Legal Access to the Global Cloud

By Paul M. Schwartz*

118 Columbia Law Review (forthcoming 2018)

* Jefferson E. Peyser Professor of Law at UC Berkeley School of Law; Director, Berkeley Center for Law & Technology. I would like to thank James X. Dempsey, Stavros Gadinis, Mark Gergen, Sonya Katyal, Katrina Linos, Karl-Nikolaus Peifer, 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 Thyssen Foundation for their research support.

INTRODUCTION

Cloud computing is one of the fastest growing areas of information technology. Data is 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 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] One case regarding this statute, *Microsoft Ireland*, is now on appeal before the Supreme Court,[6] which will decide the extra-territorial scope for SCA warrants. Yet, at best, this case will settle only the question of the international reach of a single U.S. legal statute. In this way, *Microsoft Ireland* will continue the tradition of a siloed approach to evaluating U.S. law concerning the global cloud. But policymakers must take into account the full range of legal authorities to understand the effectiveness of extra-territorial access rules. This Article carries out this task.

---

[1] *Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 5–6 (Dec. 7, 2017) (statement of Christopher A. Wray, Director, FBI).

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

[3] 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); Jennifer Daskal, *Law Enforcement Access to Data Across Borders*, 8 J.NAT'L SEC. L. & POLICY 473 (2016); 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., Aug. 16, 2013, at A1; 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.

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

[6] United States v. Microsoft, 138 S. Ct. 356 (2017) (granting certiorari).

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.[7] 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.[8]

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.[9] The old system was one of unilateral reliance by the U.S. on its own rules for extra-territorial 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 U.S.[10] This Article demonstrates the grounds for the weakening and future collapse of the current "Pax Americana" for data access rules.

It then develops principles for constructing a new legal order for a world of omnipresent cloud computing. First, U.S. access rules should be supplemented by development of new international agreements concerning extra-territorial data access.[11] These agreements should first be negotiated with individual nations whose legal rules concerning access to cloud information are closest to that of the United States. Second, the U.S. should treat extra-territorial clouds equally, regardless of the nationality of the corporate provider.[12] Any other approach would hasten Internet balkanization and encourage non-U.S. customers to favor cloud providers that are not headquartered in the U.S. Such a development would be counter-productive; it would reduce access to global clouds by U.S. law enforcement, national security agencies, and civil litigants.

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 first case, *Microsoft Ireland*, is a Second Circuit Decision now on certiorari before the Supreme Court.[13] The second case, *Google Pennsylvania*, comes to a contrary result than *Microsoft Ireland*.[14] *Google Pennsylvania* is one of a series

---

[7] See *infra* Part II.

[8] *Id.*

[9] On the past reliance on U.S. decision-making for Internet governance, which this Article calls "Pax Americana" for the Internet, see JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? 13–46 (2008).

[10] See *infra* Part II.

[11] See *infra* Part III.B.1.

[12] See *infra* Part III.B.2.

[13] United States v. Microsoft, 138 S. Ct. 356 (2017) (granting certiorari). For the path to the Supreme Court for this decision, see *In re* Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), *reh'g denied*, Microsoft Corp. v. United States, 855 F.3d 53 (2d Cir. 2017) [hereinafter *Microsoft Ireland*]; *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 (E.D. Wis. Feb. 21, 2017) (analyzing the Second Circuit's denial of a rehearing en banc before adopting its reasoning).

[14] In re Search Warrant No. 16-960-M-01 to Google, 232 F. Supp.3d 708 (E.D. Pa. 2017) [hereinafter *Google Pennsylvania*].

of important judicial decisions reaching the same conclusion for clouds run by Google; these judgments find that the SCA extends to extra-territorial clouds.[15] While *Microsoft Ireland* and *Google Pennsylvania* are polar opposites regarding their outcomes, they reflect the same basic limitation: these cases are based on a flawed understanding of technology. *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 the important distinctions among cloud technology.[16]

This Article argues for a new approach. Legal decision making 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 U.S.[17] U.S. companies quickly moved beyond this U.S.-centric approach, however, and developed globally distributed cloud networks.[18] 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 Shards, Data Localization, and Data Trust clouds.[19]

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

---

[15] 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 (E.D. Wis. June 30, 2017); In the Matter of Search of Info. Associated with [redacted]@gmail.com, No. 16-mj-757, 2017 WL 2480752 (D.D.C. June 2, 2017); *In re* Search of Content that is Stored at Premises Controlled by Google, No. 16-mc-80263, 2017 WL 1487625 (N.D. Cal. Apr. 19, 2017).

[16] 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 (2015) (global telecommunications make territoriality a meaningless concept for deciding data access questions for cloud information), *with* Woods, *supra* note 3, at 735 (traditional legal tools can be used to determine data access questions for cloud information). For other scholarship that examines the issue of territoriality in the Internet age and other issues related to global data access, see Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313, 388 (2013); David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide*, 14 INT'L J. CONST. L. 220, 231 (2016); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2013); Ned Schultheis, *Warrants in the Clouds*, 9 BROOK. J. CORP. FIN. & COM. L. 661, 683–84 (2015); *Recent Case: District Court Holds that SCA Warrant Obligates U.S. Provider to Produce Emails Stored on Foreign servers*, 128 HARV. L. REV. 1019, 1026 (2015).

[17] ANTHONY VELTE ET AL., CLOUD COMPUTING 117 (2010).

[18] *See AWS Global Infrastructure*, AMAZON, https://aws.amazon.com/about-aws/global-infrastructure (first U.S. location of AWS was in 2006 with locations following in Ireland in 2007 and Singapore in 2010); *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 (Microsoft opened its first international cloud center, one in Dublin, Ireland, in 2009).

[19] See *infra* Part I.B.

dispersed network and keeps it in constant motion among different data centers.[20] A Data Localization cloud stores data outside the U.S. It is also typically marketed to customers outside the U.S. This approach permits customers to isolate data outside the geographical boundaries of the U.S.[21] 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.[22] Through encryption and the law of trusts, the trustee effectively brings such cloud data under its domestic, non-U.S. law.

In its second Part, this Article goes beyond the SCA to explore the full range of U.S. legal authorities that permit parties to seek digital information held abroad. Looking at requests by government 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 where 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 to unilateral decision making by U.S. courts concerning legal process to be applied when the government or civil litigants seek data stored extra-territorially.

Finally, in its third Part, this Article presents a set of principles for a new U.S. approach. Its first such principle concerns the need for international cooperation around the concept of reciprocity. The U.S. should develop a series of international agreements about access to global cloud data; the first step should be U.S. negotiations with countries that most closely share its values. A current bi-partisan bill, the International Communications Privacy Act (ICPA) would pave the way for such agreements.[23] This statute supplements the current landscape of legal access rules by opening the door for the U.S. to negotiate separate Law Enforcement Cooperation Agreements (LECAs) with other nations. The U.S. and United Kingdom are now developing such an agreement.[24] With LECAs in place, there would be beneficial results regarding the current treatment of Data Shards, Data Localization, and Data Trust clouds. In particular, LECAs have the potential both to permit reasonable law enforcement access to cloud data and to promote a global and interoperable Internet.

As a second principle, this Article argues that U.S. law should treat extra-territorial data requests equally, regardless of the location of the cloud provider's headquarters.[25] One benefit of this approach would be to avoid putting U.S.-based companies between a "rock and hard place" concerning conflict of laws. At present, U.S. companies can face conflicting obligations with regard to

---

[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] International Communications Privacy Act (ICPA), S. 2986, 114th Cong. (2016).
[24] *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. (2016), https://archive.org/stream/gov.gpo.fdsys.CHRG-114hhrg98827/CHRG-114hhrg98827_djvu.txt.
[25] See *infra* Part III.2.

a single item of data.[26] U.S. law should not create stricter legal standards for the extra-territorial customer data of U.S.-based cloud companies. A legal approach that permitted a "level playing field" for global cloud 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.

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."[27] 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.[28] Such distributed computing permits rapid expansion of data processing to handle a greater load or take on new tasks.[29] Cloud computing also transfers computing responsibilities from one party to another and achieves new efficiencies in computing management.[30] Today, the cloud is ubiquitous. A Pew Foundation poll already identifies a future in which all of us access software and share information through cloud servers rather than personal computers.[31]

Beyond this description, courts in extra-territorial access cases tend to look at other aspects of the cloud. In particular, these courts have focused on where cloud data is *stored*, and how and where companies *access* it. 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 caselaw 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, one now on appeal to the Supreme Court, 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. Moreover, these cases and accompanying scholarship about territoriality fail to explore a range of normative questions about different kinds of extra-territorial clouds. This Part then sets out its three cloud models: these are the Data Shard,

---

[26] For a discussion of this conflict, see Volkswagen, A.G. v. Valdez, 909 S.W.2d 900 (Tex. 1995).
[27] *NIST Cloud Computing Program—NCCP*, U.S. DEP'T OF COMMERCE: NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/programs-projects/cloud-computing (last visited Apr. 19, 2017).
[28] For an introduction, see VELTE ET AL., *supra* note 17, at 3–4.
[29] Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1625, 1628–32 (2013).
[30] *Id.* at 1632–34; VELTE ET AL., *supra* note 17, at 77–78.
[31] JANNA ANDERSON & LEE RAINIE, PEW RESEARCH CTR., THE FUTURE OF CLOUD COMPUTING 8 (2010), http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing.

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 initial lessons.

A. Emerging Caselaw: Microsoft Ireland *and* Google Pennsylvania

Federal electronic surveillance law for domestic law enforcement consists of three statutes—the Wiretap Act, the Stored Communications Act (SCA), and the Pen Register Act.[32] Of these, the SCA is the most relevant regarding access to cloud information.[33] There are many open questions regarding this statute's applicability to information stored in a cloud located outside the U.S. 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 extra-territorial data center.[34] This case is now on appeal before the Supreme Court.[35] In *Google Pennsylvania*, the Eastern District of Pennsylvania held that the SCA required a cloud provider to supply the government with information distributed in its global network.[36] Two cases, two results. There is far more here, however, than this initial snapshot indicates. First, this litigation touches on matters of multi-billion dollar importance for U.S. companies and implicates areas of major concern for U.S. security agencies and law enforcement agencies. Second, there are significant underlying dissimilarities between these two cases. All clouds are not created equal.

Regarding the importance of this area of law, a multi-billion dollar market exists for the international clouds of U.S. companies, and U.S. law regarding access to personal data strongly affects this market. There is also 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.[37] In response, many customers of cloud services outside of the U.S. developed newfound interest in

---

[32] For an overview, see DANIEL SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 344–52 (6th ed. 2017).

[33] 18 U.S.C. §§ 2701–2712 (2012) (Stored Communications Act).

[34] *Microsoft Ireland*, 829 F.3d 197 (2d. Cir. 2016).

[35] United States v. Microsoft, 138 S. Ct. 356 (2017) (granting certiorari).

[36] *Google Pennsylvania*, 232 F. Supp.3d 708, 709 (E.D. Pa. 2017).

