researchers at the Universities of London and Cambridge have raised the risk of a "sanctions arm race" among different legal orders.[394] In evaluating a clash among legal rules, a cloud provider subject to the rule of multiple jurisdictions may have to "choose which state's laws to break."[395] In this regard, the European Union may currently have the upper hand with the provisions in its General Data Protection Regulation, which permit massive fines. The penalties in the GDPR can reach up to the greater of twenty million euros or four percent of an enterprise's annual worldwide turnover.[396]

---

detailed comity analysis when considering a request for different kinds of personnel files from a German defendant for use in a U.S. products liability case); In re Vitamins Antitrust Litig., No. 99–197TFH, 2001 WL 1049433, at *9 (D.D.C. June 20, 2001) (allowing German defendants to submit a "privacy log detailing exactly what requested information would be covered by the German privacy laws"); Volkswagen, A.G. v. Valdez, 909 S.W.2d 900, 902–03 (Tex. 1995) (reversing the lower court's order for Volkswagen A.G. to turn over information located in Germany because its order would violate the legal obligation under U.S. foreign relations law to balance the interests of a foreign sovereign with those of the U.S. court); Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c) (Am. Law Inst. 1987) (noting that when the laws of the foreign sovereign protect relevant information from discovery, the interests of the United States must be balanced with those of the foreign sovereign); see also Solove & Schwartz, Information Privacy Law, supra note 35, at 1174–77 (providing commentary on the *In re Vitamins* and *Valdez* litigations).

392. For a discussion of constitutional data privacy protections in the European Union, see Schwartz & Peifer, Transatlantic Data Privacy, supra note 2, at 123–27.

393. See, e.g., Diego Zambrano, A Comity of Errors: The Rise, Fall, and Return of International Comity in Transnational Discovery, 34 Berkeley J. Int'l L., no. 1, 2016, at 157, 179–80 (arguing that U.S. courts are now giving greater weight to foreign laws in their comity analysis than in the past); Samantha Cutler, Note, The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information, 59 B.C. L. Rev. 1513, 1532 (2018) (arguing that the courts should weigh the interests reflected in the privacy laws of foreign nations when contemplating discovery orders).

394. W. Kuan Hon et al., Policy, Legal and Regulatory Implications of a Europe-Only Cloud, 24 Int'l J.L. & Info. Tech. 251, 276 (2016).

395. Id.

396. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 83–84, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]. The GDPR also sets strict limits on transfers of data not authorized by E.U. law. See id. art. 48.

Until recently, U.S. policymakers placed little significance on issues involving access to information located outside the United States. For example, Swire and Hemmings observe that for many years the MLAT process was merely "an obscure specialty topic for international lawyers."[397] In contrast, today, U.S. law enforcement frequently seeks the cooperation of foreign jurisdictions in combating terrorism and organized crime, just as foreign authorities turn to U.S. officials for assistance in their own such efforts.[398] Access to global data greatly aids both parties.[399] Moreover, civil requests for discovery raise higher stakes than before because of the growth of global commerce and the increase in international communications.[400]

Others have predicted an end to the unilateral approach and greater difficulties for U.S. parties who seek access to data in non-U.S. clouds. Peter Swire, a member of President Obama's Review Group on Intelligence and Communications Technology, has called for legal reform based on a judgment that "the status quo of protections is likely to be weakened due to localization and other effects."[401] Daskal warns of the threat of "a Balkanized Internet and a race to the bottom, with every nation unilaterally seeking to access sought-after data, companies increasingly caught between conflicting laws, and privacy rights minimally protected, if at all."[402]

There are also indications of a growing awareness regarding the need for better mechanisms for access to international cloud data. In particular, there is an emerging E.U.–U.S. collaboration around issues relating to national security and law enforcement. A sign of this increased transatlantic cooperation is the E.U.–U.S. data protection Umbrella Agreement, which permits information sharing "to combat crime, including terrorism."[403] The Umbrella Agreement establishes data privacy protections for all personal data that is shared pursuant to it.[404]

---

397. Swire & Hemmings, Mutual Legal Assistance, supra note 62, at 688.

398. Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary, 115th Cong. (2017) (statement of Sen. Grassley, Chairman, S. Comm. on the Judiciary).

399. Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary, 115th Cong. (2017) [hereinafter McGuinness Testimony] (written testimony of Paddy McGuinness, United Kingdom Deputy National Security Adviser).

400. Chander & Lê, supra note 68, at 721 (describing the global flow of data as "the lifeblood of economies around the world").

401. Swire & Kennedy-Mayo, supra note 3, at 659.

402. Daskal, Law Enforcement Access, supra note 3, at 475.

403. Signing of the "Umbrella" Agreement: A Major Step Forward in EU–U.S. Relations, European Comm'n (June 2, 2016), http://ec.europa.eu/justice/newsroom/data-protection/news/160602_en.htm [https://perma.cc/SKP3-SF5V].

404. See id.

Within the European Union itself, the European Commission is considering different options to permit speedier access to information stored in clouds within its Member States. These national E.U. standards vary widely in their levels of privacy safeguards for the users.[405]

Turning to two final policy points, this Article first discusses the merits of the policy principle of a level playing field for tech companies. Such a policy would treat clouds equally regardless of whether these entities stored data within the United States or extraterritorially. The CLOUD Act has taken significant steps in this direction. It then discusses the importance of building a new regime for legal access to the global cloud around a principle of reciprocity. The CLOUD Act has presented a way forward that enhances international cooperation around this concept. The need is to harmonize international law in a way that respects privacy but also preserves suitable access to data with appropriate legal process.

1. *The Level Playing Field.* — The first principle for policymakers is that the United States should seek international agreements that treat extraterritorial clouds equally regardless of the provider's national origin. This Article terms this principle "the level playing field." Highlighting the need for such a principle, some jurists have discussed special limits on U.S. cloud providers whose networks have a non-U.S. component. Near the end of his concurrence in *Microsoft Ireland*, Judge Lynch raised this approach as a hypothetical issue. For Judge Lynch, Congress, in finding the "ideal balance" in an amended SCA, must do more than defer to "the mere location abroad of the server on which the service provider has chosen to store communications."[406] In listing a range of potential approaches and noting the absence of any "all-or-nothing choice," Judge Lynch observes that "[Congress] is free to decide, for example, to set different rules for access to communications stored abroad depending on the nationality of . . . the corporate service provider."[407]

In a related fashion, Kerr, in sketching the "next generation communications privacy act," explores whether this statute should mandate technological design constraints on U.S. cloud providers.[408] He writes: "Congress could regulate territoriality by adopting express rules as to when providers can or must design their networks in ways that go outside U.S. territory to subject communications to foreign government

405. For a window into these disparities, see generally Winston J. Maxwell, Systematic Government Access to Private-Sector Data in France, *in* Bulk Collection: Systematic Government Access to Private Data 49, 49–60 (Fred H. Cate & James X. Dempsey eds., 2017) [hereinafter Bulk Collection]; Giorgio Resta, Systematic Government Access to Private-Sector Data in Italy, *in* Bulk Collection, supra, at 111, 111–26; Paul M. Schwartz, Systematic Government Access to Private-Sector Data in Germany, *in* Bulk Collection, supra, at 61, 61–90.

