University of Kentucky
UKnowledge

Law Faculty Scholarly Articles | Law Faculty Publications

4-2016

Against Data Exceptionalism

Andrew Keane Woods
University of Kentucky, College of Law, andrewkwoods@uky.edu

Follow this and additional works at: https://uknowledge.uky.edu/law_facpub

 Part of the Internet Law Commons, and the Privacy Law Commons

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Repository Citation

Woods, Andrew Keane, "Against Data Exceptionalism" (2016). *Law Faculty Scholarly Articles*. 593.
https://uknowledge.uky.edu/law_facpub/593

This Article is brought to you for free and open access by the Law Faculty Publications at UKnowledge. It has been accepted for inclusion in Law Faculty Scholarly Articles by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

Against Data Exceptionalism

Notes/Citation Information

Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stan. L. Rev. 729 (2016).

This article is available at UKnowledge: https://uknowledge.uky.edu/law_facpub/593

Stanford Law Review

Volume 68 April 2016

ARTICLE

Against Data Exceptionalism

Andrew Keane Woods*

Abstract. One of the great regulatory challenges of the Internet era—indeed, one of today's most pressing privacy questions—is how to define the limits of government access to personal data stored in the cloud. This is particularly true today because the cloud has gone global, raising a number of questions about the proper reach of one state's authority over cloud-based data. The prevailing response to these questions by scholars, practitioners, and major Internet companies like Google and Facebook has been to argue that data is different. Data is "unterritorial," they argue, and therefore incompatible with existing territorial notions of jurisdiction. This Article challenges this view.

The Article argues that the jurisdictional challenges presented by the global cloud are not conceptually as novel as they seem. Despite the technological wizardry of modern life, the "cloud" is actually a network of storage drives bolted to a particular territory, and there is substantial case law suggesting that courts think of data as a physical object. Moreover, even if the cloud were a free-floating ether, data can be thought of as an intangible asset, like money or debt, which flows across borders; courts have been adjudicating such jurisdictional disputes for centuries. These precedents suggest numerous grounds for states to assert jurisdiction over data—not a single test, as major Internet companies claim.

After showing that these jurisdictional problems are not unprecedented, the Article draws from these precedents and outlines practical steps that courts, Congress, and the President can take to alleviate jurisdictional conflicts over the cloud. As Microsoft's cross-border dispute with the U.S. Department of Justice works its way through the courts, the President negotiates a treaty with the United Kingdom regarding cross-border access to the cloud, and Congress rewrites the Electronic Communications Privacy Act, finding a grounded approach to addressing this problem—one rooted in longstanding jurisdictional and conflicts principles—has never been more critical.

* Assistant Professor, University of Kentucky College of Law. The Author thanks Jack Goldsmith, Ryan Goodman, Orin Kerr, Matthew Perault, Jennifer Granick, Tino Cuellar, Jen Daskal, Al Gidari, Nicole Jones, Rick Salgado, Greg Nojeim, Nate Jones, Alex Abdo, Albertina Antognini, Alan Rozenshtein, Peter Swire, Will Baude, Shalev Roisman, as well as members of the legal and policy teams at Google, Facebook, Microsoft, and the Global Network Initiative. The Article benefited from workshops at NYU Law School, Stanford's Center for Philanthropy and Civil Society, the Junior International Law Scholars Association's annual meeting, the Center for Strategic and International Studies, and Harvard's Berkman Center for Internet and Society. The Author is especially grateful to Gail Kent for organizing a meeting with GCHQ, technology firms, and civil society groups at Wilton Park, where this Article first took shape.

Table of Contents

Introduction

On December 4, 2013, a magistrate judge in the Southern District of New York issued a search warrant for the contents and metadata associated with an e-mail account stored by Microsoft.[1] Microsoft produced the relevant data stored on its American servers.[2] But Microsoft, like many Internet companies, uses data centers located around the world to balance data loads and ensure that a user's data[3] is promptly available wherever the user accesses it.[4] Much of this particular customer's data was stored on the company's data center in Ireland.[5] The company therefore refused to hand over that data on the grounds that the Stored Communications Act (SCA),[6] which is part of the Electronic Communications Privacy Act (ECPA),[7] does not apply extraterritorially.[8] A district judge was unconvinced and upheld the warrant.[9] A number of amici have argued that allowing the U.S. government to compel

1. *See In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467-68 (S.D.N.Y. 2014) [hereinafter *Microsoft E-mail Search Warrant Case*], *appeal docketed sub nom.* Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. argued Sept. 9, 2015).

2. *Id.* at 468.

3. This Article will refer to data as a mass noun, similar to "information."

4. Microsoft alleged that it operates more than one hundred data centers in forty countries where it stores data for more than one billion customers. Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States at 8, *Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d 466 (No. 13 Mag. 2814) [hereinafter Microsoft's Objections].