[37] For a discussion by the European Court of Justice of the Snowden leaks, see Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650. The Guardian has an 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; Ewan Macaskill & Gabriel Dance, *NSA Files Decoded*, GUARDIAN (Nov. 1, 2013) at https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

using clouds that avoided the territory of the U.S. Post-Snowden, Forrester Research estimated that U.S. businesses loss up to $180 billion due to the distrust in some countries towards U.S. tech companies.[38]

In a similarly high-profile fashion, national security agencies and law enforcement in the U.S. consider this area of law as 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, posing a possible Catch-22. As Magistrate Judge Rueter observed in *Google Pennsylvania* regarding the kind of cloud at use in that case: "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."[39] 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 with the result of restricting access by national security and law enforcement agencies to communications despite having legal authority to do so.[40] Similarly, cloud data stored extra-territorially 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, the discussion of 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. In *Google Pennsylvania*, Judge Rueter held that a warrant compelling Google to disclose information was not an extra-territorial application of the SCA.[41] His analysis of the question of extra-territoriality turned on where the *access* to the information would take place.[42] Google argued that the warrants at issue could not compel it to produce records that were stored outside the U.S.[43] Functionally, however, Google could only access the extra-territorially stored information through its Legal Investigations Support Team in the United States.[44] 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.[45] Under the facts of the case, therefore, the judge found 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."[46] Magistrate

---

[38] Clint Boulton, *NSA's Prism Could Cost IT Service Market $180 Billion*, WALL ST. J. (Aug. 16, 2013), https://blogs.wsj.com/cio/2013/08/16/nsas-prism-could-cost-it-service-market-180-billion.
[39] *Google Pennsylvania*, 232 F.Supp.3d at 725.
[40] In the Matter of 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).
[41] *Google Pennsylvania*, 232 F.Supp.3d at 725.
[42] *Id.*
[43] *Id.* at 710.
[44] *Id.* at 713.
[45] *Id.* at 722.
[46] *Id.*

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.[47] The answer to both questions was the same: these activities would take place within the U.S.

Conversely, in *Microsoft Ireland*, the Second Circuit held that the SCA did not require Microsoft to give the government information from its non-U.S. data center.[48] In its interpretation of the underlying statute, the appellate court ruled that Congress did not intend for SCA warrants to have a global reach.[49] Regarding the *location* of the sought after data, the Second Circuit found that the customer content was stored in Ireland.[50] For the court, "even messages stored in the 'cloud' have a discernible physical location."[51] In the case of Microsoft, the relevant information was located at its data center in Dublin, Ireland.

These are different tests: one looks to the issue of data access, the other to the data location. The cases cannot be understood, however, without attention to the different underlying cloud management models. *Google Pennsylvania* involved a type of cloud where the cloud provider stores informationally globally and domestically.[52] It breaks data into small components, or shards, which the system routes around the globe, with different bits shifted between various locations.[53] This Article will term this model, the "Data Shard cloud." In contrast, *Microsoft Ireland* involved a type of cloud where information was stored extra-territorially.[54] This Article terms this second model, the "Data Localization cloud." As will be discussed below, a pure Data Localization cloud is one in which the information can only be accessed in the same geographic location as where the data is stored.[55] Yet, the Second Circuit in *Microsoft Ireland* did not consider whether pure Data Localization would raise different issues, and whether and how to assess the partial localization in that case.

A final distinction exists between these two cases. This concerns the practical consequences of a finding of "no access" under the SCA 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.[56] As this Article discusses below,[57] under MLATs, a public authority can ask for the assistance of the country in which the sought-after data is held, and the request will be processed

---

[47] *Id.*
[48] *Microsoft Ireland*, 829 F.3d 197, 216 (2d Cir. 2016).
[49] *Id.*
[50] *Id.* at 221.
[51] *Id.* at 220 n.28.
[52] *Google Pennsylvania*, 232 F. Supp.3d 708, 723 (E.D. Pa. 2017).
[53] *Id.*
[54] *Microsoft Ireland*, 829 F.3d 197, 221 (2d Cir. 2016).
[55] There is a twist in *Microsoft Ireland*, which is that the precise model at stake was a partial or incomplete one. *Id.* at 230 (Lynch, J., concurring). This Article explores this point below.
[56] *Id.*
[57] See *infra* at Part II.A.3.

in the foreign country consistent with the domestic law of that country.[58] In *Google Pennsylvania*, however, Judge Rueter was concerned about the absence of any such mechanism.[59] In his opinion, Data Shards clouds emerge as a new dimension of the "Going Dark" problem.[60]

B. Data Shards, Data Localization, and Data Trusts

As discussed above, different technical models for cloud computing are present in the *Microsoft Ireland* and *Google Pennsylvania* 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.

In the Data Shard cloud, a company stores information in the cloud in multiple international locations.[61] 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. 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."[62] Because data is inherently scattered under this approach, national boundaries are largely irrelevant. The data is shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world.[63]

The Google Cloud provides a leading example of the Data Shard approach. As the court in *Google Pennsylvania* noted, Google operated a cloud network that "automatically move[d] data from one location to another . . . to optimize for performance, reliability, and other efficiencies."[64] 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."[65] A user's information might be found

---

[58] *MLAT World Map, Mutual Legal Assistance Treaties*, https://mlat.info (last visited Jan 27, 2017). For an excellent overview of the MLAT process, see Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications*, 71 N.Y.U. ANN. SURV. AM. L. 687 (2017).

[59] *Google Pennsylvania*, 232 F. Supp.3d 708, 724 (E.D. Pa. 2017).

[60] *Id.*

[61] For discussion of data sharing, see Sikha Bagui & Loi Tang Nguyen, *Database Sharding*, 5 INT'L J. CLOUD APPLICATIONS & COMPUTING 36 (2015); Patrick Ryan et al., *Trust in the Cloud*, 28 COMPUTER L. & SEC. REV. 513, 520 (2012).

[62] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 679 (2015).

[63] Ryan et al., *supra* note 60, at 520.

[64] *Google Pennsylvania*, 232 F.Supp.3d at 723.

[65] *Id.* at 724.

in the U.S. as well as on Google servers throughout the world.[66] Moreover, under its Data Shard Model, Google can only access information in its cloud from the U.S.[67] Hence, it *locates* cloud information in shifting locations throughout the world but *accesses* cloud information exclusively from the U.S.[68]

In Data Localization, the second model, a company stores information in a cloud that is restricted to a single country or region.[69] A number of U.S. cloud providers, including Amazon Web Services (AWS) and Microsoft, take this approach. For example, AWS now has forty-nine "availability zones" around the world. It most recently opened a European region in France.[70] German telecommunication companies have also developed clouds that store data exclusively in Germany.[71] As one trade publication explains, "[th]e main selling points for cloud operators in Germany are location, location, and location."[72] An important distinction should be made, however, between data localization as a technical and as a legal matter. 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 that 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.[73]

A Data Localization model was at the center of the *Microsoft Ireland* litigation.[74] 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.[75] Thus far, this Article has only discussed 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.[76] In that case, Microsoft technicians and attorneys in both Dublin and Redmond, Washington could access the sought-after information.[77] In *Microsoft Ireland*, the *location* of the data was Ireland, but *access* to the information could take

---

[66] *Id.* at 712–13.
[67] *Id.*
[68] *Id.*
[69] For a critical account of the "push for data localization," see Patrick Ryan et al., *When the Cloud Goes Local*, COMPUTER 57 (Dec. 2013).
[70] 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.
[71] 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.
[72] *Id.*
[73] Chander & Lê, *supra* note 62.
[74] *Microsoft Ireland*, 829 F.3d 197 (2d Cir. 2016).
[75] *Id.* at 203.
[76] *See id.* at 197.
[77] As Judge Gerald Lynch noted in his concurrence in *Microsoft Ireland*, Microsoft employees located domestically were capable of reviewing the records in question "and [could] provide the relevant materials to the demanding government agency, without ever leaving their desks in the United States." *Id.* at 229–30 (Lynch, J., concurring).

place either from Dublin or Redmond.[78] Unlike the cloud model at issue in *Microsoft Ireland*, other Data Localization clouds are complete. For example, cloud services offered by AWS and Microsoft's Regional European Union (EU) cloud are not accessible from the U.S.[79]

Finally, the Data Trust model, the third approach, builds on and further refines the Data Localization approach.[80] 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.[81] 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 extra-territorial *location* of information and an extra-territorial *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.

At present, only Microsoft makes use of the Data Trust model.[82] It offers a "Microsoft German Cloud" to customers in the European Union and European Economic Area.[83] The Microsoft Data Trust stores customer data exclusively within Germany, in data centers located in Frankfurt-am-Main and Magdeburg. Most significantly, T-Systems is the trustee for the stored information, which means it alone controls the ability to access the network.[84] The trust arrangement, which is a contractual obligation between the two parties, significantly restricts the access of Microsoft Germany to the information in its cloud.[85] Beyond law,

---

[78] *Id.*

[79] *Azure Germany Cloud Computing*, MICROSOFT AZURE, https://azure.microsoft.com/en-us/overview/clouds/germany.

[80] One early discussion of cloud computing pointed to a "Cloud Cube Model" in which one element concerned "ownership of technology." BARRIE SOSINSKY, CLOUD COMPUTING BIBLE 6 (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 also is somewhat similar to the idea of the Data Trust. NAYAN B. RUPARELIA, CLOUD COMPUTING 119 (2016).

[81] A Data Trust model, the Microsoft German Cloud, has been the subject of legal analysis in the German legal literature concerning cloud privacy. See Paul M. Schwartz & Karl-Nikolaus Peifer, *Datentreuhändermodelle—Sicherheit vor Herausgabeverlangen US-amerikanischer Behörden und Gerichte?*, COMPUTER UND RECHT 165 (2017) ("Data Fiduciary Model—Protection from Data Requests of U.S. Governmental Authorities and Courts?"); Michael Rath et al., *Die neue Microsoft Cloud in Deutschland mit Datentreuhand als Schutzschild gegen NSA & Co?*, COMPUTER UND RECHT 98 (2016) ("The New Microsoft Cloud in Germany: a Data Fiduciary as Protective Shield against the NSA and Company?").

[82] MICROSOFT CLOUD GERMANY DATASHEET 2, https://go.microsoft.com/fwlink/?LinkId=839380&clcid=0x409.

[83] *Id.*

[84] *Id.*

[85] See MICROSOFT AZURE, *supra* note 79 ("An independent data trustee controls access to all customer data in the Azure Germany datacenters. T-Systems International GmbH, a subsidiary of

moreover, customer data in the Microsoft German cloud is encrypted, and only T-Systems holds the keys to the data.[86] 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. 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.[87] Moreover, Microsoft can access the information only for a limited number of reasons, such as for network maintenance, and can do so only under the supervision of T-Systems. Moreover, 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. Finally, as noted earlier, the data in the system is 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.

Thus, the Microsoft German Cloud 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 caselaw 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

---

Deutsche Telekom and an experienced, well-respected IT provider incorporated in Germany, serves as trustee, protecting disclosure of data to third parties except as the customer directs or as required by German law. Even Microsoft does not have access to customer data or the datacenters without approval from and supervision by the German data trustee.").

[86] *Microsoft Trust Center, Encryption*, MICROSOFT, https://www.microsoft.com/en-us/trustcenter/security/encryption.

[87] *Id.* For an analysis of these provisions, see Schwartz & Peifer, *supra* note 81, at 170–71.

discussion are 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.