406. *Microsoft Ireland*, 829 F.3d 197, 231 (2d Cir. 2016) (Lynch, J., concurring).

407. Id. at 232.

408. Kerr, Next Generation, supra note 18, at 416–18.

access."[409] Ultimately, Kerr turns away from this solution and calls for a user-based regime for territoriality.[410] He is wise to do so; it would be highly problematic for different U.S. legal rules to apply to an extraterritorial cloud based on the nationality of the provider.

The law should not demand more of domestic companies than non-U.S. companies in regulating requests for information in extraterritorial clouds. Today's market for information technology is an international one, and different legal standards for domestic and nondomestic companies would simply encourage the use of non-U.S. services by non-U.S. customers.[411] These customers would route around U.S. regulation by avoiding U.S. tech companies and storing their information in their national clouds. Current efforts by U.S. companies to demonstrate their "careful stewardship of private data" would be undercut.[412] Looking to the future of digital services, Neelie Kroes, former E.U. Commissioner for Digital Affairs, predicted: "It is often American providers that will miss out, because they are often the leaders in cloud services. If European cloud customers cannot trust the United States government, then maybe they won't trust [U.S.] cloud providers either."[413] Differing legal standards for U.S. companies would also prevent global specialization by cloud providers and limit the resulting benefits of expertise and scalability of technology.[414] It would also encourage balkanization of the internet into competing national or regional fiefdoms with the threat of future interoperability snafus on the horizon. The stakes are high; as two scholars note, the wrong kind of legal regime runs the risk of destroying the global nature of the internet.[415]

As an additional policy matter, U.S. law generally does not impose the full United States Code on U.S. companies when they engage in business outside this country. It permits U.S. companies that do business internationally to follow laws of the applicable foreign jurisdiction and does not limit the ability of foreign nations to regulate behavior in their territories.[416] This policy reflects respect for other states, which is a bul-

409. Id. at 416.

410. See id.

411. As background on the new world of international commerce and for an impassioned plea for a technological-neutrality principle to promote "Trade 2.0," see generally Anupam Chander, The Electronic Silk Road: How the Web Binds the World Together in Commerce 142–57 (2013).

412. Swire & Hemmings, Mutual Legal Assistance, supra note 62, at 714.

413. Traynor, supra note 4.

414. See Chander & Lê, supra note 68, at 719 (explaining that the local provider "offering storage and processing services may be more likely to have weak security infrastructure than companies that continuously improve their security to respond to the ever-growing sophistication of cyberthieves").

415. See id. at 713–14.

416. As the Supreme Court has noted, "It is a basic premise of our legal system that, in general, 'United States law governs domestically but does not rule the world.' . . . Absent clearly expressed congressional intent to the contrary, federal laws will be construed to

wark of international law. As Judge Lynch observed in his concurrence in *Microsoft Ireland*, U.S. demands for records about a foreign national stored on servers in her own country raise the possibility for "diplomatic strife."[417] In particular, there is a danger of "diplomatic consequences" from "over-extending the reach of American law enforcement officials."[418] In his reference to "consequences," Judge Lynch was alluding to the power of foreign nations to make U.S. cloud companies subject to reciprocal claims for information of their citizens that is stored in the United States. As the saying goes, "what's sauce for the goose is sauce for the gander." Or, as Swire and Hemmings warn, "[a]t least for the near future, the United States is a primary exporter of electronic evidence."[419] In similar terms, Richard Salgado, the Director for Law Enforcement and Information Security at Google, explained to a congressional committee that since 2009, Google has received more requests from foreign legal authorities than from U.S. criminal law enforcement agencies.[420]

To be sure, there are circumstances in which U.S. lawmakers regulate behavior by U.S. actors that takes place outside this country. The Foreign Corrupt Practices Act (FCPA) provides a useful comparison.[421] This 1977 statute prohibits corporate bribery of foreign officials; it does so because this behavior has a deeply destructive impact on the fair market system, both overseas and within the United States.[422] Entities that engage in such banned corrupt practices act unfairly. The unfairness is, first, to those U.S. companies that do not wish to violate foreign law by bribing officials and, second, to U.S. investors, who face uncertainty in making investment decisions due to the lack of accounting transparency

---

have only domestic application." RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2100 (2016) (quoting Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 454 (2007)); see also EEOC v. Arabian American Oil Co., 499 U.S. 244, 248 (1991) ("It is a longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'" (quoting Foley Bros., Inc. v. Filardo, 336 U.S. 281, 285 (1949))).

417. 829 F.3d 197, 231 (2d Cir. 2016) (Lynch, J., concurring).

418. Id. at 229.

419. Peter Swire & Justin Hemmings, Stakeholders in Reform of the Global System for Mutual Legal Assistance, *in* Bulk Collection, supra note 405, at 395, 400. They add that "many more requests for mutual legal assistance for electronic evidence are made *of* the [U.S.] government than *by* the [U.S.] government." Id.

420. Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary, 115th Cong. (2017) [hereinafter Salgado Testimony] (written testimony of Richard Salgado, Director, Law Enforcement and Information Security, Google).

421. 15 U.S.C. § 78dd-1 (2012); see also Rahul Kohli, Foreign Corrupt Practices Act, 55 Am. Crim. L. Rev. 1269, 1270 n.1 (2018) (noting places in the U.S. Code at which scattered portions of the Foreign Corrupt Practices Act have been codified).

422. For an overview of the FCPA and the policy rationales behind it, see generally Dep't of Justice & SEC, FCPA: A Resource Guide to the U.S. Foreign Corrupt Practices Act (2012), https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf [https://perma.cc/TP8E-3L2E].

that typically accompanies corrupt practices.[423] In comparison to the FCPA, a restriction on U.S. cloud service providers abroad does not deter negative externalities. The FCPA prevents a bad act: bribery abroad. The existence of a cloud service is not inherently a bad act, although it is possible that someone might engage in a bad act using a cloud service. In short, the FCPA is not an apt model for regulation of extraterritorial access to data held in a cloud.

U.S. tech companies' leadership in the global cloud market has been a positive marketplace factor due to the efficiencies of large-scale cloud computing. Moreover, the cloud services of U.S. companies are based on a business model built around compliance with foreign jurisdictions. In fact, some of the open questions under the SCA pre–CLOUD Act followed from U.S. tech companies trying to comply with aspects of the law of foreign jurisdictions regarding extraterritorial data requests that are in tension with U.S. law.[424] The critical need is for policy reform that promotes a global and interoperable internet, safeguards privacy, and permits reasonable access to cloud data for law enforcement and civil litigants.