5. The user signed up with a non-U.S. country code, which led Microsoft to store the data in its Irish data centers. *See Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d at 467 ("[B]ased on the 'country code' that the customer enters at registration, Microsoft may migrate the account to the datacenter in Dublin. When this is done, all content and most noncontent information associated with the account is deleted from servers in the United States." (citation omitted)).

6. 18 U.S.C. §§ 2701-12 (2014). Congress passed the SCA in order to ensure a measure of privacy for individuals whose communications are held remotely by third-party providers of communications and remote storage services—communications that are not protected by the Fourth Amendment. For a short history of the SCA, see Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 378-85 (2014).

7. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2701-12, 3121-27). In addition to the provisions of the SCA, ECPA also placed limitations on the use of pen registers—devices used to track the numbers called by a particular phone—and it extended the Wiretap Act's limitations on interception from telephone calls to computer data. *See* Kerr, *supra* note 6, at 382-83.

8. *See Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d at 470.

9. Order at 1, *Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d 466 (No. 13 Mag. 2814).

the data would encroach on foreign sovereignty,[10] and Ireland filed an amicus brief to assert its interest in the matter.[11] The case is currently pending in the Second Circuit.[12]

The *Microsoft Corp.* case is only the most recent symptom of a much larger problem: while many people now store their most personal data in the cloud—that is, on remote servers scattered around the globe—there is no settled understanding of who has jurisdiction over that data.[13] Companies and countries have taken a number of different positions—some incompatible with each other—regarding the reach of the state's jurisdiction over Internet data.[14]

---

10. *See, e.g.*, Brief of Amici Curiae AT&T Corp. et al. in Support of Appellant Microsoft Corp. at 3, Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. Dec. 15, 2014); Brief of Verizon Communications, Inc. et al. as Amici Curiae in Support of Appellant at 16, *Microsoft Corp.*, No. 14-2985-cv (2d Cir. Dec. 15, 2014); Brief Amicus Curiae of Electronic Frontier Foundation in Support of Microsoft Corp. at 11-14, *Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d 466 (No. 13 Mag. 2814).

11. Brief of Amicus Curiae Ireland at 1-3, *Microsoft Corp.*, No. 14-2985-cv (2d Cir. Dec. 23, 2014).

12. *See Microsoft Corp.*, No. 14-2985-cv (2d Cir. argued Sept. 9, 2015). For a rough transcript of the oral argument, see Transcript of Oral Argument, *Microsoft Corp.*, No. 14-2985-cv, https://lawfare.s3-us-west-2.amazonaws.com/staging/090915%20hearing%20rough.txt.

13. The Article will use the term "data" to refer to personal information that has been digitized and made capable of uploading to the Internet. A letter written with ink on paper is "data" of a certain kind, of course, but this Article is concerned with the jurisdictional implications of taking that handwritten letter, digitizing it, and storing it online in the cloud. Cloud computing is characterized by users' remote storage of data and services, which can be accessed anywhere on a network. *See* PETER MELL & TIMOTHY GRANCE, U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800-145, THE NIST DEFINITION OF CLOUD COMPUTING: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2 (2011); *see also* Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself."). It is difficult to describe the problem without belying a particular answer to it because the meaning of the phrase "the cloud," and who has jurisdiction over it, are the heart of the dispute. For example, it is tempting to refer to "foreign data" and "data stored abroad" in order to refer to data that is beyond the state's jurisdictional reach. But doing so presumes an answer—the location of the data—to the question of how to define the state's jurisdictional reach. The word "data" is used here as a generic term to refer to content, basic subscriber information, and metadata.

14. *See* Vidal-Hall v. Google Inc, [2014] EWHC (QB) 13 (rejecting Google's contention that the court did not have jurisdiction to hear a tort claim because the act complained of did not occur within the United Kingdom); Kerr, *supra* note 6, at 407 ("So what determines territoriality? The location of the data? The company? The employee? Or the requesting party?"); Warwick Ashford, *Google Claims It Is Not Subject to UK Privacy Laws*, COMPUTERWEEKLY (Aug. 19, 2013, 8:12 AM), http://www.computerweekly.com/news/2240203739/Google-claims-it-is-not-subject-to-UK-privacy-laws (noting Google's domicile theory of jurisdiction); Christopher Williams, *Google Argues UK Privacy Laws Do Not Apply to It*, TELEGRAPH (Aug. 18, 2013, 5:26 PM BST), http://www.telegraph.co.uk/technology/google/10250801/Google-argues-UK-privacy-laws-do-not-apply-to-it.html ("Google has argued that as an American company it is not

footnote continued on next page

These jurisdictional disagreements have wide-ranging implications for law enforcement and individual privacy, especially now that the cloud is global.[15] Consider, for example, what will happen when the Internal Revenue Service (IRS) seeks to collect back taxes by levying a Bitcoin account—how should a court determine whether the IRS has jurisdiction over the virtual currency?[16] Or consider the applicability of the Health Insurance Portability and Accountability Act (HIPAA) of 1996[17] to personal health data stored in the cloud—how should a court decide the location of the data for the purposes of determining whether it falls within the reach of HIPAA? Relatedly, what should a court do when, as in *Microsoft Corp.*, two nations assert jurisdiction over the same piece of data? As that Second Circuit case works its way through the courts, Congress considers reforming ECPA,[18] and the United States and