On one side in the debate, Woods views data as a physical object. As he puts it: "the 'cloud' is actually a network of storage drives bolted to a particular territory."[88] In the context of 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."[89] In his view, some scholars in this area mistakenly begin from a starting point of "data exceptionalism."[90] 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.[91]

This perspective is unconvincing for Woods, who points to other assets, such as money in a bank account, that are similarly mobile and divisible.[92] 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."[93] Indeed, Woods would go so far to argue that cloud data that is not "debt, money, or other assets" does not present a hard case for the legal system.[94] Unlike a variety of intangible assets, it has a physical presence; it resides on "physical drives that can be seized."[95]

Woods proposes that a standard comity test be applied to data in the global cloud. This analysis considers whether the nation seeking the information stored in the cloud "has an interest in the data that outweighs competing state interests."[96] In the classic international comity approach, courts decide whether or not another jurisdiction's interests weigh against the transfer of the sought-after evidence.[97] Although such a test can be unpredictable, Woods finds any possible uncertainty to be "a small price to pay for 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."[98] Woods does not explain, however, if decentralization is merely the best likely solution, a second-best solution, or whether it has merits of its own in this context.

---

[88] Woods, *supra* note 3, at 735.
[89] *Id.*
[90] *Id.* at 788.
[91] *Id.* at 788–89.
[92] *Id.* at 729.
[93] *Id.* at 758.
[94] *Id.*
[95] *Id.* at 761.
[96] *Id.* at 774.
[97] *Id.* at 778.
[98] *Id.*

In addition, Woods sees a need for reciprocity among foreign legal authorities in recognizing and enforcing foreign judgments.[99] 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 govern requests for data expeditiously."[100] Like his judicial comity analysis, the policy solution here also will 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."[101] As the mention of "pixie dust" indicates, Woods is skeptical of the merits of a global treaty for access to international cloud data.[102] 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.[103] Additionally, a treaty regime would likely reach only the lowest common-denominator to ensure that all parties sign on to the agreement.[104] 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 U.S.[105]

In contrast to Woods, Jennifer Daskal views the "unterritoriality of data" as raising fundamentally new challenges.[106] She argues that "data undermines longstanding assumptions about the link between data location and the rights and obligations that should apply."[107] Digital information is different because data now flow across international borders with "ease, speed, and unpredictability."[108] Moreover, there is a physical disconnect between the location of the data and the location of the user. Indeed, the cloud user may not even know where her information is located. Daskal states: "[w]hereas 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."[109] In sum, "[d]ata is shaking territoriality at its core."[110]

Daskal warns us 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

---

[99] *Id.*
[100] *Id.*
[101] *Id.* at 781.
[102] *Id.*
[103] *Id.* at 788.
[104] *Id.*
[105] See Daskal, *supra* note 3, at 490 (warning of a "free-for-all" which would harm human rights).
[106] Daskal, *supra* note 16, at 326.
[107] *Id.*
[108] *Id.* at 329.
[109] *Id.* at 397.
[110] *Id.*

nations."[111] Daskal further argues that this result will impose another set of costs, including "the balkanization of the Internet into multiple, closed off systems."[112] Her policy solution is to call for "a series of bilateral or multilateral agreements among a handful of like-minded nations."[113] These solutions depend on jurisdictional tests that apply to both regulatory and compulsory process goals. In shaping these solutions, Congress and the Executive should both be involved.

Daskal also rejects data location as the sole determinant of the rules that should apply.[114] 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.[115] Daskal suggests that such factors might supplement or substitute for other factors. Another possible jurisdictional approach would look to "the place where the company controlling the data operates or maintains its headquarters; user nationality; or user location."[116] Under such a framework, many jurisdictional flowers would bloom in place of the current approach of "unilateral, extraterritorial law enforcement."[117] The hope? In time, a series of tailored, superior approaches would emerge to the "unterritoriality" of data.[118]

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. 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, the issue of propertization of personal information is highly contested.[119] There is also no agreement in the U.S. as to the extent that personal information should be viewed as the property of an individual, and, even more to the point, unclear how propertization would clarify questions relating to access to global cloud data.

At the same time, data in the cloud raises different issues than, for example, data in a filing cabinet. Most crucially, "one size does not fill all" when

---

[111] *Id.* at 326.
[112] *Id.* at 333–34.
[113] *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." The government can rebut this "presumptive Fourth Amendment" by establishing that none of the parties to the communication is a U.S. person. *Id.* at 383.
[114] *Id.* at 395.
[115] *Id.*
[116] *Id.*
[117] *Id.* at 333.
[118] *Id.* at 333–34.
[119] For a window into the debate about personal data propertization, see Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2005 (2004).

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 "unterritoriality of data," some clouds do not call into question the "here" and "there."[120] 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.[121] Such data operations, which this Article terms complete Data Localization clouds, are not "shaking territoriality at its core."[122] 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).

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. Additional examples from *Microsoft Ireland* are possible. We have already seen Judge Susan Carney's insistence that "even messages stored in the 'cloud' have a discernible physical location."[123] For a Data Shard cloud, however, such a location is fleetingly evanescent.

The Second Circuit's denial of a petition for a rehearing en banc in *Microsoft Ireland* further illustrates the judicial struggle to understand different cloud models.[124] The dissenting judges in the rehearing struggled 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 alluded to the kind of network that this Article terms "the Data Shard model" and appeared to believe that such a network might be present in the case before him.[125] Judge Jacobs was even willing to jettison the question of location of cloud data entirely. In a *cri de coeur,* he warned against those who would "reify the notional."[126] In his view, "[l]ocalizing the data in Ireland is not marginally more useful than thinking of Santa Claus as a denizen of the North Pole."[127] In case we missed the point, Judge Jacobs provided a final dramatic flourish: "Where are the snows of yesteryear?"[128]

Second, Data Trustee clouds point to an additional lesson previously mentioned—namely divisibility. It is now possible to separate management of

---

[120] Daskal, *supra* note 16, at 326.

[121] 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 search of a computer to a search of a locked footlocker).

[122] Daskal, *supra* note 16, at 397.

[123] Microsoft Ireland, 829 F.3d 197, 220 n.28. (2d Cir. 2016).

[124] See generally *Microsoft Ireland*, 855 F.3d 53 (2d Cir. 2017) (rehearing en banc denied).

[125] *Id.* at 61–62 (Jacobs, J., dissent).

[126] *Id.* at 62.

[127] *Id.*

[128] *Id.* As comparative literature majors and fans of medieval French literature will recognize, Judge Jacobs is quoting François Villon: "*Mais où sont les neiges d'antan*." 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 provider, the situation would be quite different." *Id.* at 76 (Droney, J., dissent).

networked information from the ability to access it. This division can be achieved through technology (software that places access controls in the hands of a Data Trustee). It can be further bolstered through domestic law (through the creation of a formal data trust). 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.[129] 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, where network management structures it, and legal data localization, where a statute or other kind of legal mechanism mandates it. 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 home-grown 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.[130] One benefit will be to end the "tacit transmission of our information to U.S. intelligence services."[131] 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 EU.[132]

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 Peter Swire and Justin Hemmings write, "[C]ompanies have sought ways to show global customers their careful stewardship of private data."[133] U.S. tech companies have felt the losses from these marketplace decisions and are now responding by offering localized services. In a joint amicus brief before the Second Circuit in *Microsoft Ireland*, Verizon, Cisco, Salesforce and other corporations cautioned about the counter-productive impact of extending extra-territorial effect to the SCA. The tech companies warned: "[f]oreign 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 . . . ."[134]

---

[129] The basic point: 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* at Part III.A.

[130] STEFAN AUST & THOMAS AMMANN, DIGITALE DIKTATUR 341 (2014) ("Digital Dictatorship").

[131] *Id.*

[132] *Id.*

[133] Swire & Hemmings, *supra* note 58, at 714.

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

Data localization is also being driven by legal requirements. European law already contains stray bits of legal data localization. For example, a recent German law requires providers of publicly available telecommunications services to store certain traffic data within Germany.[135] Outside the EU, non-democratic countries, such as Russia, have enacted different kinds of legal data localization requirements.[136] There are multiple reasons for these laws, including protectionism for native technology companies and making surveillance easier for domestic intelligence agencies and law enforcement agencies.[137] The perverse result, as Chander & Lê argue, is that the centralizing of user information can lighten the surveillance burden for outside intelligence agencies.[138]

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 U.S. 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; policymakers must consider the full range of legal authorities and how law and technological 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 extra-territorial access to data held in non-U.S. clouds.

II.
EVALUATING LEGAL AUTHORITIES FOR EXTRA-TERRITORIAL ACCESS TO DATA

This Article argues that different cloud management models raise distinct issues concerning extra-territorial 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 MLAT's, which will incorporate foreign law into data access questions. Additionally, there

---

[135] Lothar Determann & Michaela Weigl, *Data Residency Requirements Creeping into German Law*, BNA PRIVACY LAW REPORTER (Apr. 11, 2016).
[136] Chander & Lê, *supra* note 62, at 717–19.
[137] Swire & Hemmings, *supra* note 58, at 712.
[138] Chander & Lê, *supra* note 62, at 717.

will be increased incentives for non-U.S. customers, who are concerned about U.S. access to their data, to favor 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. Extra-Territorial 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."[139] The Fourth Amendment also contains a provision stating that no warrants shall be issued except "upon probable cause."[140] But in their role of restricting governmental activities, these interests are limited in their ability to safeguard data privacy rights against extra-territorial surveillance.

The Fourth Amendment is a restriction on governmental power, not a grant of power. Accordingly, the authority to execute search warrants on foreign soils must be located elsewhere.[141] For example, *Microsoft Ireland* examined whether the SCA could provide such authority to compel a company to disclose data stored outside the U.S.[142] 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.[143] 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."[144] This axiom is reflected

---

[139] U.S. CONST. amend. IV.
[140] *Id.*
[141] *See* FED. R. CRIM. P. 41(b)(5) (permitting warrants for searches on property outside the U.S. owned or leased by the U.S. for diplomatic or consular purposes).
[142] *Microsoft Ireland*, 829 F.3d 197 (2d Cir. 2016).
[143] 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* United States v. Gorshkov, 2001 WL 1024026 (W. D. Wash. 2001) (FBI agents in U.S. accessed criminal suspect's server in Russia; Russia indicted the FBI agents, which was a largely symbolic action.).
[144] Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1082–83 (2017).

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."[145]

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 U.S., 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 made it clear that the warrant clause of the Fourth Amendment has no extra-territorial effect.[146] While a warrant is not required for searches outside the U.S., *Verdugo-Urquidez* has also been interpreted to mean that the Amendment's reasonableness requirement applies to searches outside the U.S., but only if they involve a U.S. person or a person with significant contacts with the U.S.[147] 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.[148] In contrast, the Second and Seventh Circuits hold that Fourth Amendment reasonableness for extra-territorial searches requires a balancing of the government's need for the information and the privacy interest at stake.[149] Most crucially, the extent of Fourth Amendment protection will vary depending on whether a cloud is organized as a Data Shard, Data Localization, or a Data Trust network.

Data Shards. We begin with an analysis of a governmental request for information located outside the U.S. and stored in a 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 a search and, hence, does not implicate the Fourth Amendment.[150]

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.[151] Similarly, Orin Kerr, the leading scholar of electronic criminal procedure, has

---

[145] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 432(2) (AM. LAW INST. 1987).
[146] 494 U.S. 259 (1990).
[147] *See id.* at 274–75
[148] *See* United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987).
[149] *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) (balancing the appellant's Fourth Amendment rights against the alleged unreasonable cooperation between the United States Drug Enforcement Agency and the Turkish National Police).
[150] *See, e.g.*, Minnesota v. Dickerson, 508 U.S. 366 (1993).
[151] Google Pennsylvania, 232 F. Supp. 3d 708, 721 (E.D. Pa. 2017).