As has been discussed above, the CLOUD Act takes a major step toward leveling the playing field for SCA data requests. Specifically, it makes Data Localization and Data Shard clouds equally subject to the SCA requests. The statute also treats Data Trust clouds on the same footing as Data Localizations in a comity analysis while preventing a disfavoring of U.S. cloud providers who set up such arrangements in foreign countries.[425] The law's impact on privacy is a thornier question, however, and this Article turns to it below.

2. *The Principle of Reciprocity.* — The second and final point of orientation for policy reform should be the recognition of reciprocal national interests concerning legal access to the global cloud. There is a need to develop new agreements to regulate extraterritorial data access. The U.S. Congress has now taken a decisive step toward the principle of reciprocity in enacting the CLOUD Act. This Article has already discussed this statute in the context of the SCA; it now examines it in the larger context of foreign requests for data in U.S. clouds.[426] After sketching the CLOUD Act's advancement of reciprocity, this Article develops three critical points. First, the merit of the agreements developed under the CLOUD Act depends on how well the executive branch and Congress use the Act's processes to monitor the compliance of other nations with resulting agreements. Second, the Act should be improved through amendment. Finally, the CLOUD Act creates strong incentives for cloud

423. Id. at 3.

424. See Salgado Testimony, supra note 420, at 2.

425. See infra section III.B.2.

426. The CLOUD Act builds on an earlier bill, the International Communications Privacy Act (ICPA), S. 2986, 114th Cong. (2016).

providers to know who their users are. It encourages a new know-your-customer regime for the global cloud.

a. *Reciprocity*. — The CLOUD Act has already amended the SCA to extend U.S. government requests to reach data stored extraterritorially. Step One took effect immediately with enactment of the statute.[427] Looking to the future, however, the CLOUD Act opens up a new way for foreign governments to access data stored in the United States, including real-time data requests. These accords require reciprocity; the foreign government must grant the United States similar treatment. Step Two is not yet effective; it requires development of "executive agreements" with "qualifying foreign government[s]."[428] Once in place, such agreements will allow a foreign country to bypass the MLAT process and make requests directly to a U.S. cloud provider, but only for law enforcement purposes regarding "serious crime."[429]

To understand how this law approaches reciprocity, we begin with its central statutory term of art, the "qualifying foreign government." The definition of a "qualifying foreign government" has two essential elements. First, and as a threshold matter, the laws of the foreign jurisdiction can be qualifying only if they supply providers with "substantive and procedural opportunities" similar to those provided by the CLOUD Act.[430] These include, in particular, the abilities of the provider to seek to "quash or modify" legal requests for content of communications based on a conflict of laws, and to disclose to the foreign government the legal request for the disclosure of communication.[431] These are important safeguards for transparency.

Second, a qualifying foreign government is one with which the United States has entered into "an executive agreement."[432] The CLOUD Act establishes the necessary elements of such an agreement in great detail. The executive branch of the United States is to develop the agreement with the foreign government in question.[433] The Attorney General

---

427. See CLOUD Act, H.R. 1625, 115th Cong. div. V, § 103(a)(1) (2018) (adding 18 U.S.C. § 2713, titled "Required Preservation and Disclosure of Communications and Records").

428. Id. § 105(a) (adding 18 U.S.C. § 2523, titled "Executive Agreements on Access to Data by Foreign Governments"); see also id. § 103(a)(1) (defining "qualifying foreign government").

429. Id. § 105(a) (adding 18 U.S.C. § 2523(b)(4)(D)(i)). This ability even extends beyond stored data; the CLOUD Act also permits real-time interceptions, as U.S. law permits under the Wiretap Act but not the SCA. Such requests, however, are to be for interceptions of a "fixed, limited duration" and may "be issued only if the same information could not reasonably be obtained by another less intrusive method." Id. (adding 18 U.S.C. § 2523(b)(4)(D)(vi)).

430. Id. § 103(a)(1) (adding 18 U.S.C. § 2713(h)(1)(A)(ii)).

431. Id. (adding 18 U.S.C. § 2713(h)(2)).

432. Id. § 105(a) (adding 18 U.S.C. § 2523(b), titled "Executive Agreement Requirements").

433. Id.

must then certify it to Congress.[434] In making this certification, the Attorney General is to evaluate the domestic law of the foreign government and find that it "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement."[435] The CLOUD Act then spells out a detailed list of factors to be used in making this determination, including whether the foreign government "adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights."[436] The CLOUD Act also sets requirements for each data request by the qualifying foreign government. The request must be particularized, based on "articulable and credible facts," and subject to "review or oversight by a court, judge, magistrate, or other independent authority" in the foreign jurisdiction.[437]

As international agreements under the CLOUD Act begin to follow the policy principle of reciprocity, the key question will be the nationality of the data. The United States will now begin the process of constructing a series of international agreements about access to global data by proceeding first with states that most closely share its values. As an initial attempt in this regard, one can point to the proposed U.S.–U.K. Bilateral Agreement on Data Access, which would permit "reciprocal targeted access to data, enabling companies based in one country to comply with lawful orders from the other."[438]

In sum, the CLOUD Act takes a dramatic step toward a global interoperable system that will expedite law enforcement's data requests. A similar process is happening within the European Union itself. In April 2018, the Commission proposed a new "e-evidence" regulation to create the "European Production Order."[439] This regulation would allow a judicial authority in one E.U. Member State to obtain orders for electronic evidence.[440] It would also permit a judicial authority in one E.U. Member State to obtain electronic evidence directly from a service provider in another state.[441] The proposed regulation would be an initial move to a CLOUD Act for the European Union itself. Talks are also underway

434. Id.

435. Id. (adding 18 U.S.C. § 2523(b)(1)).

436. Id. (adding 18 U.S.C. § 2523(b)(1)(B)(iii)).

437. Id. (adding 18 U.S.C. § 2523(b)(4)(D)(iv)–(v)).

438. McGuinness Testimony, supra note 399.

439. See Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, at 4, COM (2018) 225 final (Apr. 7, 2018) [hereinafter Proposal for a Regulation for Electronic Evidence].

440. See E-Evidence, European Comm'n, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en [https://perma.cc/5DA4-EC9Z] (last updated July 27, 2018) (outlining the key provisions and legislative history of the proposed regulation).

441. See Proposal for a Regulation for Electronic Evidence, supra note 439, at 4.

between the United States and the European Union regarding a possible E.U.–U.S. general framework under the CLOUD Act.[442]

b. *Evaluating the CLOUD Act.* — The decentralized approach of the CLOUD Act is promising. There are too many variations in this area of law within the international landscape and across different legal and political systems for any single treaty or statute to control. Indeed, Woods makes an important point in this regard about the danger that such a single-world agreement could be based only on the least common denominator.[443] Outside the United States, countries have differing standards with respect to privacy and due process rights when it comes to accessing stored digital data. From this perspective, decentralization is a compelling second-best solution.