---

covered by British privacy laws. It said there was 'no jurisdiction' for the case to be heard [in the United Kingdom] because its consumer services are provided by Google Inc, based in Silicon Valley, rather than Google UK."); *see also* Orin Kerr, *Verizon Responds to My Blog Posts on the Foreign E-mail Case*, WASH. POST: VOLOKH CONSPIRACY (July 30, 2014), http://wpo.st/ZLgO1 ("At bottom, does this case involve regulation of providers that are inside the U.S. or data that is outside the U.S.?").

15. *See* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 287 (2015) ("The last twenty years have witnessed a dramatic globalization of the Internet.").

16. Bitcoin is a digital currency that is managed by a peer-to-peer process and does not technically reside anywhere—rather, the data that creates the code gives it value among other Bitcoin traders. It is classified by the U.S. Treasury Department as a decentralized virtual currency. *See The Present and Future Impact of Virtual Currency: Joint Hearing Before the Subcomm. on Nat'l Sec. & Int'l Trade & Fin. & the Subcomm. on Econ. Pol'y of the S. Comm. on Banking, Hous. & Urban Affairs*, 113th Cong. 33 (2013) (statement of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, Department of the Treasury). The U.S. Internal Revenue Code provides that the government may collect delinquent taxes by "levy," which is the equivalent of a seizure. I.R.C. §§ 6331-44 (2014); United States v. New England Merchs. Nat'l Bank, 465 F. Supp. 83, 86 (D. Mass. 1979) ("Levy is the equivalent of seizure . . . ."). Courts have not yet weighed in on the question of Bitcoin's location for tax purposes. However, at least one court has upheld the Securities and Exchange Commission's authority to regulate investment instruments based on Bitcoin, suggesting that a suit may proceed if the court can assert personal jurisdiction over a defendant with control over those assets. *See* SEC v. Shavers, No. 4:13-CV-416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013).

17. Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.). Sections 261 through 264 of HIPAA require the Department of Health and Human Services to promulgate standards—now known as the Privacy Rule—regarding the storage and dissemination of electronic health data. *See* OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE (2003).

18. *See* Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015); Electronic Communications Privacy Act Amendments Act of 2015, S. 356, 114th Cong. (2015).

United Kingdom negotiate a treaty regarding government access to data stored in the cloud,[19] these questions have never been more pressing.

Fortunately, these questions are not as novel as some scholars suggest. A number of lawyers and academics have recently made the case for "data exceptionalism," suggesting that cloud-stored data is fundamentally incompatible with existing territorial limits on jurisdiction.[20] But, despite the wizardry and wonder of modern technological advances, cloud-based data is not conceptually novel enough to support this view.[21] Data has physical and intangible features, both of which provide helpful precedent for states seeking to assert jurisdiction over that data.[22] Cloud-based data resides on servers—essentially large hard drives—and wherever those servers sit, they are subject to territorial assertions of jurisdiction.[23] Even if this data were somehow stored

19. *See* Ellen Nakashima & Andrea Peterson, *The British Want to Come to America—with Wiretap Orders and Search Warrants*, WASH. POST (Feb. 4, 2016), http://wpo.st/kFcD1.

20. *See, e.g.*, Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313, 388 (2013) (arguing that the cloud represents unprecedented legal challenges, and that existing jurisdiction and choice-of-law rules are in "dire need" of fundamental change); Zachary D. Clopton, *Territoriality, Technology, and National Security*, 83 U. CHI. L. REV. 45 (2016) (making the case for "technology exceptionalism"—the argument that courts ought to evaluate territoriality differently in the context of technology); David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide?: The United States, the European Union, and the Protection of Privacy Across Borders*, INT'L J. CONST. L. (forthcoming 2016) (manuscript at 14-55) (explaining the limits of the existing international regime to regulate the global cloud and calling for a transatlantic privacy agreement); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 397 (2015) (arguing that "data is everywhere and anywhere," making it incompatible with traditional notions of territorial sovereignty); *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) (arguing that because "data, including fragments and copies, can be stored everywhere," the territoriality requirement of the SCA makes little sense and suggesting that Congress should rely on the location of the service provider rather than the location of the data to determine the reach of the Act); Ian Brown et al., Towards Multilateral Standards for Surveillance Reform 2-3 (2015) (unpublished manuscript), https://cihr.eu/wp-content/uploads/2015/01/Brown_et_al_Towards_Multilateral_2015.pdf (describing the limits of national conflicts-of-laws rules to adequately delimit government access to data stored in the global cloud, pointing to the need for a multilateral agreement); *Time for an International Convention on Government Access to Data*, MICROSOFT ON ISSUES (Jan. 20, 2014), http://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data (calling for an international convention to regulate government access to personal data stored in the cloud).