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."[152]

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 U.S.[153] If the answer is yes, the Fourth Amendment safeguards such information because a search conducted within the U.S. 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.

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 extra-territorial search of data belonging to a non-U.S. person generally does not implicate the Fourth Amendment.[154] In other words, these constitutional protections do not apply to searches of property held in a location outside the U.S. 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 Localized or Data Trust Cloud and searched outside the U.S. 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." Under the Ninth Circuit's approach, which looks to compliance with foreign law in the jurisdiction where the search occurs, the Data Trustee will only be obliged to comply with search requests that fulfill the requirements of foreign domestic law.[155] As for the Data Cloud 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 the Microsoft German Cloud, U.S. courts that follow the Ninth Circuit are likely to honor the validity of the trustee model.

There is less certainty regarding the test shared by the Second and Seventh Circuits.[156] These appellate courts have held that Fourth Amendment reasonableness for extra-territorial searches requires balancing the government's need for the information with the privacy interest at stake.[157] Restricting our analysis to the EU, the requirements of EU and Member States' "data protection" law demonstrate a strong interest in privacy.[158] EU data protection law has a

---

[152] *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551 (2005).
[153] United States v. Verdugo-Urquidez, 494 U.S. 259, 270–71 (1990).
[154] *See id.* at 274–75.
[155] *See* United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987).
[156] *See* cases cited *supra* note 149.
[157] *See* cases cited *supra* note 149.
[158] The EU, like most of the rest of world, refers to its information privacy law as "data protection law." DANIEL SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 31 (2017).

strong anchoring in the constitutional law of the EU as well as of Member States.[159] For example, there are at least three important foundational expressions of a constitutional right of privacy in the EU: 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.[160]

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 U.S. to be considered part of the U.S. "national community," the Fourth Amendment might apply even to information stored overseas. Such a relationship might be created through physical contacts with the U.S. or a legal relationship, such as being a resident alien.[161]

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 contracts with the U.S. In contrast, non-U.S. users of such clouds will not receive Fourth Amendment protection. Information stored in extra-territorial 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 SCA in *Microsoft Ireland* and *Google Pennsylvania*.[162] The SCA forms part of the Electronic Communication Privacy Act (ECPA), which supplies the current framework for federal surveillance law.[163] Enacted in 1986, the SCA is the most important part of ECPA for international clouds; it regulates access to communications in "electronic storage," which is where cloud data spends most of its lifecycle.[164]

The relevant aspects of SCA can be quickly summarized. Section 2702 limits the disclosure of stored communications by service providers except for certain listed exceptions.[165] Section 2703 establishes the conditions under which the government may require a service provider to disclose the content of stored communications.[166] Finally, the SCA requires warrants to be issued under the procedures of Federal Rules of Criminal Procedure Rule 41.[167] Beyond these

---

[159] Schwartz & Peifer, *supra* note 2, at 122–27.
[160] Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 22 [hereinafter the European Convention on Human Rights]; Charter of Fundamental Rights of the European Union, art. 8(1), Dec. 18, 2000, 2000 O.J. (C 364) 1; Treaty on the Functioning of the European Union, art. 16, May 9, 2008, 2008 O.J. (C 115) 47.
[161] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 270–71 (1990).
[162] *See supra* Section I.A.
[163] For an overview, see SOLOVE & SCHWARTZ, *supra* note 158, at 69–74.
[164] *See* 18 U.S.C.A. §§ 2701–2711 (West 2015) (Stored Communications Act).
[165] *See* 18 U.S.C. § 2702.
[166] *See* 18 U.S.C. § 2703.
[167] *See id.*

basic elements, however, the SCA leaves many issues unresolved concerning Internet services.[168]

Open questions under this framework include whether a SCA warrant is to be interpreted as similar to other domestic "warrants," as the term is used in the Constitution or elsewhere, or whether such a SCA-issued court order is better characterized as a "warrant-subpoena" hybrid. This distinction is important because subpoenas, as this Article will discuss below, are generally executed by the party on whom they are served rather than by a governmental agent.[169] Moreover, U.S. governmental subpoenas can be international in scope. Thus, this question about the underlying nature of the SCA warrant relates to a further question, which is whether the SCA has international reach. As we have seen, *Microsoft Ireland* answered this question in the negative, and *Google Pennsylvania*—as well as a few other courts—have answered it in the affirmative. Here, too, the "warrant" or "hybrid" question is a significant one, as some caselaw holds that subpoenas served on a U.S. entity may require it to produce a document that is in its control overseas.[170]

Data Shards. In addition to *Google Pennsylvania*, other courts that have looked at Data Shard clouds in the context of the SCA have found that this statute can compel a request for information stored extra-territorially but accessed within the U.S. For example, an opinion from a magistrate judge in the Northern District of California found that "the conduct relevant to the SCA's focus took place" inside and not outside the United States.[171] In deciding this case, Magistrate Judge Laurel Beeler noted, "the only place to access the information is in the United States."[172]

As we have seen, moreover, a fear of "Going Dark" encouraged the same result in *Google Pennsylvania*. 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 the Google Legal Team from within the U.S. Due to this management model, a court that focused solely on the location of the data outside the U.S. would place this system outside the reach of the SCA and also MLATs.

Data Localization. *Microsoft Ireland* gives one reading of how to treat a Data Localization cloud where access to data would occur in the U.S., but the data is stored abroad. Yet, this result is far from set in stone, as shown by the evenly divided Second Circuit denying the request for a rehearing en banc.[173] In four separate opinions, four judges explained their views of why the SCA should or should not have an extra-territorial reach in that case.[174] The U.S. Supreme

---

[168] For an overview, see ORIN KERR, COMPUTER CRIME LAW 632–66 (4th ed. 2017).
[169] *See infra* Section II.A.4.
[170] *See, e.g.*, *In re* Grand Jury Proceedings the Bank of Nova Scotia, 740 F.2d 817, 826–29 (11th Cir. 1984); United States v. Vetco, 691 F.2d 1281, 1287–91 (9th Cir. 1981).
[171] *In re* Search of Content that is Stored at Premises Controlled by Google, No. 16-mc-80263, 2017 WL 1487625 at *3–4 (N.D. Cal. Apr. 19, 2017).
[172] *Id.* at *4.
[173] *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 855 F.3d 53 (2d Cir. 2017).
[174] *See id.*

Court now has the matter before it.[175] An important technical nuance exists, however, which may greatly limit the reach of the decision in this matter. The difference is between a complete and partial Data Localization cloud. Depending on the scope of the Court's decision, it may reach a result only for partial Data Localization clouds, such as the one at stake in *Microsoft Ireland.* In that variant, the data was located abroad *and* the service provider could access it from within the U.S. A complete Data Localization cloud might not fall under the Supreme Court's opinion regarding the reach of the SCA. Silence on that issue by the Court would leave the matter open.

Data Trusts. A Data Trust cloud splits access to customer data from management of it. In the context of the SCA, this approach provides strong insulation from U.S. data requests for exterritorial data located in this type of cloud. First, unlike the Data Shard model, this approach removes the "Going Dark" concern from the discussion. There is a fixed location for the information; it is not in motion ceaselessly. Additionally, the MLAT process is available for these data requests (as noted in the next section).

Second, beyond the protections found in a Data Localization cloud, the Data Trust cloud further insulates data stored in non-U.S. networks from SCA requests. It does so because of divisibility of management. The party running the cloud does not have access to the information, and the party with that access is governed by the law of the non-U.S. jurisdiction of the cloud in question. This aspect of the Data Trust model will be especially helpful before any U.S. court that believes SCA-warrants to be hybrid warrant-subpoenas. By separating access to the data from management of the servers, it permits U.S. cloud providers to run non-U.S. clouds while avoiding the entangling question as to whether they "control" the information.

SCA Summary. Data Shard clouds are likely to be treated as falling within the scope of the SCA. This result is driven in part by judicial recognition of the dangers of "Going Dark," that is, law enforcement agencies being unable, as a technical matter, to access digital data even with proper legal authorization. As for Data Localization clouds, one leading case, *Microsoft Ireland*, has found that the SCA does not have an extra-territorial effect.[176]

Finally, of the three models, a Data Trust cloud is likely to have the greatest insulation from extra-territorial use of the SCA. This outcome rests on two grounds. First, a Data Trust cloud lacks any "Going Dark" concern, unlike the Data Shard model, because the process of seeking foreign assistance is available in many jurisdictions through the MLAT process. Second, the cloud provider itself will be unable to respond to such requests due to its lack of control over the information. Under the Data Trust model, the cloud provider must direct such requests to the Data Trustee, who will respond pursuant to non-U.S. law of the jurisdiction where the respective cloud is located.

---

[175] United States v. Microsoft Corp., 138 S. Ct. 356 (2017) (granting certiorari).
[176] *See Microsoft Ireland*, 829 F.3d 197, 197–98 (2d Cir. 2016).

3. MLATs

A long-established way for the U.S. government to access private information held abroad is through Mutual Legal Assistance Treaties (MLATs). 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.[177] MLATs establish legal mechanisms for cooperation between signatory nations in criminal matters and proceedings, including the exchange of evidence and information during criminal proceedings.[178] The *Microsoft Ireland* case—which limited the ability of the U.S. government to leverage the SCA's warrant authority for global data requests—has increased the relevancy of the MLAT process.

While MLATs are more important than ever, 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.[179] For example, the U.S. has MLATs in place with numerous EU Member States and with the EU itself.[180] Building on the EU-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."[181]

After the Second Circuit's decision in *Microsoft Ireland*, the U.S. government still retains the ability to draw on its U.S.-Ireland agreement for mutual assistance in criminal proceedings and investigations.[182] That agreement states that the U.S. may approach the Irish government with a request for "documents, records, and articles of evidence."[183] In turn, the Irish government is to process the request under Irish law.[184] Ireland has the authority to issue orders deemed necessary to execute the request, whether by search warrant, subpoena, or other order. It can also postpone or alter the execution of the request if it feels it would interfere with Irish criminal investigations or similar legal proceedings.[185]

The use of MLATs has been widely criticized, however, as time consuming and inefficient. The district court in *Microsoft Ireland* singled it out

---

[177] *See* MUTUAL LEGAL ASSISTANCE TREATIES, *supra* note 58.
[178] For an overview, see Swire & Hemmings, *supra* note 58, at 696–700.
[179] Woods, *supra* note 3, at 749.
[180] *See Country Profile: United States*, MUTUAL LEGAL ASSISTANCE TREATIES, https://mlat.info/country-profile/united-states (last visited Aug. 12, 2017).
[181] European Comm'n, 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.
[182] Treaty with Ireland on Mutual Legal Assistance in Criminal Matters, Ir.-U.S., Jan. 18, 2001, S. TREATY DOC. NO. 107-9.
[183] *Id.* at art. 1.
[184] *Id.* at art. 5(3).
[185] *Id.* at art. 5(4). The Irish Department of Justice provides a comprehensive analysis of the treatment in Ireland of requests pursuant to this MLAT. *See* DEP'T OF JUSTICE, EQUALITY AND LAW REFORM, MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS: A GUIDE TO IRISH LAW AND PROCEDURES (2008).

as impractical.[186] Woods also speaks of "the extremely long time" that a MLAT request typically takes to complete.[187] He notes: "The entire process has been estimated to take ten months, and in some cases can take much longer."[188] In recent testimony before Congress, Christopher Kelley, Assistant Attorney General in Massachusetts, flatly states that the "MLAT process . . . is not a viable solution" to the problem of law enforcement access to international cloud data.[189]

Data Shards. Analysis regarding the Data Shard cloud is clear: the MLAT process is irrelevant because courts will consider the locus of the search as domestic in nature. In fact, the MLAT is doubly irrelevant. As Judge Rueter noted in *Google Pennsylvania*, information in this cloud model is constantly shifting from country to country.[190] Hence, in language regarding "Going Dark" that this Article has already cited, Judge Rueter noted, "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 locations has been identified."[191]

Data Localization. Assuming that a court decides that access to the data occurs extra-territorially, as the Second Circuit did in *Microsoft Ireland*, the MLAT process under a Data Localization cloud would proceed under the specific and applicable national and regional agreements. Accordingly, the U.S. government's data request in *Microsoft Ireland* would proceed through the U.S.-Ireland MLAT.