On a positive note, there are important elements of the CLOUD Act that protect privacy. First, regarding U.S. citizens and residents, the CLOUD Act's executive agreements permit foreign government requests concerning the data only of non-U.S. persons who are located outside the United States.[444] Accessing the data of U.S. persons and others located in the United States will still require use of the MLAT process. There are additional safeguards to prevent a foreign government from targeting a U.S. person or a non-U.S. person in the United States. For instance, the statute forbids an action sometimes called "authority-hopping"; this term refers to a practice in which one nation engages in surveillance and shares the resulting data with a second nation, one whose own law prevents it from engaging in this action.[445] The law also requires a recertification process after five years;[446] in this fashion, the CLOUD Act creates an opening for pressure when shortcomings appear in a foreign country's use of specific executive agreements.

As another positive step, the CLOUD Act forbids executive agreements from requiring a company to be capable of decrypting data.[447] This aspect of the law is perhaps surprising in light of the ongoing law enforcement concerns about going dark.[448] The CLOUD Act takes this matter off the table for executive agreements. Specifically, it protects a

---

442. Jennifer Daskal & Peter Swire, A Possible US–EU Agreement on Law Enforcement Access to Data?, Just Security (May 21, 2018), https://www.justsecurity.org/56527/eu-agreement-law-enforcement-access-data/ [https://perma.cc/SLD7-Q3GM].

443. See Woods, supra note 3, at 788.

444. A foreign government may not "intentionally target a United States person or a person located in the United States" or "target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States." H.R. 1625, 115th Cong. div. V, § 105(a) (2018) (adding 18 U.S.C. § 2523(b)(4)(A)–(B)).

445. See id. (adding 18 U.S.C. § 2523(b)(4)(C), which provides that "the foreign government may not issue an order at the request of or to obtain information to provide to . . . a third-party government").

446. Id. (adding 18 U.S.C. § 2523(e), titled "Renewal of Determination").

447. See id. (adding 18 U.S.C. § 2523(b)(3)).

448. See supra note 1 and accompanying text.

cloud provider under a Data Trust arrangement from being compelled to hack its own encrypted servers. It helps guarantee that resulting data requests will instead be made to the Data Trustee, who holds the keys to the encrypted data.

There is much, however, that is open concerning the ultimate impact of the CLOUD Act. In the abstract and at this juncture, it is difficult to evaluate the merits of future agreements developed under the CLOUD Act.[449] A key factor will be how well the executive branch and Congress use the statute's mandated processes and how they approach undefined or broadly defined terms in the statute. Moreover, as a price of entry, the statute requires a foreign country to have or to adopt U.S.-style privacy safeguards in its domestic laws.[450] Human rights advocates have found much to criticize in the law's standards in this regard.[451] Others are more optimistic about how the law will function.[452]

Regarding the process, the CLOUD Act details a number of substantive requirements that the Attorney General must accomplish before certifying that an executive agreement meets the statute's requirements. Thus, the Attorney General must obtain "the concurrence of the Secretary of State" and take into account "credible information and expert input."[453]

Another requirement concerns the significant oversight role of Congress. During a 180-day period, the legislature can disapprove the

---

449. At present, whether the CLOUD Act will lead to an increase or decrease in global privacy standards can be considered an open question. In a recent blog post, lawyers from Amnesty International and the ACLU warned against a move to executive agreements in place of "case-by-case consideration" under the MLAT process. Sometimes human rights can rapidly deteriorate, and it is a mistake to believe that countries could simply be "safe-listed as human rights-compliant." Neema Singh Guliani & Naureen Shah, The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them, Lawfare (Mar. 16, 2018), https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them [https://perma.cc/6DC3-L86B].

450. See H.R. 1625 div. V, § 105(a) (adding 18 U.S.C. § 2523(b)(1), which establishes that an executive agreement may not be submitted to Congress unless the foreign government "affords robust substantive and procedural protections for privacy and civil liberties").

451. See, e.g., Robyn Greene, Somewhat Improved, the CLOUD Act Still Poses a Threat to Privacy and Human Rights, Just Security (Mar. 23, 2018), https://www.justsecurity.org/54242/improved-cloud-act-poses-threat-privacy-human-rights/ [https://perma.cc/92G5-GA2S].

452. Some commentators praise the presence in this law of "substantive and procedural privacy standards that are preconditions for entering into bilateral agreements" and view it as likely to increase the world's privacy baseline. Daskal, International Lawmaking 2.0, supra note 234, at 15; see also Jennifer Daskal & Peter Swire, Privacy and Civil Liberties Under the CLOUD Act: A Response, Lawfare (Mar. 21, 2018), https://www.lawfareblog.com/privacy-and-civil-liberties-under-cloud-act-response [https://perma.cc/JP7R-HZW3]; 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/3BQY-MUSH].

453. H.R. 1625 div. V, § 105(a) (adding 18 U.S.C. § 2523(b), (b)(1)(A)).

certified executive agreement by joint resolution.[454] Depending on one's feelings about increased legislative scrutiny, it might be desirable to require that Congress affirmatively approve agreements rather than rely only on its weaker power to issue joint resolutions of disapproval of executive agreements.[455] The present approach means that only a veto-proof majority in Congress can overturn a President's decision to approve an executive agreement. On the other hand, giving greater power to Congress may slow the process of reaching executive agreements and even hinder the President's ability to effectively negotiate with foreign governments.

As a further open matter under the statute, one of the statute's most critical terms lacks a definition. The CLOUD Act provides that a foreign government can issue an order to a provider only for a "serious crime," but lacks specificity as to which offenses are covered.[456] An amendment to this statute should define the concept of "serious crime" more precisely.[457]

Finally, there is the matter of the most expansive element of the CLOUD Act, which makes its real-time access to communications subject to its executive agreements.[458] It permits service providers operating in the United States to carry out real-time interceptions in this country in compliance with orders issued by foreign governments.[459] In so doing, it goes beyond the reach of the SCA, which concerns only stored data.[460] While imposing some limits on the type of foreign interception orders that U.S. providers can comply with, the CLOUD Act does not require foreign law enforcement agencies seeking real-time access to meet the tough warrant standards found in the U.S. Wiretap Act.[461]

---

454. Id. (adding 18 U.S.C. § 2523(d)(4), titled "Congressional Review").

455. See id.; see also Jennifer Daskal & Peter Swire, Suggestions for Implementing the Cloud Act, Lawfare (Apr. 30, 2018), https://www.lawfareblog.com/suggestions-implementing-cloud-act [https://perma.cc/F2GU-ADXX] (providing additional amendment suggestions).