21. *See infra* Part II.

22. *See infra* Part II.B.

23. *See* Kate Vinton, *The Feds Explain How They Seized the Silk Road Servers*, FORBES (Sept. 8, 2014 11:02 AM), http://www.forbes.com/sites/katevinton/2014/09/08/the-feds-explain-how-they-seized-the-silk-road-servers (explaining how the FBI worked with Icelandic authorities to search servers in Reykjavik, Iceland, that hosted an online bazaar for illegal activities).

in a free-floating ether, it would not be so different from other forms of intangible assets, like intellectual property and debts, which have been the subject of extraterritorial seizures going back many years.[24] Contrary to prevailing wisdom, jurisdiction over cloud-based data has nearly everything to do with territoriality—it requires an inquiry into the location of the data, the domicile of the data controller, the location of the crime, the citizenship of the victim, and/or the citizenship of the perpetrator.[25] Of course, these different bases for jurisdiction mean that the same piece of data may be subject to a number of different jurisdictions at the same time. But overlapping and conflicting laws are not a novel legal problem either; rather, conflicts of laws casebooks are filled with such disputes, and the fact that the subject of the dispute is Internet data changes very little as a conceptual matter.[26]

Showing that the jurisdictional challenges presented by the global cloud are not conceptually novel does not resolve those problems, but it does suggest a number of helpful insights drawn from past precedents. For example, if data is not as different as many have suggested, then states need not commit to narrowly defining their authority over data based on a single test, such as the location of the data or the domicile of the company.[27] Major Internet firms have adopted strikingly different views about the relevant test for when states have the authority to compel data. Microsoft treats the relevant test as the location of the data; under this test, states have the authority to compel data stored only on servers in their territory.[28] Google and Facebook appear to take

24. *See infra* Part II.B.1.a; *see also* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 455 reporters' note 2 (AM. LAW INST. 1987) (reviewing cases going back decades regarding the seizure of intangible assets); Aaron D. Simowitz, *Siting Intangibles*, 48 N.Y.U. J. INT'L L. & POL. 259, 270-92 (2015) (describing how courts determine jurisdictional disputes over intangible assets such as intellectual property, debts, stock, and more).

25. *See infra* Part III.A.

26. *See infra* Part IV. This discussion may give some readers déjà vu—data exceptionalists make a number of the same arguments as the early cyber anarchists. This response therefore closely tracks the responses to the cyber anarchist camp, most notably from Goldsmith and Wu. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006) (describing the enduring power of states to regulate the Internet through controls over infrastructure); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998) (arguing that many scholars exaggerate the difficulties of state regulation of the Internet) [hereinafter Goldsmith, *Against Cyberanarchy*]; Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EUR. J. INT'L L. 135, 138 (2000) (defending the idea that it is within states' prerogative to regulate extraterritorial Internet activity that has harmful local effects) [hereinafter Goldsmith, *Unilateral Regulation*].

27. *See infra* Part III.A.

28. Microsoft argues that the search and seizure of e-mails on a global network of servers occur at the location where the e-mails are stored. Brief for Appellant at 31-33, Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. Dec. 8, 2014). Implicit in this

footnote continued on next page

a different view, suggesting in a number of different contexts that states have authority to compel data only if the data controller (the company) is domiciled in that state's territory.[29] Neither view is right as a matter of longstanding principles of jurisdiction. Well-established precedent suggests that if a court has personal jurisdiction over the defendant or the defendant's assets—in this case, an Internet company or its offices, servers, or bank accounts—it can lawfully compel the data in connection with a legitimate law enforcement effort, regardless of where the data is stored or where the company is domiciled.[30]

Moreover, a rich vein of conflicts jurisprudence suggests that states can take simple steps to reduce jurisdictional disputes with other states.[31] For

---

argument is a claim that the relevant jurisdictional test for locating e-mails on a global server is the location of server (or servers) where the e-mails are resting.