In addition, the 2016 Umbrella Agreement between the EU and U.S. establishes additional protections before EU law enforcement agencies can give data to U.S. law enforcement agencies.[192] This Agreement does not provide a new substantive basis for such exchanges, which would continue to be governed by the law of the EU Member State to which the information request is directed. Rather, it makes such transfers subject to an overarching set of principles, which are also found in that year's Privacy Shield agreement with the U.S.[193] 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.[194]

---

[186] *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).
[187] Woods, *supra* note 3, at 749.
[188] *Id.*
[189] *See Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the Subcomm. on Crime and Terrorism of the S. Judiciary Comm.*, 115th Cong. 5 (2017) (statement of Christopher W. Kelly, Assistant Att'y Gen., Office of the Mass. Att'y Gen.), https://www.judiciary.senate.gov/imo/media/doc/05-24-17 Kelly Testimony.pdf.
[190] *Google Pennsylvania*, 232 F. Supp. 3d 708, 725 (E.D. Pa. 2017).
[191] *Id.*
[192] 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, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf (entered into force Feb. 1, 2017) [hereinafter Umbrella Agreement].
[193] *See id.* The Umbrella Agreement's protections generally track those of the Privacy Shield. For an overview of the Privacy Shield, see SOLOVE & SCHWARTZ, *supra* note 32, at 1187–97.
[194] Umbrella Agreement, *supra* note 192, art. 5(2).

Data Trusts. Under the Data Trust model, the MLAT process 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 extra-territorially. It would make it clear that the *location* of the data was outside the U.S. and the *search* of it was also extra-territorial in nature.

To explore how such MLAT access would proceed, we can consider the Microsoft German Cloud. Were U.S. law enforcement to seek data in Germany stored in this network, it would turn to T-Systems, the Data Trustee, pursuant to the U.S.-German treaty on Mutual Legal Assistance in Criminal Matters.[195] Article 12(1) of the U.S.-Germany MLAT foresees the use of "surveillance of telecommunications" as a justification for an extra-territorial data request.[196] At the same time, however, the law of the "Requested State," namely, Germany, "governing criminal investigations or proceedings" would apply to such a request.[197] 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).[198] Between the protections of EU Member State law and those of the Umbrella agreement, the MLAT process provides strong safeguards for users of EU-stored cloud data.

MLAT Summary. Under the three cloud management models, different results occur when data requests are made pursuant to MLATs. First, Data Shards clouds are not likely to implicate MLATs as the data request will be considered as purely domestic. Second, Data Localization clouds in the EU will have strong protections against U.S. data requests under the Umbrella agreement and EU Member State law. Third, MLATs are likely only to increase in importance if additional courts follow the precedent of *Microsoft Ireland* and find that the SCA lacks extra-territorial scope. 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 U.S. for property under its control that is located *outside* the U.S. 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, which a Canadian bank with U.S. branches had maintained in the Bahamas.[199] The Eleventh Circuit held that the bank had to release the

---

[195] Mutual Legal Assistance with Germany in Criminal Matters, Ger.-U.S., Oct. 14, 2003, S. TREATY DOC. NO. 108–27.
[196] *Id.* art. 12(1).
[197] *Id.* art. 19(1).
[198] For a discussion, see Schwartz & Peifer, *supra* note 81, at 165.
[199] *In re* Grand Jury Proceedings Bank of Nova Scotia, 740 F.2d 817 (11th Cir. 1984).

records, even though disclosure would violate Bahamian law.[200] Thus far, there has been no case applying the *Bank of Nova Scotia* rule to data stored by cloud providers on behalf of third parties.

In the wake of *Microsoft Ireland*, the government's ability to use its subpoena power extra-territorially is likely to become even more important. Understanding this result requires a brief return to the SCA. As we have seen, there are two relevant sections of this statute in this context. The first, Section 2702, prohibits a service provider from divulging the contents of a communication or a record pertaining to a customer unless a statutory exception permits this behavior.[201] The second, Section 2703, permits disclosure to a government entity "only pursuant to a warrant," which functions as a ban on the use of *subpoenas* to gain the contents of customer communications or documents.[202] Recall, however, that *Microsoft Ireland* held that Congress did *not* intend for the SCA's warrant provision to have an extra-territorial effect.[203] A possible consequence of this holding is that Section 2702 no longer serves to limit the extra-territorial effect of *subpoenas*. Hence, the U.S. government will likely be able to turn to subpoenas, as opposed to warrants, for cloud data stored extra-territorially.

In reaching this same conclusion, Orin Kerr has wondered if a subpoena approach leads to less protection than a requirement to obtain a SCA warrant.[204] As Kerr observes, "[W]ith the SCA out of the picture, the government [can] just subpoena the e-mails stored on the foreign server."[205] From this perspective, the most decisive aspect of *Microsoft Ireland* may prove to be its removal of the SCA's prohibition on use of subpoenas for oversea requests by U.S. law enforcement agencies. In her dissent from the denial of a petition for an en banc hearing in *Microsoft Ireland*, Judge Reena Raiggi of the Second Circuit also raised the possibility of this outcome. She ultimately decided that the government did need a search warrant for such material, but worried that such a finding would allow Microsoft to keep material free from U.S. government access "simply by moving material abroad."[206] There is a lack of clarity, however, regarding Congressional intent in enacting the SCA. It might have intended a broad extra-territorial effect for Section 2702's prohibition on disclosure in the absence of a statutory exception; it is not clear, moreover, whether Congress crafted the Section 2703 warrant exception to serve as a bulwark against extra-territorial use of subpoenas.

---

[200] *Id.* at 826–28.
[201] *See* 18 U.S.C. § 2702. (2012).
[202] *Id.* § 2703(a).
[203] *See Microsoft Ireland*, 829 F.3d 197, 201 (2d Cir. 2016).
[204] *See* Orin Kerr, *What Legal Protections Apply to E-Mail Stored Outside the U.S.?*, WASH. POST: VOLOKH CONSPIRACY (July 7, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/.
[205] *Id.*
[206] In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 855 F.3d 53, 74 (2d Cir. 2017) (Raggi, J., dissent) (order denying rehearing en banc).

Regarding such extra-territorial subpoena requests, caselaw 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."[207] For example, in *Marc Rich*, 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."[208] The subpoena in *Marc Rich* was directed to a corporation for its own overseas records. The *Marc Rich* court found that the grand jury had jurisdiction over the corporation under the "territorial principle"; this concept permits governments to punish an individual or entity for acts outside their boundaries when such acts are "intended to produce and do produce detrimental effects within it."[209]

In contrast, a foreign-based entity that holds records on behalf of another party is generally considered to have a stronger interest against extra-territorial subpoenas than the non-U.S. entity who is a party to the underlying litigation in the U.S. 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 tribune approaches the laws and interests of other states."[210] It is a concept of "judicial self-restraint in furtherance of policy considerations which transcend individual lawsuits."[211] As the Texas Supreme Court stated in recognizing the importance of this principle, comity requires careful examination of "[t]he circumstances of each situation."[212]

The leading test for comity is found in the Restatement (Third) of Foreign Relations Law.[213] It contains a five-part yardstick, which looks to: "[1] the 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."[214] Such a comity analysis is also common when private parties seek information as part of litigation in the U.S. We discuss it in more detail below at Part II.B.2.

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 will lack a justiciable foreign relations interest in the data request. Hence, a comity analysis is likely to be unnecessary, and a subpoena

---

[207] *Microsoft Ireland*, 829 F.3d at 221.
[208] *Id.* at 215 (discussing *In re* Grand Jury Subpoena Direct to Marc Rich & Co., A.G, 707 F.2d 663 (2d Cir. 1983)).
[209] *In re Marc Rich & Co.*, 707 F.2d at 666.
[210] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court, 482 U.S. 522, 543 n.27 (1987).
[211] Volkswagenwerk Aktiengesellschaft v. Superior Court, 176 Cal. Rptr. 874, 884 (Ct. App. 1981).
[212] Gannon v. Payne, 706 S.W.2d 304, 307 (Tex. 1986).
[213] See RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(c) (AM. LAW INST. 1987).
[214] *Id.*

issued to a Data Shard cloud would be considered as 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.

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 U.S. 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."[215]

Other circuits have ruled differently regarding custodial records found overseas when the holding entity was a bank.[216] After acknowledging such decisions in other circuits upholding subpoenas for oversea bank records, the *Microsoft Ireland* court drew a distinction between banks and cloud providers. For the Second Circuit, it had been long established that bank customers do not have a privacy interest in their records. It pointed to *United States v. Miller*, a 1976 Supreme Court decision, which found such records, for purposes of Fourth Amendment analysis, to be the bank's "business records" and not the "private papers" of the depositors.[217] In the future, other courts are likely to explore the distinction between banks-as-custodians and cloud-providers-as-custodians. Accordingly, much here will depend on how U.S. courts carry out their comity analysis.

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."[218] 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. Moreover, as a technical matter, the Trustee controls the actual access to the data, which means that Microsoft Germany, as the cloud provider, cannot even view customer data in the cloud.

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 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 renders this information as much the business records of the bank as that of the individual.

---

[215] *Microsoft Ireland*, 829 F.3d 197, 215 (2d Cir. 2016).
[216] *See id.* at 216.
[217] *Id.* (citing United States v. Miller, 425 U.S. 435, 440–41 (1976).
[218] *See id.* at 201.

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 customers' behalf, as when a bank executes a wire transfer. The amount and kind of data collected varies 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.

At the same time, however, the "Third Party" doctrine provides a plausible counterargument. Under this doctrine, people who voluntarily give information to so-called "third parties" have no "reasonable expectation of privacy" under the Fourth Amendment.[219] And 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.[220] At the same time, however, a Data Trustee is clearly a non-U.S. based entity that holds records on behalf of another party. Hence, it may not seem like a classic third party for a U.S. court.[221] Rather it may fall into another category—one that typically triggers the stronger protections of comity analysis.