456. H.R. 1625 div. V, § 105(a) (adding 18 U.S.C. § 2523(b)(4)(D)(i)).

457. See Daniel Sepulveda, Opinion, Bill on Cross-Border Data Access Needs to Change, Despite Laudable Goal, Hill (Mar. 16, 2018), http://thehill.com/opinion/technology/378785-bill-on-cross-border-data-access-needs-to-change-despite-laudable-goal [https://perma.cc/L9LH-R84X].

458. H.R. 1625 div. V, § 105(a) (adding 18 U.S.C. § 2523(b)(4)(D)(vi)).

459. Id.

460. See supra section II.A.2.

461. The CLOUD Act provides for "interception of wire or electronic communications" as long as it is "for a fixed, limited duration"; it does not "last longer than is reasonably necessary"; and "the same information could not reasonably be obtained by another less intrusive method." H.R. 1625 div. V, § 105(a) (adding 18 U.S.C. § 2523(b)(4)(D)(vi)). On the other hand, the Wiretap Act requires much more rigorous justifications for real-time interception warrants, also commonly known as "super warrants." Requirements include, for example, "full and complete statement[s]" as to why an order should be issued and "whether or not other investigative procedures have been tried and failed." 18 U.S.C. § 2518 (2012).

If the U.S. government obtains reciprocity from foreign governments, as is required by the CLOUD Act, the foreign government must amend its law so that it does not block providers from carrying out real-time interceptions in that country on behalf of a U.S. governmental entity.[462] This aspect of the CLOUD Act raises numerous policy questions about a subject—the interception of real-time data—that U.S. law has accorded its highest privacy protections since the enactment of the Wiretap Act in 1968.[463] In particular, it imports a "targeting" concept from the Foreign Intelligence Surveillance Act into wiretap law.[464] As a result, incidental collection of data about U.S. persons becomes likely. Collection of real-time communications data about a British person in the United States, for example, will also sweep in information about U.S. persons with whom the British person communicated.

Moreover, the CLOUD Act's "minimization" requirement for such data is much lower than the Wiretap Act's concept of minimization. For the CLOUD Act, minimization applies only to information affirmatively found not to be "relevant to the prevention, detection, investigation, or prosecution of serious crime."[465] Put in more straightforward terms, the CLOUD Act's requirement of a finding of "not . . . relevant" permits information to be collected unless it can be said to be irrelevant to the prevention, detection, investigation, or prosecution of serious crime.[466]

At a minimum, these dramatic policy developments deserved greater policy scrutiny rather than being buried in a nearly thousand-page budget bill.[467] A comparison with the European Union's GDPR and the E.U.–U.S. Privacy Shield is useful. The GDPR is the main touchstone for E.U.-wide information privacy; among its requirements is the presence of "adequate" privacy protections in any non-E.U. country that receives personal data from the European Union.[468] In reaction to the GDPR, the United States and the European Union have negotiated a Privacy Shield agreement, which allows U.S. companies to voluntarily self-certify their compliance with a set of E.U.-friendly fair information practices.[469]

---

462. H.R. 1625 div. V, § 105(a) (adding 18 U.S.C. § 2523(b)(4)(I)). These foreign service providers must, however, be otherwise subject to the jurisdiction of U.S. wiretap orders. See id.

463. Solove & Schwartz, Information Privacy Law, supra note 35, at 344–53.

464. See H.R. 1625 div. V, § 105(a) (adding 18 U.S.C. § 2523(b)(4)(A)).

465. Id. § 105(b)(4)(G).

466. See id.

467. For an objection to the real-time power authorized by the CLOUD Act, see 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/WMX6-QVAY].

468. See GDPR, supra note 396, art. 45.

469. U.S. Dep't of Commerce, EU–U.S. Privacy Shield Framework Principles § III.6 (2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [https://perma.cc/Z5M3-82D7].

Companies that agree to follow the Privacy Shield are deemed to have "adequate" data protection for the European Union; international data transfers can flow from the European Union to these companies.[470] The result is that the United States and European Union have created a normative infrastructure for bringing E.U.-style privacy practices into the United States.[471] Over three thousand U.S. companies have entered the Privacy Shield.[472]

In a similar fashion, the CLOUD Act starts the process of developing global standards under which law enforcement agencies can seek information from cloud providers throughout the world. There is, however, a likely collision ahead with the substantive standards of the GDPR. In its Article 48, the GDPR establishes a legal regime for a situation in which E.U. law does not otherwise permit a data transfer but a court or administrative authority in a third country would require it.[473] Such a transfer is permissible, however, only "if based on an international agreement, such as a mutual legal assistance treaty."[474]

Understanding the interaction between Article 48 of the GDPR and the CLOUD Act requires an analysis of the latter's Step One and Step Two.[475] First, the CLOUD Act extends the SCA extraterritorially. Second, the CLOUD Act permits the creation of executive agreements with foreign countries.

Regarding the SCA, a request by U.S. law enforcement to a foreign provider is merely a U.S. legislative decision. Article 48 of the GDPR clearly requires more than that: an international agreement.[476] Moreover, a law enforcement request under the CLOUD Act likely cannot be shoehorned into any GDPR exception that would allow an international data transfer without such an agreement.[477] Finally, the Privacy Shield is

---

470. For a discussion of the Privacy Shield, see Solove & Schwartz, Information Privacy Law, supra note 35, at 1187–97.

471. Schwartz & Peifer, Transatlantic Data Privacy, supra note 2, at 174–78.

472. Privacy Shield List, Privacy Shield Framework, https://www.privacyshield.gov/list [https://perma.cc/9MZF-QM5X] (last visited July 26, 2018). As of July 2018, 3,344 organizations were active participants of the Privacy Shield Framework. Id.

473. See GDPR, supra note 396, art. 48.

474. Id.

475. See supra text accompanying notes 227–243 (discussing the two-step framework of the CLOUD Act).

476. There is already an emerging legal consensus on this issue in Germany. See, e.g., Mathias Lejeune, Der US CLOUD Act: eine neue Rechtsgrundlage für den internationalen Datenzugriff? [The US CLOUD Act: A New Legal Framework for International Data Access?], 18 IT Rechtsberater 118, 121 (2018); Axel Spies, USA: Gesetzgeber billigt Datenzugriff außerhalb der USA (CLOUD Act) [Legislature Approves Data Access Outside the U.S. (CLOUD Act)], 8 Zeitschrift für Datenschutz 197, v, vi (2018).