29. In a wide range of lawsuits around the world, Google and Facebook have both articulated that the relevant jurisdictional hook for determining which states can compel stored data ought to be the domicile of the corporation, which for both companies is the United States. *See, e.g.*, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. para. 60, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN (holding that the European Court of Justice had jurisdiction over Google Inc. under the European Council's Data Protection Directive 95/46 because Google set up a subsidiary in Spain to sell advertising there and directed its services to Spain's inhabitants); Ashford, *supra* note 14 (describing Google's view that domicile of the corporation decides jurisdiction—not location of the data); Miranda Prynne, *Britons Should Be Able to Sue Google for Privacy Breaches, Court Hears*, TELEGRAPH (Dec. 16, 2013, 3:06 PM GMT) http://www.telegraph.co.uk/technology/google/10520755/Britons-should-be-able-to-sue-Google-for-privacy-breaches-court-hears.html (noting that upon being sued for surreptitiously collecting data about British Apple Safari users, Google "asked London's High Court to throw out the case claiming it is not governed by the British justice system"). For examples of Facebook's views, see Douez v. Facebook, Inc., 2014 BCSC 953, paras. 134-35 (Can. B.C.), *rev'd*, 2015 BCCA 279 (Can. B.C.) (holding the court had jurisdiction due to a British Columbian statutory cause of action, despite Facebook's argument that proper jurisdiction was in California); Aurelien Breeden, *French Court Rules It Has Jurisdiction over Facebook in Nude Painting Case*, N.Y. TIMES (Mar. 6, 2015, 10:17 AM), http://nyti.ms/1Bb3G5p (describing a French court's determination that it had jurisdiction to hear a dispute over Facebook's takedown of a user account, despite Facebook's argument that the terms of service called for all disputes to be resolved in California); and Richard Chirgwin, *Belgium Privacy Commish Ambushes Facebook with Lawsuit*, REGISTER (June 16, 2015, 5:03 AM), http://www.theregister.co.uk/2015/06/16/belgium_privacy_commish_ambushes_facebook_with_lawsuit (describing Facebook's assertion that "Belgium doesn't have jurisdiction").

30. *See infra* Part III.B.

31. For example, Congress could elect to narrow the state's ability to access data in the cloud for privacy reasons, and the President might agree with another country to voluntarily limit the state's reach into the cloud within these jurisdictional limits. As Larry Kramer explains:

> [I]t is not necessary to rely on the Constitution, for the principles of mutual accommodation and comity underlying its prohibitions suggest the result as a matter of ordinary interpretation. That is, while a state's laws may indeed reflect the judgment of the state's

footnote continued on next page

example, one of the lessons of transnational litigation regarding offshore bank accounts—perhaps the best analogy to offshore data storage—is that blocking statutes, which prevent citizens from complying with foreign law enforcement requests, greatly exacerbate conflicts of laws. Repealing those statutes is therefore one of the simplest steps that states can take to encourage regulatory harmonization and reduce conflicts.[32] The implication of this insight for cloud-based data is simple but far reaching: it suggests reforming many states' privacy statutes, which often operate as blocking statutes. Applying this insight to U.S. law, for example, would mean reforming ECPA.[33] While there are a number of ECPA reform proposals pending in Congress,[34] and ECPA reform has been widely discussed in the press,[35] none of the current proposals would have any effect on the statute's blocking features.[36] This Article therefore applies insights from transnational conflicts cases to ECPA reform efforts, suggesting a number of specific changes that might minimize cross-border conflicts over government access to data.[37] These changes are a promising alternative to the fraught idea of a global treaty on government access to data.[38]

This is the first Article to look to longstanding jurisdictional principles to assess the state's ability to compel personal data stored on the global cloud.[39]

> lawmakers about how best to organize society, each state presumably recognizes that other states can have different views about what is best. Conflicts are inevitable, and it is necessary to develop means of avoiding or resolving them. The presumption that a state's law does not reach cases with which the state has no contact is one such means: it avoids conflicts while increasing the utility of all states by facilitating each state's ability to regulate matters that are connected to that state.

Larry Kramer, *Rethinking Choice of Law*, 90 COLUM. L. REV. 277, 294-95 (1990).

32. *See infra* Part IV.B.

33. *See infra* Part V.A.

34. *See supra* note 18.

35. *See, e.g.*, Editorial, *Adapting Old Laws to New Technologies: Must Microsoft Turn Over Emails on Irish Servers?*, N.Y. TIMES (July 27, 2014), http://nyti.ms/1teVwpx; Somini Sengupta, *Updating an E-mail Law from the Last Century*, N.Y. TIMES (Apr. 24, 2013), http://nyti.ms/YSV2Ck.

36. *See* Andrew K. Woods, *ECPA Reform: A Primer*, JUST SECURITY (Sept. 16, 2015, 9:59 AM), https://www.justsecurity.org/26120/ecpa-reform-primer (summarizing five competing proposals to reform ECPA).

37. *See infra* Part V.A.

38. *See infra* Part V.D.

39. I am aware of one article that looks at how the cloud affects jurisdiction and choice of law, but the authors conclude that the cloud is so radically novel that it requires entirely new legal concepts. Andrews & Newman, *supra* note 20, at 372-73 ("[T]he territorial-based conception of states and nation-states may be quickly becoming archaic in an increasingly connected world, calling into question the validity of choice-of-law methodologies that were developed in the Pre-Network Era." (footnote omitted)).