Subpoena Authority Summary. Post-*Microsoft Ireland*, the U.S. government is likely to increase its use of subpoena authority. In the case of a Data Shard cloud, such writs 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 institutions. 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).[222] 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." 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

---

[219] *See* SOLOVE & SCHWARTZ, *supra* note 32, at 288–99.
[220] *See* Smith v. Maryland, 442 U.S. 735 (1979); SOLOVE & SCHWARTZ, *supra* note 32, at 288–95.
[221] The Third Party doctrine may be on uncertain ground with a case before the Supreme Court this term offering the Justices a chance to revisit it. Carpenter v. United States, 137 S. Ct. 2211 (2017) (No. 16-402) (certiorari granted).
[222] 50 U.S.C. §§ 1801–1885 (2012). One provision of the FAA regulates surveillance outside the U.S. that targets U.S. persons. 50 U.S.C. § 1881a(b) (2012).

power."[223] In a roughly analogous structure to the SCA, FISA's Title I and Title III permit court-ordered access to stored content. Laura Donahue refers to these aspects of the statute's pre-9/11 orientation as "traditional FISA."[224]

After 9/11, there were many changes in the government's data collection and analysis in this area and subsequent efforts by Congress to bring the law into accord with the changes as well as to modify some of these practices.[225] Regarding international cloud computing, the most important legal changes are found in provisions of the FISA Amendments Act of 2008 (FAA).[226] The FAA permits the U.S. government to compel service providers in the U.S. to assist in the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[227] 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 of the U.S.[228] 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 U.S.[229]

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."[230] The acquisition must also be "conducted only in accordance with" some kind of "minimization procedures" to limit the acquisition, retention, and dissemination of non-relevant information.[231] 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 U.S.

The FAA is, in fact, mainly focused on surveillance *inside* the U.S. The FAA requires U.S.-based service providers to turn over data on persons *outside* the U.S., but it mainly contemplates the disclosure of data stored or otherwise accessible inside the U.S. 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 U.S.? While the Second Circuit resolved that issue for the SCA, there is no public case about its resolution under the FAA.

Beyond FISA and the FAA, Executive Order 12333 defines, at a high level of generality, the authority of the U.S. government to obtain access to data

---

[223] 50 U.S.C. §§ 1802, 1805.
[224] LAURA DONAHUE, THE FUTURE OF FOREIGN SURVEILLANCE 13–15 (2016).
[225] For a highly negative account of these practices, see OWEN FISS, A WAR LIKE NO OTHER 225–61 (2015).
[226] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (2008) (codified in 50 U.S.C. §§ 1881–1885).
[227] 50 U.S.C. § 1881a(a).
[228] *Id.*
[229] *Id.* § 1881a(c)(2). For a discussion, *see* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 17:3 (2d ed. 2016).
[230] 50 U.S.C. § 1881a(d)(1).
[231] *See id.* § 1881a(c)(1).

stored on computers outside the U.S.[232] 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 collection.[233] 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."[234]

Data Shards. The Data Shard cloud is accessed in the U.S., and, hence, will be subject to provisions of the FISA and 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.

Data Localization. FISA and the FAA do not extend to the capture of communications that lack some geographic connection with the U.S.[235] Thus, the issue of necessary connection to the U.S. will be a critical question regarding a Data Localization cloud accessible within the U.S. FISA applies only to the acquisition of communications that occurs within the U.S. or when the government is targeting a known U.S. person outside the U.S. It appears, therefore, that a Data Localization cloud whose content can be accessed from the U.S. will fall under FISA. There is no publicly available FISC opinion, however, regarding this issue.

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 U.S. Additionally, these parties do not fall within the definition of "an electronic communication service provider" under the Act.[236] Both parties would be considered as 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 12333.[237] Their ability to effectively do so, as under the FAA, will turn on their ability to overcome data security measures, including any use of encryption, provided in a Data Trust cloud.[238]

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 U.S. Its status is the same as any U.S.-based "electronic service provider." In contrast, a Data Localization cloud will be subject to FISA and the FAA only so long as there is a geographic connection with the U.S. A Data Localization cloud accessible from the U.S. will likely fall under the

---

[232] Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (1981).
[233] KRIS & WILSON, *supra* note 229, at 663–64.
[234] Exec. Order No. 12,333, supra note 232, at pt. 2.3.
[235] 2 JAMES G. CARR ET AL., THE LAW OF ELECTRONIC SURVEILLANCE § 9.13 (2017).
[236] *See* § 1885(6).
[237] *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941.
[238] Whether the data security will be breakable will turn on a range of security and non-security issues. For a discussion, see BRUCE SCHNEIER, BEYOND FEAR 264–66 (2003).

applicable foreign intelligence surveillance statutes. Finally, a Data Trust cloud located outside the U.S. is not an "electronic service provider" under relevant statutory provisions.

B. Extra-Territorial 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 U.S. for such information. In comparison to its 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."[239] Unlike civil law countries, discovery in the U.S. is not managed by a judge, but is largely self-executing by parties to the litigation. 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."[240]

When private parties seek extra-territorial 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 U.S. is a signatory to the Hague Evidence Convention, which provides a non-exclusive means of taking evidence in civil and commercial matters.[241] In 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."[242] From the perspective of U.S. litigants, however, the Hague Convention proves to be a flawed method for gathering evidence.

First, all EU Members are not parties to the Hague Convention.[243] Second, many EU signatory states filed reservations at the time of ratification that essentially prevent its use as part of pre-trial discovery.[244] These countries

---

[239] 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.

[240] GIL KETELTAS, *US E-discovery*, *in* E-DISCOVERY AND DATA PRIVACY: A PRACTICAL GUIDE 3–6 (Catrien Noorda & Stefan Hanloser eds., 2011).

[241] 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. 241. For a useful concise analysis of the letters rogatory process, see Swire & Hemmings, *supra* note 57, at 702–04.

[242] Article 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation 00339/09/EN (WP 158) 6, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf.

[243] *Id.*

[244] *Id.*

include France, Germany, Spain and the Netherlands.[245] 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.[246]

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 U.S. As a consequence, courts are likely to consider this information as located in the U.S. In such cases, normal domestic discovery pursuant to the Federal Rules of Civil Procedure will occur.

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 U.S. seeking discovery might argue, however, that the U.S. provider running a Data Localization cloud should not require use of the Hague Convention, but be 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 was also technically accessible for the cloud provider from within the U.S. A different result is likely if a Data Trust arrangement is at stake. Here, a litigant in the U.S. 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.

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, that is 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 defense.[247] These rules define "relevancy" broadly.[248] In 2006, Amendments to the Federal Rules included "electronically stored information" as being among the information covered by the "duty to disclose."[249] 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."[250]

A distinction must be drawn between discovery directed against a party in litigation and discovery directed at a non-party that holds data that may be

---

[245] *Id.*
[246] Swire & Hemmings, *supra* note 58, at 702.
[247] FED. R. CIV. P. 26(b)(1).
[248] *See* FED. R. CIV. P. 26(b) advisory committee's note to 1970 amendment.
[249] *See* FED. R. CIV. P. 26(a).
[250] *See* FED. R. CIV. P. 26(d)(1).

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.[251] ECPA does, however, permit cloud providers to disclose customer identifying information and other metadata in response to civil discovery requests.[252]

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 U.S. When parties in the U.S. 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 U.S. is the Restatement (Third) of Foreign Relations Law. The Restatement sets up a multi-part test concerning the necessary comity analysis.[253] 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."[254] As noted above, there are five parts to this approach: "[1] the 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."[255] Far different results are likely for discovery requests made under this test depending on the type of global cloud in which the data is stored.

Data Shards. As we have seen regarding letters rogatory, a U.S. court is not likely to view a Data Shard cloud—where data is searchable from the U.S.—as involving a foreign data request. In a similar fashion, 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 U.S. will apply and not the multi-factor comity test of the Restatement (Third) of Foreign Relations Law.

Data Localization and Data Trusts. EU data protection law will be important to the comity analysis for Data Localization and Data Trust clouds. In cases where such discovery requests are contested, litigants from EU Member States will typically present U.S. courts with evidence of the fundamental importance of data protection in their legal order.[256] Information privacy in the

---

[251] 18 U.S.C. § 2702 (2012).
[252] *Id.* § 2702(c).
[253] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(c) (AM. LAW INST. 1987).
[254] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court, 482 U.S. 522, 544 n.28 (1987).
[255] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(c).
[256] Volkswagen, A.G. v. Valdez, 909 S.W.2d 900, 902 (Tex. 1995).

U.S. 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.[257]

In addition to the data protection law of the non-U.S. Trustee, a Data Trust outside the U.S. 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."[258]

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. As we have seen, this distinction is important for international discovery requests made pursuant to subpoenas.[259] 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.

Federal Rules of Civil Procedure Summary. Discovery requests to a Data Shard cloud are likely 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 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 "an important interest of the state" threatened by the foreign discovery request.[260] 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 extra-territorially.

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 extra-territorial data access. Its main conclusion will be that the old status quo, based on a unilateral approach by the U.S., is breaking down. Pax Americana for the Internet is not what it used to be; or more precisely, the ability of the U.S. to go it alone concerning requests for extra-territorial data law is diminishing. The key factors in this decline are the growth of the Internet outside the U.S.; the increased trend towards localization of data, both legal and technical; and the international skepticism towards U.S. privacy protections. In place of the unilateral approach, this Article advocates for new international agreements regarding extra-territorial data

---

[257] Schwartz & Peifer, *supra* note 2, at 122–37.
[258] *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(c).
[259] See *infra* Part II.A.4.
[260] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(c).

access. These are to be based, first, on the recognition of reciprocal interests among nations. As a second principle, this Article calls for a "level playing field"—the need is for equal treatment of global clouds, regardless of the location of the provider's headquarters.

A. Initial Lessons Revisited

This Article's Part I.C drew four preliminary lessons. The first is that distinct legal issues are raised by Data Shard, Data Localization, and Data Trust clouds. 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 extra-territorial data access confirms this point. In particular, Data Shard and Data Trust clouds are at different ends of the spectrum with respect to such data requests. 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, courts will reach this outcome under the SCA and for subpoena requests. 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. Over time, these outcomes may make Data Shard networks relatively less attractive for those non-U.S. clients who are concerned about data access requests from the U.S. and skeptical of U.S. privacy law.

The second lesson regards the "divisibility of control"—that is, the ability to separate access to the information stored in a cloud from other aspects of network management. This dimension—found primarily in Data Trust clouds—dramatically increases the ability of certain cloud providers to resist extra-territorial requests from the U.S. In contrast, Data Trust clouds, under the current state-of-play, offer additional protections from extra-territorial requests from the U.S. for localized cloud information. This network model shifts U.S. governmental requests to the MLAT process and the law of the non-U.S. jurisdiction in which the cloud information is stored.[261] On the civil side, requests for information to a Data Trust cloud are analyzed according to the comity analysis of the Restatement (Third) of Foreign Relations. Data Trustees will be able to draw on the protections of both their domestic data protection law and their domestic law of trusts to demonstrate strong interests in non-disclosure of cloud data both on their part and on the part of the country where the information is located.[262]

The third lesson concerns the growth of data localization, both of the technical and legal kind. Jack Goldsmith and Tim Wu have identified the important role of intermediaries in assisting governments in the control of Internet behavior.[263] 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)."[264] Rather, governments exercise extra-

---

[261] See *infra* Part II.A.3.
[262] *Id.*
[263] GOLDSMITH & WU, *supra* note 9, at 67–68.
[264] *Id.* at 68.

territorial control over the Internet by controlling the behavior of intermediaries.[265] This process has certainly occurred in the context of global clouds. Through legal mandates, governments have acted to require their surveillance "targets" to store data domestically with regulated "intermediaries," that is, cloud companies. Moreover, customers who do not fall under such a legal requirement may seek such services for their own reasons. 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 parties 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 extra-territorial access to data held in non-U.S. cloud, it is also possible to predict the nature of the strategic changes in behavior.