477. Dr. Axel Spies has come to this same conclusion. See Spies, supra note 476, at vi. The matter is one of some complexity. To be sure, GDPR Article 49(1)(e) does permit a transfer when "necessary for the establishment, exercise or defence of legal claims." GDPR, supra note 396, art. 49. Nonetheless, under the so-called two-step process, there must first be a legal basis in E.U. law for the European entity—in this case, the cloud

insufficient as a mechanism to permit a cloud provider subject to E.U. data protection law to respond to an SCA warrant. U.S. law enforcement agencies are not Privacy Shield entities.[478]

Hence, from the European Union perspective, the CLOUD Act requires a new arrangement with the Commission for SCA requests to be permissible. In fact, E.U. Justice Commissioner Vera Jourova has criticized the enactment of the CLOUD Act "in a fast-track procedure" and denounced this unilateral act by the United States as one that "narrows the room for [a] potential compatible solution between" the European Union and the United States.[479] Without conceding these points, the U.S. Department of Justice has already met with the E.U. Commission to discuss the development of an E.U.–U.S. agreement to permit reciprocal exchange of data between law enforcement authorities.[480]

As for the second area of necessary analysis, the SCA's executive agreements would be "an international agreement" under Article 48.[481] This provision of the GDPR explicitly permits accords not only between the Union and a third country but also between an E.U. Member State and a third country, in this case the United States.[482] Hence, a bilateral accord under the CLOUD Act would comport with the GDPR's Article 48.

Yet, such two-party agreements will not represent the final word regarding whether the CLOUD Act is consistent with E.U. data protection law. The Court of Justice of the European Union (CJEU) will ultimately decide on the sufficiency of any executive agreements developed under the CLOUD Act. In a series of important decisions, the CJEU has constitutionalized E.U. data protection law as well as the overarching "adequacy" standard for transfers to third countries.[483] In its *Schrems* deci-

---

provider—to *process* the information before Article 49(1)(e) can apply to justify the *transfer*. See Christopher Kuner, European Data Protection Law: Corporate Compliance and Regulation 242 (2d ed. 2007) ("[C]ompanies become almost mesmerized with the mechanism to provide an adequate legal basis for the transfer, while neglecting to ask themselves what the legal basis is for the processing in the first place."). In the absence of an international agreement, such as an MLAT, there is no such basis in law for the processing. Jan Phillip Albrecht & Florian Jotzo, Das neue Datenschutzrecht der EU [The New Data Protection Law of the EU] 110 para. 23 (2017) (Ger.).

478. This result follows because U.S. law enforcement and intelligence agencies are not "organisations that have self-certified their adherence to the Principles" with the Department of Commerce. Commission Implementing Decision No. 2016/1250 of 12 July 2016, 2016 O.J. (L 207) 1, 6, 7 (EU). The Commission found the Privacy Shield to extend only to such entities. Id. at 4.

479. Nikolaj Nielsen, Rushed US Cloud Act Triggers EU Backlash, EUobserver (March 26, 2017), https://euobserver.com/justice/141446 [https://perma.cc/T749-PKKJ].

480. See Catherine Stupp, Jourova to Press for EU-US Data Sharing Deal Next Week, EURACTIV (May 18, 2018), https://www.euractiv.com/section/data-protection/news/jourova-to-press-for-eu-us-data-sharing-deal-next-week/ [https://perma.cc/U39H-T9ZD].

481. GDPR, supra note 396, art. 48.

482. Id. recital 115.

483. For a discussion, see Orla Lynskey, The Foundations of EU Data Protection Law 38–40 (2015); Schwartz & Peifer, Transatlantic Data Privacy, supra note 2, at 122–27.

sion, the CJEU declared that adequacy of data privacy, as a standard for international transfers, means that protections must be "essentially equivalent."[484] As Christopher Kuner perceptively observes, the *Schrems* opinion connects the requirement of adequacy "to the level of protection required by the Charter."[485] He adds, "By defining the standard that third countries must meet to be declared 'adequate' as that of essential equivalence with E.U. law, the CJEU has set the global data protection bar at a high level."[486] Thus, the CLOUD Act conflicts with E.U. data protection.

There are also high levels of interest in both the United States and the European Union in working together to combat international terrorism and organized criminality. Both political systems are already collaborating in this area, and the European Union is working to put in place its own internal equivalent of the CLOUD Act. On April 17, 2018, it introduced a Proposal for a Regulation of the European Production and Preservation Orders for Electronic Evidence in Criminal Matters.[487] Unlike the CLOUD Act, however, these orders would not permit surveillance of real-time data, but only the preservation of stored data.[488]

These E.U.-wide proposals indicate a possible common meeting ground for international data sharing. It is clear, moreover, that the European Union prefers a direct agreement with the United States rather than individual agreements between Member States and the United States. From the viewpoint of the Commission, then, the actual content of the CLOUD Act may pose less of a concern than the possibility that the United States might act unilaterally to seek nation-by-nation agreements that would cut the European Union itself out of the debate. As a final twist, however, the CLOUD Act itself looks to conformity with international human rights as one factor for the permissibility of an executive agreement with a foreign country.[489] In this light, it is notable that the European Court of Human Rights is now deciding a case concerning the U.K. intelligence community's collection of bulk data.[490] A ruling against the United Kingdom would be a factor against the United States coming

---

484. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650 ¶ 73, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362 [https://perma.cc/G4YP-33Z2].

485. Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post *Schrems*, 18 German L.J. 881, 893 (2017).

486. Id.

487. See Proposal for a Regulation for Electronic Evidence, supra note 440.

488. Id. at 5.

489. See CLOUD Act, H.R. 1625, 115th Cong. div. V, § 105 (2018) (adding 18 U.S.C. 2523(b)(1)(B)(iii)).

490. See Owen Bowcott, UK Intelligence Agencies Face Surveillance Claims in European Court, Guardian (Nov. 7, 2017), https://www.theguardian.com/world/2017/nov/07/uk-intelligence-agencies-face-surveillance-claims-in-european-court [https://perma.cc/UH3A-GQ2H].

to an executive agreement with the United Kingdom under the CLOUD Act's own terms.

c. *Know-Your-Customer in the Cloud.* — A last point should be made regarding a "grand bargain" inherent in the CLOUD Act. We can break down this grand bargain into two parts. Part One is simply stated: The executive agreements under the Act focus on the nationality or location of the user, and therefore make the locus of data storage far less important. The result is that the CLOUD Act reduces the significance of data localization in data access requests. This outcome maps with a significant goal identified by President Obama's Review Group on Intelligence and Communications Technologies in 2013, which identified a policy need for "a globally interoperable, open, and secure Internet architecture," as opposed to one that increasingly requires "servers to be physically located within a country or limits on transferring data across borders."[491] This first step will delight the advocates of an open and interoperable internet.

A grand bargain typically has two sides, however, and the other part of the CLOUD Act is to incentivize cloud providers to take greater steps to identify their customers.[492] Hence, Part Two will undoubtedly dismay privacy advocates. Under this law, the nationality and location of the user become paramount issues. The ability of a foreign country to object to the extraterritorial use of an SCA warrant is present only *when the cloud provider can reasonably point to the nationality and location of the user.*[493] Data Shard and Data Localization clouds gain the benefit of having their non-U.S. customers receive additional protection under an executive agreement. Even Data Localization clouds with data accessible in the United States benefit if the location of the data user was in a foreign country with an executive agreement. But cloud providers would need to document the nationality of their customers and their location to benefit from the executive agreements that will be developed under the CLOUD Act.