There is a large and growing literature on the U.S. government's surveillance of Internet data[40] and, relatedly, American search and seizure law.[41] These are important inquiries, to be sure, but existing statutory and constitutional law are insufficient on their own to settle these antecedent jurisdictional questions.[42] Early Internet jurisdiction scholarship touches on these questions only obliquely.[43] That scholarship was largely about spillovers: behavior in one state spilling over into another state via the Internet.[44] The jurisdictional question in such a case is whether a nation may "apply its law to extraterritorial behavior with substantial local effects."[45] This Article is concerned with something else: how a nation can apply its laws to local behavior with local effects when the data related to the act happens to be stored in the global cloud.

---

40. For a recent sampling, see Ryan Calo, *Can Americans Resist Surveillance?*, 83 U. CHI. L. REV. 23 (2016); Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291 (2015); Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513 (2014); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013); and Christopher Slobogin, *Standing and Covert Surveillance*, 42 PEPP. L. REV. 517 (2015).

41. *See, e.g.*, Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. (forthcoming 2016); Kerr, *supra* note 15; Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

42. The only brief, out of the dozens filed, in the *Microsoft Corp.* litigation that recognizes this fact is Apple's. *See* Brief in Support of Appellant Microsoft, Inc. by Apple Inc. as Amicus Curiae at 10-14, Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. Dec. 15, 2014) (arguing that the case raises fundamental conflict-of-laws and comity concerns, which were ignored by the lower court). This is consistent with the Supreme Court's decisions on prescriptive jurisdiction. *See, e.g.*, Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 272 (2010) (noting the distinction between the permissible scope of prescriptive jurisdiction pursuant to customary international law and what Congress in fact authorized by statute). For further discussion of this distinction, see Simowitz, *supra* note 24, at 302 n.159.

43. *See, e.g.*, Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1202-05 (describing the view of so-called "regulation skeptics" who argue that Internet disputes are difficult or impossible to regulate); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1400-01 (1996) (arguing that cyberspace requires an entirely new set of regulatory rules distinct from those that apply to physical space); *see also* Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991, 1019-23 (1998) (arguing that regulatory arbitrage will play out differently for big and small players).

44. Jack Goldsmith, *The Internet, Conflicts of Regulation, and International Harmonization*, *in* GOVERNANCE OF GLOBAL NETWORKS IN THE LIGHT OF DIFFERING LOCAL VALUES 197, 200 (Christoph Engel & Kenneth H. Keller eds., 2000) ("[T]he extraterritorial spillover effects of unilateral national regulation of Internet transactions are both inevitable and legitimate.").

45. Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1208.

The Article proceeds in five parts. Part I outlines the scope of the problem, one in which state laws and company policies conflict, international cooperation is effectively broken, and states have incentives to take drastic measures to get access to data needed to enforce the law. Part II then shows that although this problem is consequential, it is not without precedent; data can be easily analogized to physical goods—and a large number of courts have suggested in insurance claims that data is a physical good—as well as intangible assets such as money and debts. Drawing from these precedents, Part III identifies the relevant bases upon which a state might legitimately assert jurisdiction over cloud data, and Part IV looks for lessons drawn from similar cases regarding transnational conflicts of laws. Finally, Part V applies these lessons to a number of pending legal issues, including, most importantly, ECPA reform.

I. The Problem

There is an enormous amount of personal data stored in the global cloud, and there are times when governments have a legitimate interest in accessing that data. But for various reasons—competing claims of jurisdiction, blocking statutes, company policies, and more—governments often find that they are unable to lawfully access cloud-stored data, especially when the data is managed by a foreign company or stored on foreign servers. This has a number of undesirable consequences, including incentivizing governments to pursue that data by covert means, demanding that all Internet companies store data in-country, and more.[46] Paradoxically, existing barriers to legitimate government access to online data—barriers that are celebrated by electronic privacy advocates—have contributed to the further erosion of online privacy by encouraging states to seek the data by other means.

A. Evidence in the Global Cloud

As the Supreme Court noted in 2014, a growing number of people store their most sensitive personal data in the cloud.[47] Indeed, one of the greatest societal and technological shifts in recent years has been the move from storing data and software on a local machine—such as a cell phone or computer—to storing that data remotely on faraway servers, which can be accessed by a

46. ANDREW K. WOODS, GLOB. NETWORK INITIATIVE, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET AGE 3-4 (2015).

47. *See* Riley v. California, 134 S. Ct. 2473, 2489-91 (2014) (noting that the privacy aspects of the case dwarf those of earlier cases because of the highly personal information stored digitally, both on cell phones and in the cloud).

network such as the Internet.[48] The evolution of e-mail services provides a nice example of this trend. When e-mail was first introduced, users stored their messages locally, on their computers.[49] If a user sent an e-mail, she retained a copy on her machine and the recipient retained a copy on his machine.[50] The data existed in two locations, known to both users; intermediaries may have stored the emails briefly, but the user was responsible for storing and maintaining the inbox, much like physical mail.[51] This is no longer the way e-mail works for many people. The inbox is now managed by a third party that stores the e-mails on its own servers rather than on the user's computer, and users access these remotely stored inboxes whenever they need them, using a series of different tools—websites, applications, and so on.[52] E-mail has largely shifted from being a local service to being a cloud-based service. The same shift has occurred in many other aspects of digital life: photos, movies, music, online banking, and much more.[53]