The "Big Picture"? First, U.S. law is likely to subsume Data Shard clouds within its existing rules for domestic clouds. As a consequence, certain non-U.S. customers of networked computing are likely to avoid these clouds. These will be the customers who are skeptical of U.S. law, or would prefer to have data requests for their information handled under their own legal system. Regarding Data Localization clouds, *Microsoft Ireland* may cause a shift to law enforcement use of the subpoena power. The Supreme Court may decide, however, that the SCA does have an extra-territorial reach. Under either outcome, the relative attractiveness of Data Trust clouds is likely to increase.

It is also clear that MLAT's will be more important than ever. Legal data localization is one of the ways that many countries are now threatening the "open Internet." As a historical matter, the U.S. developed the Internet and subsequently had great power over its rules.[266] This "Pax America" also meant that much of the world's data traffic passed through the territory of the U.S.[267] The result was a bonanza for U.S. national security agencies and law enforcement. Today, the old Internet status quo is under assault in many policy areas, including global access to extra-territorial data. The next section considers the breakdown of the "Pax America" for extra-territorial data access and points to best principles for U.S. policymakers.

B. International Cooperation and Equal Treatment of Extra-Territorial Clouds

In a world of Data Localization and Data Trust clouds, the unilateral approach of the U.S. is breaking down. The U.S. cannot expect solely to determine the kind of legal process that will be applied when the U.S.

---

[265] *Id.*

[266] One of the best histories of this development is KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE (1996).

[267] BERNARD E. HARCOURT: EXPOSED 76–79 (2015).

government or civil litigants seek data stored extra-territorially.[268] The future will be one of increased Data Localization and Data Trust clouds, which will limit the reach of the SCA and subpoenas. On the civil side as well, foreign litigants will seek to shield data under a comity analysis by emphasizing their important constitutional and statutory interests in data protection and privacy.[269]

There has also been a dramatic growth of the Internet outside of the U.S. The International Telecommunication Union estimates that approximately 3.2 billion people were online in 2015.[270] Of these, approximately two billion were from developing countries. According to one estimate, fewer than ten percent of Internet users are found in the U.S.[271] As the center of gravity of Internet usage shifts so greatly, more countries will resist exclusivity status for U.S. data access rules. At the same time, U.S. cloud companies in the U.S. will continue to face their own set of data requests from parties outside of the U.S. The need is to harmonize international law in way that respects privacy and also preserves suitable access to data with appropriate legal process.

Others have predicted the end to the unilateral approach and more 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."[272] 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."[273]

Creation of a new regime for legal access to the global cloud should be around a principle of reciprocity. This Article will now discuss the path towards enhancement of international cooperation around this concept. A good way forward is presented by a bi-partisan Congressional bill, the International Communications Privacy Act (ICPA). Finally, this Article discusses the merits of a level playing field for U.S. tech companies in devising a policy regarding access questions.

---

[268] For an insightful definition of "the unitary approach," Swire & Kennedy Mayo, *supra* note 3, at 663–64.

[269] See Volkswagen, A.G. v. Valdez , 909 S.W.2d 900 (Tex. 1995) (reversing 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 interest of foreign sovereign with those of the U.S. Court); *In re* Vitamins Antitrust Litig., 2001 WL1049433 (D.D.C. June 20, 2001) (allowing German defendants to maintain a "privacy log detailing exactly what requested information would be covered by the German privacy laws"); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(c) (AM. LAW INST. 1987) (when 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); *see also* SOLOVE & SCHWARTZ, *supra* note 32, at 1174–77.

[270] INT'L TELECOMM. UNION, FACTS AND FIGURES: THE WORLD IN 2015 (2015), https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

[271] *Internet Users in the World by Regions—June 30, 2017*, Internet World Stats, http://www.internetworldstats.com/stats.htm.

[272] Swire & Kennedy Mayo, *supra* note 3, at 664.

[273] Daskal, *supra* note 3, at 475.

1. The Principle of Reciprocity

The key point of orientation for policy reform should be the recognition of reciprocal national interests in new international agreements concerning extra-territorial data access. Until recently, U.S. policymakers viewed issues involving access to information located outside of the U.S. as of minor significance. For example, Swire and Hemmings observe that for many years the MLAT process was merely "an obscure specialty topic for international lawyers."[274] 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. Moreover, civil requests for discovery raise higher stakes than before because of the growth of global commerce and the increase in international communications. Both civil litigation discovery and governmental data demands are further complicated by the constitutional status of information privacy in important foreign jurisdictions, most notably the EU.[275]

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 U.S.-EU collaboration around issues relating to national security and law enforcement. As a sign of increased transatlantic cooperation, a new U.S-EU data protection "Umbrella Agreement" was signed in June 2016 to permit information sharing "to combat crime, including terrorism."[276] The Umbrella Agreement establishes data privacy protections for all personal data that is shared pursuant to it.[277] Within the EU itself, the EU Commission is considering different options to permit speedier access to information stored in clouds within its Member States. These national EU standards vary widely in their levels of privacy safeguards for the users.[278]

At the same time as these international developments, there has been nascent acknowledgment in the U.S. Congress of the principle of reciprocity. For a sense of the current state-of-play, we can examine a bi-partisan bill, the International Communications Privacy Act (ICPA).[279] This law would amend ECPA in a way that promotes the adoption of a shared system for responding to law enforcement requests for cloud information. Notably, it takes a path that Kerr has already identified: its focus is on the cloud user and not on the location of the data.[280] This emphasis means, however, that cloud providers will have a strong incentive to know who their users are.

To understand this Bill's advancement of reciprocity and how it supplements and enhances current legal authorities, we begin with its central

---

[274] Swire & Hemmings, *supra* note 58, at 688.
[275] For a discussion, see Schwartz & Peifer, *supra* note 2, at 122–27.
[276] *Signing of the Umbrella Agreement: A Major Step Forward in EU-U.S. Relations*, EUROPEAN COMMISSION (June 2, 2016), http://ec.europa.eu/justice/newsroom/data-protection/news/160602_en.htm.
[277] *Id.*
[278] A window into these disparities is provided by the scholarly reports on France, Germany, and Italy in BULK COLLECTION (Fred H. Cate & James X. Dempsey eds., 2017).
[279] International Communications Privacy Act (ICPA), S. 2986, 114th Cong. (2016).
[280] *See* Kerr, *supra* note 124.

statutory term of art, which is that of the "Law Enforcement Cooperation Agreement" (LECA).[281] This term refers to a variety of possible international agreements that would establish a reciprocal process for notifying and obtaining consent with respect to data requests.[282] The U.S. and the United Kingdom are now developing a treaty that would constitute a LECA.[283]

This decentralized approach 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 only could be based on the least common denominator.[284] Outside the U.S., countries have far 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. The U.S. should build up a series of international agreements about access to global cloud data by proceeding initially among states that most closely share its values.

Using the presence or absence of a LECA as its regulatory linchpin, ICAP establishes a two-step regime. First, a warrant can be used to disclose the contents of cloud data only once the U.S. government has "taken all reasonable steps to establish the nationality and location of the subscriber or customer whose contents are sought."[285] These warrants extend to U.S. persons just as they would if the sought-after data were stored in the U.S. The warrants also apply, in different ways, to nationals of a foreign country, or persons located in it, depending on whether a LECA is in place. Second, if the U.S. government has a LECA with the foreign jurisdiction in which the warrant is to be served, ICPA permits use of this process only if the foreign government does not object to its use in the case at hand.[286] The foreign government, informed by a local service provider, could object to the request if it felt that it infringed its sovereignty or would violate domestic legal protections. If so, the country would deny the ICPA request, and the matter would be contested by the cloud provider in the foreign jurisdiction. In the absence of an objection by the foreign state, the cloud provider would directly respond to the request without recourse to the MLAT process or the use of a foreign court.

By encouraging nations to negotiate with the U.S. government for LECA's, this approach would open the door for reciprocal recognition of the other country's process for data requests for non-U.S. customers made to U.S.

---

[281] ICPA, S. 2986, § 3(h)(6).

[282] *See id.* § 4.

[283] *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. (2016), https://archive.org/stream/gov.gpo.fdsys.CHRG-114hhrg98827/CHRG-114hhrg98827_djvu.txt.

[284] Woods, *supra* note 3, at 788.

[285] ICPA, S. 2986, § 3(a)(2)(i).

[286] If the foreign country does *not* have such an agreement with the U.S., ICPA foresees extraterritorial use of the ICPA warrant. The result is that under ICPA, unlike *Microsoft Ireland*, a warrant would apply to the extra-territorial data of a U.S. cloud provider. The non-U.S. cloud providers in countries without a LECA might still refuse to obey the order if the U.S. court lacked jurisdiction over it.

cloud providers. As a model, 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 others."[287] Thus, under ICPA, the key question concerns the nationality and location of the subscriber and not the location of the data. This Bill centers on whether the subscriber of customer is a U.S. person, physically located in the United States, or "a national of or located in a foreign country."[288]

ICPA would largely flatten differences regarding data requests among the three kinds of cloud networks. A U.S.-based Data Shard provider who can demonstrate use of the cloud by a national of or a person located in a foreign country would have the access question determined under the pertinent LECA, just as if the data were accessed or stored outside the U.S. This result would flip the current treatment of Data Shard networks, in which the law tends to treat them simply as a U.S.-located network. As for the Data Localization cloud and the Data Trustee Cloud, the question of whether the data is accessible from the U.S. becomes irrelevant under ICPA. A warrant request made to either cloud model would look to the nationality and location of the subscriber. Assuming that such subscribers are not U.S. persons and are located outside of the U.S., a U.S. court would then consider the presence or absence of a cooperation agreement with the U.S. In cases where such an agreement exists, the foreign government, informed by a local service provider, could object to the request if it felt that it infringed its sovereignty or violated domestic legal protections.[289]

By treating the three cloud management models similarly, ICPA would be technologically neutral. Currently, the state-of-play in U.S. data access laws encourages privacy-sensitive non-U.S. customers to favor Data Localization and Data Trust clouds. The law should permit the market to decide which cloud services are superior, however, and not lead customers to favor certain kinds of cloud to avoid aspects of U.S. regulation.

ICPA would also reduce the current burden on the MLAT process. This statute would promote greater use of LECA's, and, in turn, recourse to these agreements would mean that the easiest access cases would never be submitted to the MLAT process. Where a foreign country did not raise an objection, the cloud provider would supply the requested data without use of the MLAT process or involvement of a foreign court. ICPA also takes significant actions to improve the MLAT process, such as creating an online docketing system for MLAT requests and increasing transparency regarding the length for processing

---

[287] *Written Testimony of Paddy McGuiness, UK Deputy Nat'l Sec. Adviser, Before the Subcomm. on Crime and Terrorism of the S. Judiciary Comm.*, 115th Cong. (2017).

[288] ICPA, S. 2986, § 3(a)(2).

[289] There is a remaining benefit of a Data Trustee even should the ICPA be enacted. The "divisibility of control" in such a network has an additional benefit beyond dealing with discovery requests, whether from public authorities or civil litigants. Much of the Internet depends on different approaches to data monetization. A Data Trustee is insulated from a potential "business model" conflict of interest; its job is simply to respond to requests for stored information pursuant to transparent agreements with the cloud service provider as well as with the customers of the cloud.

these requests by the Department of Justice as well as foreign governments.[290] Thus, there are reasons to be optimistic that the MLAT approach can be streamlined and made more efficient in the future.