As illustrated by *Microsoft Ireland*, however, cloud providers do not currently verify customer identity in any rigorous manner. The system is loose especially when it comes to free services, such as email, in which there is no need to collect billing information. Thus, in *Microsoft Ireland*, the customer who used the contested Hotmail account had merely self-

---

491. President's Review Group on Intelligence & Commc'ns Tech., supra note 285, at 214–15.

492. See H.R. 1625 div. V, § 103(b) (adding 18 U.S.C. § 2713(h)(3)(D), which establishes as a factor in the comity analysis "the location and nationality of the subscriber or customer whose communications are being sought, if known").

493. A foreign government may not "intentionally target a United States person or a person located in the United States" or "target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States." See id. § 105(a) (adding 18 U.S.C. § 2523(b)(4)(A)–(B)).

identified as being associated with Ireland.[494] As the Second Circuit stated, Microsoft relied on this information in storing information relating to his account in Dublin, Ireland. The court observed: "[Microsoft] does not verify user identity or location; it simply takes the user-provided information at face value, and its systems migrate the data according to company protocol."[495] In his concurrence, Judge Lynch termed this approach "self-reporting" by customers.[496]

Under the CLOUD Act, the era of such self-reporting of customer location and identity is likely to end. The CLOUD Act asks providers where their clients are located and who these persons are—that is, what their nationality is.[497] Providers are likely to translate these legal rules into a corporate compliance structure.[498] The resulting rationalized process, driven by in-house lawyers, will seek to answer these questions regarding location and identity in a quest for legal certainty and, hence, lowered risk.

The GDPR is likely to have a similar policy influence.[499] In Europe, this move to know-your-customer is being made, ironically enough, in the name of privacy and security. The GDPR intends to create greater obligations for cloud companies vis-à-vis their customers and, as a step toward that goal, is requiring detailed contracts between these parties. The key provisions in this regard are found in Article 28(3) of the GDPR.[500] The mandated contracts are only possible, however, when both parties have detailed information about each other, which means that cloud providers will know more about their customers than under the old legal regime, one that was governed by the European Union's Privacy Directive of 1995.[501]

Whether promoted by the European Union's GDPR or the United States' CLOUD Act, global cloud companies face a know-your-customer future. This step will move cloud providers closer to a paradigm already

---

494. 829 F.3d 197, 203 (2d Cir. 2016).

495. Id.

496. Id. at 230 (Lynch, J., concurring).

497. See H.R. 1625 div. V, § 103(b) (adding § 2713(h)(3)(D)).

498. For the leading work on the professionalization of the privacy industry and the development of a compliance culture in U.S. firms, see Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Ground 74–87 (2015).

499. See GDPR, supra note 396, arts. 60–62 (highlighting the GDPR's provisions on cooperation between supervisory authorities, mutual assistance, and joint operations of supervisory authorities).

500. See id. art. 28(3). For an analysis of the likely content of such contracts, see Nick Westbrook, Internet Technology and Communications, *in* European Data Protection: Law and Practice 317, 320–22 (Eduardo Ustaran ed., 2018).

501. The Directive had limited obligations for processors. A processor was obliged to act on instructions from the controller and to provide security to protect personal data. Council Directive 95/46/EC of the European Parliament and of the Council of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, arts. 16, 17(2), 1995 O.J. (L 281) 43.

present for U.S. banks, which are subject to strict laws and rules requiring them to identify as well as monitor their customers.[502] Instead of relative anonymity in using cloud services, cloud providers will collect identification information about customers. The next move, in the future, might be a requirement to look for "red flags" of suspicious activities. Such scrutiny is now mandated for a broad range of financial institutions under federal banking regulations in the United States.[503]

The impact of this know-your-customer step will spill over into civil litigation. As this Article has shown, when faced with extraterritorial data requests, cloud networks currently can argue that they are not like banks, some of whom have been ordered to comply with such data demands. Today, a non-U.S. cloud network located entirely outside the United States might plausibly liken itself to a storage facility in another country. To the extent, however, that clouds begin to function like banks by collecting detailed identification information from their customers, more courts may order compliance with discovery requests under a comity analysis.

Beyond banking and cloud computing, large internet platform companies are voluntarily adopting a know-your-customer approach to make political discourse more transparent. Both Google and Facebook introduced new rules in spring 2018 that require verification of identity before allowing anyone to run ads on political issues (Facebook)[504] or purchase election ads in the United States (Google).[505] Preservation of the global internet is now encouraging a broad range of steps that reduce user anonymity. As for the CLOUD Act, it acts to preserve the internet as a global space, but does so at the cost of greater collection of customer identification information by cloud providers. Different parties will evaluate the costs and benefits of this approach differently.

---

502. The clearest expression of these obligations is found in the final rules on "Customer Due Diligence Requirements for Financial Institutions," issued by the Financial Crimes Enforcement Network (FinCEN). See 81 Fed. Reg. 29,398 (2016) (codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, 1026).

503. For background on FinCen as well as the Bank Secrecy Act, see Solove & Schwartz, Privacy Law Fundamentals, supra note 210, at 146–47. The post-9/11 USA PATRIOT Act added a strict Customer Identification Program requirement to existing requirements placed on banks. See Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. at 29,399; Fed. Fin. Inst. Examination Council, Core Examination Overview and Procedures for Regulatory Requirements and Related Topics, Bank Secrecy Act/Anti-Money Laundering InfoBase, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_011.htm [https://perma.cc/45TT-Y9SD] (last visited July 26, 2018).

504. Ali Breland, Facebook to Require Verification for Political Ads, Hill (Apr. 6, 2018), http://thehill.com/policy/technology/381988-zuckerberg-announces-new-facebook-measures-to-improve-political-ad [https://perma.cc/PUD6-UTT8].

505. Mallory Locklear, Google Will Verify the Identity of Those Buying US Political Ads, Engadget (May 4, 2018), https://www.engadget.com/2018/05/04/google-verify-identity-those-buying-us-political-ads/ [https://perma.cc/5UBK-74HD].

CONCLUSION

All clouds are not created equal, and different networks dictate distinct outcomes for actual cases involving data access requests. This Article has presented three models of cloud computing: the Data Shard, Data Localization, and Data Trust clouds. This new typology reveals how the same legal authority leads to notably different results in data access cases depending on the technical architecture of the cloud network. In order to treat global clouds accurately and fairly, U.S. courts must take these disparities in technology into account when judging actual cases.

There is also an important international consequence following from use of these different cloud technologies. The writing is on the wall; the rest of the world can and will shift to cloud models that shelter its data beyond the exclusive reach of U.S. law. Cloud technologies now provide a way to route around law. The availability of Data Localization clouds as well as Data Trust clouds demonstrate that companies and individuals outside of the United States have multiple ways to shelter their data beyond the exclusive reach of U.S. law. This analysis points to the grounds for a breakdown in the current Pax Americana for data access rules. This trend spells the end of unilateral decisionmaking by U.S. courts concerning the legal process to be applied when the government or civil litigants seek data stored extraterritorially.