It is hard to quantify this shift, but it has been enormous. One estimate suggests that while 7% of all electronic data was stored in the cloud in 2011, that

48. *See, e.g.*, JANNA QUITNEY ANDERSON & LEE RAINIE, PEW RESEARCH CTR., THE FUTURE OF CLOUD COMPUTING 2 (2010), http://www.pewinternet.org/files/old-media//Files/Reports/2010/PIP_Future_of_the_Internet_cloud_computing.pdf ("A solid majority of technology experts and stakeholders participating in the fourth Future of the Internet survey expect that by 2020 most people will access software applications online and share and access information through the use of remote server networks, rather than depending primarily on tools and information housed on their individual, personal computers.").

49. Indeed, the early technical protocols for e-mail were built around the concept of locally stored e-mail. The Post Office Protocol (POP) is designed for users to pull e-mails down to their local machines, rather than store them remotely on the server. *See* J.K. Reynolds, *Post Office Protocol* 1-2 (Internet Eng'g Task Force (IETF) Network Working Grp. Request for Comments (RFC) No. 918, 1984), https://tools.ietf.org/html/rfc918 (describing how the client requests mail from the server, which is delivered to the local machine and removed from the server). Today, the technical standard used by the most popular services is Internet Message Access Protocol (IMAP), which calls for remotely stored e-mails. *See* M. Crispin, *Internet Message Access Protocol—Version 4*, at i (IETF Network Working Grp. RFC No. 1730, 1994), https://tools.ietf.org/html/rfc1730 (stating IMAP "allows a client to access and manipulate electronic mail messages on a server").

50. Eric Z. Goodnight, *Email: What's the Difference Between POP3, IMAP, and Exchange?*, HOW-TO GEEK (Sept. 29, 2014), http://www.howtogeek.com/99423/email-whats-the-difference-in-pop3-imap-and-exchange.

51. *Id.*

52. *Id.*

53. *See, e.g.*, Harry McCracken, *Four Ways to Put Your Stuff in the Cloud*, TIME (July 14, 2011), http://ti.me/SHDqZO (describing how to move towards remote storage for photos, videos, music, and more).

number is projected to be 36% by the end of 2016.[54] According to another estimate, 55% of the consumer Internet population will use personal cloud storage by 2019, and 86% percent of data processing will happen remotely—in cloud data centers—rather than locally.[55] And because many of us now store much of our personal data online, using services provided by companies from different countries, our data is spread around the world.[56] There has been, in other words, an "internationalization" of personal data.[57]

This is especially true for Internet users located outside the United States, given that the largest global technology companies are currently U.S.-based. For example, U.S. firms run 9 out of the 10 most popular websites in India,[58] 7 out of 10 in Brazil,[59] 9 out of 10 in the United Kingdom,[60] and 7 out of 10 in Germany.[61] A few years ago, one might have attempted to explain this fact by arguing that only a small sliver of these countries' populations use the Internet, a cosmopolitan elite that primarily accesses American sites, but today the reality is far different: the Internet has simply become globalized.[62] As of November 30, 2015, the United States accounted for less than nine percent of the world's Internet users, which are estimated to number over three billion people.[63] Moreover, as the rest of the world comes online, the United States'

54. Kaamil Nakhasi, *Almost 50% of World Data to Be on the Cloud—Gartner*, CLOUDTWEAKS (July 10, 2012), http://cloudtweaks.com/2012/07/50-percent-of-world-data-to-be-on-the-cloud-gartner.

55. CISCO, CISCO GLOBAL CLOUD INDEX: FORECAST AND METHODOLOGY, 2014-2019, at 1-2 (2015), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf.

56. *See* Kerr, *supra* note 15, at 287-88 (describing the global spread of information as the Internet spreads).

57. WOODS, *supra* note 46, at 2 (quoting industry analyst).

58. *See Top Sites in India*, ALEXA, http://www.alexa.com/topsites/countries/IN (last visited Apr. 4, 2016).

59. *See Top Sites in Brazil*, ALEXA, http://www.alexa.com/topsites/countries/BR (last visited Apr. 4, 2016).

60. *See Top Sites in United Kingdom*, ALEXA, http://www.alexa.com/topsites/countries/GB (last visited Apr. 4, 2016).

61. *See Top Sites in Germany*, ALEXA, http://www.alexa.com/topsites/countries/DE (last visited Apr. 4, 2016).