Finally, we come to the "grand bargain" inherent in this approach. We can break down the grand bargain into two parts. Part One is simply stated: ICPA focuses on the nationality or location of the user, and, therefore, makes the locus of data storage far less important.[291] The result is that ICPA minimizes the significance of data localization in data access requests. This outcome maps with a significant goal identified by the 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 with increasing requirements regarding "servers to be physically located within a country or limits on transferring data across borders."[292] 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 ICPA is to incentivize cloud providers to take greater steps to identify their customers. Hence, Part Two will undoubtedly dismay privacy advocates. Under ICPA, the nationality and location of the user become paramount issues. The ability of a foreign country to object to extra-territorial use of a SCA warrant is present only *when the cloud provider can reasonably point to the nationality and location of the user*.[293] Data Shard clouds gain the benefit of having their non-U.S. customers receive additional protection under a LECA. Data Localization clouds with data accessible in the U.S. would no longer have to depend on *Microsoft Ireland*, and the possible reluctance of other federal circuits to follow it. But this type of cloud would need to document the nationality of its customers and their location.

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 e-mail, where no need exists to collect billing information. Thus, in *Microsoft Ireland*, the customer who used the contested Hotmail account had merely self-identified as associated with Ireland. 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 identify or location; it simply takes the user-provided information at face value, and its systems migrate the data

---

[290] A Review Group under the Obama Administration similarly proposed important ways to improve the MLAT process, including by increasing in resources to the office in the Department of Justice that is responsible for these requests. PRESIDENT'S REVIEW GROUP ON INTELLIGENCE & COMMC'NS TECH., LIBERTY AND SECURITY IN A CHANGING WORLD 226–28 (2014).

[291] ICPA, S. 2986, § 3(a)(1).

[292] PRESIDENT'S REVIEW GROUP ON INTELLIGENCE & COMMC'NS TECH., *supra* note 290, at 214–15.

[293] *See* ICPA, S. 2986, § 3(a).

according to company protocol."[294] In his concurrence, Judge Lynch termed this approach, "self-reporting" by customers.[295]

Under ICPA, the era of such self-reporting customer location and identity would end. The EU's General Data Protection Regulation (GDPR) is likely to have a similar policy influence.[296] In Europe, this move to "Know Your Customer" is being made, ironically enough, in the name of privacy and security. The GDPR's intent is to create greater obligations on cloud companies vis-à-vis their customer, and, as a step towards that goal, is requiring detailed contracts between these parties. The key provisions in this regard are found in GDPR, Article 38(3).[297] 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.

Whether promoted by the EU's GDPR or the U.S.'s ICPA, global cloud companies face a "Know Your Customer" future. This step will move cloud providers closer to a paradigm already present for U.S. banks, which are subject to strict laws and rules requiring them to identify as well as monitor their customers.[298] 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 regulation in the U.S.[299]

The impact of this "Know Your Customer" step will spill-over into civil litigation. As this Article has shown, faced with extra-territorial 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 U.S. 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. In sum, ICPA acts to preserve the Internet as a global space, but does so at the price of greater collection of customer identification information by cloud providers. Different parties will evaluate the costs and benefits of this approach differently.

---

[294] *Microsoft Ireland*, 829 F.3d 197, 203 (2d Cir. 2016).
[295] *Id.* at 230 (Lynch, J., concurring).
[296] Commission Regulation 2016/679, 2016 O.J. (L 119), 1, 60–62 (EU).
[297] *Id.* at art. 38(3). For an analysis of the likely content of such contracts, see Nick Westbook, *Internet Technology and Communications*, *in* EUROPEAN DATA PROTECTION: LAW AND PRACTICE 317, 320–22 (Eduardo Ustaran ed., 2018).
[298] 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), 81 Fed. Reg. 29,398 (2016).
[299] For background on FinCen as well as the Bank Secrecy Act, see SOLOVE & SCHWARTZ, *supra* note 158, at 146–47.

2. The Level Playing Field

The second and final principle for policymakers is that the U.S. should seek international agreements that treat extra-territorial clouds equally regardless of the provider's national origin. This Article terms this principle, "the level playing field." Regarding the need for such a principle, we can point to the discussion by some jurists of 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."[300] 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."[301]

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.[302] 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 access."[303] Ultimately, Kerr turns away from this solution and calls for a user-based regime for territoriality.[304] He is wise to do so; it would be highly problematic for different U.S. legal rules to apply to an extra-territorial 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 extra-territorial clouds. Today's market for information technology is an international one, and different legal standards for domestic and non-domestic companies would simply encourage the use of non-U.S. services by non-U.S. customers. 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.[305] Looking to the future of digital services, Neelie Kroes, EU Commissioner for Digital Affairs, predicted: "It is often American providers that will miss out, because they are often the leaders of cloud services. If European cloud customers cannot trust the United States government, then maybe they won't trust U.S. cloud providers either."[306] Differing legal standards for U.S. companies would also prevent global specialization by cloud providers and limit

---

[300] *Microsoft Ireland*, 829 F.3d at 231 (Lynch, J., concurring).
[301] *Id.*
[302] Kerr, *The Next Generation Communications Privacy Act*, *supra* note 16, at 373.
[303] *Id.* at 416.
[304] *Id.*
[305] Swire & Hemmings, *supra* note 58, at 714.
[306] Traynor, *supra* note 4.

the resulting benefits of expertise and "scalability" of technology.[307] 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 "breaking" the Internet.[308]

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 of 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 territory. This policy reflects respect for other states, which is a bulwark of international law. As Judge Lynch observed in his concurrence in *Microsoft Ireland*, U.S. demands for records about foreign nationals stored on servers in her own country raise the possibility for "diplomatic strife."[309] In particular, there is a danger of "diplomatic consequences" from "over-extending the reach of American law enforcement officials."[310] 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 U.S. 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 U.S. is a primary exporter of electronic evidence."[311] In similar terms, Richard Salgado, a Google Legal Director, explained to a Congressional committee that since 2009, and the start of its collecting relevant statistics, Google has received more requests from foreign legal authorities than from those in the U.S.[312]

To be sure, there are circumstances in which U.S. lawmakers regulate behavior by U.S. actors that takes place outside of this country. The Foreign Corrupt Practices Act (FCPA) provides a useful comparison.[313] 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 U.S.[314] 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

---

[307] See Chander & Lê, *supra* note 62, at 719 (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 . . . .").
[308] *Id.* at 713.
[309] *Microsoft Ireland*, 829 F.3d at 231 (Lynch, J., concurring).
[310] *Id.* at 229.
[311] Peter Swire & Justin Hemmings, *Stakeholders in Reform of the Global Legal System for Mutual Legal Assistance*, *in* BULK COLLECTION, *supra* note 278, at 7. They add: "[There are] many more requests for mutual legal assistance for electronic evidence are made *of* the U.S. government than *by* the U.S. government" (emphasis in original).
[312] *Written Testimony of Richard Salgado, Dir., Law Enforcement and Info. Sec., Google, Hearing on "Data Stored Abroad" Before the H. Comm. on the Judiciary*, 115th Cong. (2017).
[313] 15 U.S.C. § 78dd-1 et seq. (2012).
[314] For an overview, see DEP'T OF JUSTICE & SEC. & EXCH. COMM'N, FCPA: A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT (2012).

transparency that typically accompanies corrupt practices.[315] In comparison, a restriction on U.S. cloud service providers abroad does not provide the same benefits of deterring negative externalities that the FCPA provides. 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 extra-territorial 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 follow from U.S. technology companies trying to comply with aspects of the law of foreign jurisdictions regarding extra-territorial data requests that are in tension with U.S. law. The critical need is for policy reform that permits countries to harmonize their shared interests in international law enforcement and counter-terrorism as well as in international civil discovery. The necessary principle should be one of reciprocity.

CONCLUSION

All clouds are not created equal, and different networks dictate notably distinct outcomes for actual cases involving data access requests. The 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 U.S. 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 to unilateral decision making by U.S. courts concerning legal process to be applied when the government or civil litigants seek data stored extra-territorially.

The need is for new principles for a world of omnipresent global cloud computing. This Article has identified two such concepts. First, the legal system should develop new international agreements for legal access to the global cloud. These should be based on the concept of reciprocity among nations. An insistence by U.S. policymakers on exclusivity for its legal access rules will be counterproductive; it will drive foreign customers to Data Localization and Data

---

[315] *Id.* at 15-16.

Trust clouds, which will only increase the relevancy of the law of foreign jurisdictions; limit the access of government and litigants in the U.S. to global cloud data; and harm U.S. tech companies. As a second and final point, a new cloud access regime should treat extra-territorial 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.

The stakes are high. The interests affected by legal rules for global access to data include privacy; law enforcement and national security; and the pursuit of justice by civil litigants in seeking international discovery. At the same time, developments in network technology and management mean that the current U.S. legal approach will become increasing irrelevant. The "Pax Americana" in this area is ending, and the wisest course for U.S. policy is to establish new international agreements for global data access.

APPENDIX: CLOUD MODELS AND LEGAL AUTHORITIES: A SUMMARY

	Data Shard Model	Data Localization Model	Data Trust Model
The Fourth Amendment	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 non-resident 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 non-resident 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.
The Stored Communications Act	*Google Pennsylvania* and other cases have found that a warrant issued under the SCA can compel a request for information stored extraterritorially but accessed within the U.S.	*Microsoft Ireland* found that a warrant issued under the SCA cannot compel a request for information stored extraterritorially but accessed within the U.S. This case is now before the U.S. Supreme Court.	Data Trust is likely to have greater insulation from extra-territorial use of the SCA due to availability in many jurisdictions of the MLAT process.
MLAT's	The MLAT process is irrelevant for a Data Shard Cloud if court continue to rule that the locus of the search of this cloud is domestic in nature.	Assuming that a court decides that access to cloud data occurs extra-territorially, as *Microsoft Ireland* did, the MLAT process would proceed under the specific national and regional agreements that are applicable.	A MLAT process for a Data Trust Cloud would be directed to the Data Trustee and not the service provider. Request would be judged by the Data Trustee's local jurisdiction.
Administrative or Grand Jury Subpoenas	If the Data Shard access is deemed to happen in the U.S., the SCA would apply and bar use of a subpoena. If access is deemed to occur outside the U.S., SCA would not apply and subpoenas would be permitted.	In *Microsoft Ireland*, 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 U.S.	Likely 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	If the Data Shard cloud is deemed to be accessed in the U.S., it will be subject to provisions of FISA and 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 no released FISC opinion, however, regarding this precise issue.	U.S. intelligence unlikely to be able to compel cooperation from a non-U.S. Data Trust cloud under the FAA. Pursuant to Executive Order 12333, U.S. intelligence may surveil information stored electronically. "Arms race" will follow with encryption of Data Trust.
The Hague Convention	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 pursuant to the Federal Rules of Civil Procedure will control.	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 judicial authority in country where cloud is located.
The Federal Rule of Civil Procedure	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 comity analysis for a Data Trust Cloud. This type of cloud may fare better in a comity analysis than a Data Localization Cloud; the former can make strong showing of "important interest of the state" in a foreign discovery request.