There is a need for new principles in a world of omnipresent global cloud computing. This Article has identified two such concepts. First, a new cloud access regime should treat extraterritorial clouds equally, regardless of where the cloud provider has its headquarters. Among the many reasons for doing so is to prevent a balkanization of the internet, which risks future interoperability snafus and other problems. Second, the legal system should develop new international agreements for legal access to the global cloud based on a concept of reciprocity among nations. An insistence by U.S. policymakers on exclusivity for U.S. legal access rules will be counterproductive: It will drive foreign customers to Data Localization and Data Trust clouds, which will only increase the relevancy of the law of foreign jurisdictions, limit the access of government and litigants in the United States to global cloud data, and harm U.S. tech companies.

As a second and final point, the CLOUD Act of 2018 takes a major step toward incorporation of these principles. Regarding "the level playing field," this statute largely reduces differences in the law's treatment of clouds based on the nationality of the cloud provider or the location of the stored data. Regarding reciprocity, the CLOUD Act has important provisions in this regard. It opens up a new way for foreign governments to access provider data stored in the United States if the foreign state permits the United States the same access rights on its own soil. Currently, much about the required executive agreements is uncertain; there are no such accords at present. One result is already foreseeable, however, and it

is the encouragement of a know-your-customer global regime for the internet. The CLOUD Act creates powerful incentives for cloud providers to be able to document the nationality and location of their users. In return, the location of their own servers becomes less important, which benefits the maintenance or creation of global data networks and promotes an open internet. Yet, the ultimate cost may be one paid in privacy.

APPENDIX: CLOUD MODELS AND LEGAL AUTHORITIES—A SUMMARY

Legal Authority	Data Shard Model	Data Localization Model	Data Trust Model
Fourth Amendment[506]	Information acquisition by the government in the U.S. is likely to be considered a Fourth Amendment search. If the search or seizure occurs outside the U.S., only U.S. customers of Data Shard services will receive Fourth Amendment protection.	Constitutional protections do not apply to searches of property owned by a nonresident alien that is held in a foreign country. However, if the *Verdugo-Urquidez* test is met, Fourth Amendment protections apply for information searched outside the U.S.	Constitutional protections do not apply to searches of property owned by a nonresident alien that is held in a foreign country. However, if the *Verdugo-Urquidez* test is met, Fourth Amendment protections apply for information searched outside the U.S.
Stored Communications Act[507]	The SCA can compel a request for information stored extraterritorially but accessed within the U.S. The CLOUD Act creates a "qualifying foreign government" provision; the provider can refuse requests for data of a non-U.S. person if it would violate foreign law.	The CLOUD Act extends the SCA to information *outside* the U.S. The provider can move to quash. The CLOUD Act creates two new provisions: (1) general comity analysis, and (2) "qualifying foreign government."	Data Trusts are likely to have greater insulation from extraterritorial use of the SCA post–CLOUD Act. Data Trustees, not cloud providers, will handle requests for customer data. One key issue is the "possession, custody, or control" language in the CLOUD Act.
MLATs[508]	The MLAT process is irrelevant for a Data Shard cloud if a court rules that the locus of the search of this cloud is domestic in nature.	Assuming that a court decides that access to cloud data occurs extraterritorially, as *Microsoft Ireland* did, the MLAT process would proceed under the specific national and regional agreements that are applicable.	An MLAT process for a Data Trust cloud would be directed to the Data Trustee, not the cloud provider. Requests would be judged by the law of the Data Trustee's local jurisdiction.

506. See supra section II.A.1.
507. See supra section II.A.2.
508. See supra section II.A.3.

Legal Authority	Data Shard Model	Data Localization Model	Data Trust Model
Administrative or Grand Jury Subpoenas[509]	If a Data Shard cloud is accessed within the U.S., the SCA will apply and bar use of a subpoena. If the cloud is accessed from outside the U.S., the SCA will not apply and subpoenas will be permitted.	In *Microsoft Ireland*, the Second Circuit indicated in dicta that it did not think that a subpoena should be used to order access to information in a Data Localization cloud when held outside the U.S. by a party who is "merely a caretaker for another individual."	Data Trusts will likely enjoy greater protection from subpoena requests because the ability to access information in the network is separate from other aspects of managing the data.
Foreign Surveillance[510]	If a Data Shard cloud is accessed within the U.S., it will be subject to provisions of FISA and the FAA regarding searches of stored content in the U.S. A Data Shard provider will be subject to the same requirements as any other "electronic service provider" under these statutes.	A Data Localization cloud whose content can be accessed from the U.S. likely falls under FISA. There is, however, no released FISC opinion regarding this precise issue.	U.S. intelligence will be unlikely to be able to compel cooperation from a non-U.S. Data Trust cloud under the FAA. Pursuant to Executive Order 12,333, U.S. intelligence may surveil information stored electronically. An "arms race" may follow with encryption of Data Trust clouds as a key issue.
Hague Convention[511]	The letters rogatory process, pursuant to the Hague Convention, is not relevant to the Data Shard cloud because access to information in such a cloud is exclusively from the U.S. Normal domestic discovery will be controlled by the Federal Rules of Civil Procedure.	The Hague Convention is implicated by a Data Localization cloud. A letter requesting evidence will be served from a U.S. court to a judicial authority in the country where the cloud is located.	A Data Trust provides additional protection to its users; it insulates the cloud provider from these data requests and shifts them to the local, non-U.S. Data Trustee. A letter requesting evidence will be served from a U.S. court to a judicial authority in the country where the cloud is located.

509. See supra section II.A.4.
510. See supra section II.A.5.
511. See supra section II.B.1.

Legal Authority	Data Shard Model	Data Localization Model	Data Trust Model
Federal Rules of Civil Procedure[512]	If the Data Shard cloud is deemed to be accessed in the U.S., a civil litigation request to a Data Shard provider may be treated as subject to the same rules as standard domestic requests.	Non-U.S. data protection law will be important to the comity analysis for a Data Localization cloud.	Non-U.S. data protection law will be important to the comity analysis for a Data Trust cloud. This type of cloud may fare better under a comity analysis than a Data Localization cloud. A foreign Data Trustee could point to an "important interest of the state" in a foreign discovery request.

GLOSSARY

Data Shard Model: A company stores information in the cloud in multiple international locations; the network itself dynamically distributes data to domestic and international servers.

Data Localization Model: A company stores information in a cloud that is restricted to a single country or region.

Data Trust Model: A company bifurcates network management (controlled by the Data Manager) from the ability to access data (exclusively held by the Data Trustee).

512. See supra section II.B.2.