62. Kerr, *supra* note 15, at 287 ("The last twenty years have witnessed a dramatic globalization of the Internet.").

63. *See North America Internet Usage Statistics, Population and Telecommunications Reports*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats14.htm (last updated Feb. 15, 2016) (estimating that 280,742,532 of the world's 3,366,261,156 Internet users, or 8.3%, were based in the United States as of November 30, 2015).

share of Internet users is in decline.[64] This helps to explain why Internet companies see expansion into foreign markets as a top priority.[65]

The combination of the rise of cloud computing and the globalization of the Internet means that a person and his data are now often separated by great distances and possibly several jurisdictions.[66] This has practical and legal consequences. As a practical matter, it has obvious security implications. One estimate suggests that fifty percent of adult Americans had their data compromised in a single year, spanning 2013 to 2014—not because their computers were compromised, but because they wittingly or unwittingly stored data in a cloud service that was hacked.[67] As a jurisdictional matter, resolving these security breaches is complicated by the fact that people and their data may be in different jurisdictions, or in multiple jurisdictions, which means that the government with the most regulatory power over their data may not be the user's own.[68]

Just as this data has become precious to citizens, it has become indispensable to governments. Governments seek lawful access to Internet data for a host of reasons, including counterterrorism operations, immigration control, and many other administrative matters.[69] Data is crucial to many law enforcement investigations, and not only as a supplement to physical evidence. As people live more of their lives online, the evidence sought by law

64. Orin Kerr cites the figure as 9.6% as of December 2013, less than two years prior to the November 2015 statistics. Kerr, *supra* note 15, at 287 & n.7.

65. *See* Evelyn M. Rusli, *Tech Companies Struggle to Get World on Internet*, WALL ST. J. (Apr. 21, 2015, 11:54 AM ET), http://on.wsj.com/1mqmYzl.

66. *See* Bruce Schneier, Programme Dir., Int'l Diplomatic Acad., Cloudy Jurisdiction: Addressing the Thirst for Cloud Data in Domestic Processes, Remarks at the Seventh Annual Internet Governance Forum (Nov. 7, 2012) ("[O]ur data is moving to the cloud[,] . . . [p]erhaps held by a third party, perhaps held in a different country . . . .").

67. Jose Pagliery, *Half of American Adults Hacked This Year*, CNN MONEY (May 28, 2014, 9:25 AM ET), http://cnnmon.ie/1wkryAp (attributing the vulnerability of so much personal data to the fact that it is stored online).

68. For example, the European Court of Justice recently invalidated a safe harbor agreement that had enabled U.S. firms operating in Europe to transfer customer data back to the United States for storage and analysis, and the court's analysis turned in part on the claim that European governments could not guarantee that the data would be safe from intrusion if it was stored in the United States. Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R., http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

69. *See, e.g.*, SEC'Y OF STATE FOR THE HOME DEP'T, DRAFT INVESTIGATORY POWERS BILL (2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf (detailing a bill that would, if adopted, grant the U.K. government the authority to seek Internet data in a wide range of scenarios beyond criminal law enforcement).

enforcement is often available exclusively online.[70] Twenty years ago, a kidnapper might have confessed to a crime by writing in his diary. The police, with cause and a warrant, might search the suspect's apartment for that admission. Today, the same admission is just as likely to be stored online, far from the reach of the police. Instead of seeking access to the suspect's apartment, the police would seek access to his e-mail account, which may or may not be managed within their jurisdiction. Increasingly, the evidence that law enforcement officers seek is stored on servers controlled by a foreign company, and that company would assert that the data is in another jurisdiction.[71] Suppose, for example, that a British user creates an e-mail account with Google, and his data is stored in California.[72] Suppose further that this British user runs into trouble with the law for not having paid his taxes. The state might effect a seizure of his assets and a search of his apartment. If the police thought that his cloud-based data was relevant to their investigation, they might approach Google to ask for the location data and time of his last login, the contents of his e-mails, the e-mail address associated with his name, and more. Google would probably refuse to hand over most of that data—including the stored contents of his online files and e-mails—on the grounds that the only state with the authority to compel it is the United States.

This problem is not limited to a small number of exotic cases. In 2014 alone, the British government sought customer data for at least 53,947 separate user accounts controlled by American technology companies.[73] Collectively,

---

70. *See* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 279-80, 307 (2005).

71. This is because the vast majority of the world's most popular e-mail and cloud storage platforms are American, and many of those providers assume that the data they store is, for jurisdictional purposes, held in the United States. This is the view of Google and Facebook, for example. *See supra* note 29.

72. Or the data may be moved around and stored in a number of different places, as Google deems fit. *See, e.g.*, Transcript of July 31, 2014 Hearing at 20, *Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d 466 (S.D.N.Y 2014), *appeal docketed sub nom.* Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. argued Sept. 9, 2015) (No. 13 Mag. 2814) ("[T]oday with cloud services, it has been increasingly common for location of data to change from day to day, hour to hour.").

73. These statistics are not comprehensive; they represent simply the number of requests made to six major Internet companies: Apple, Facebook, Google, Microsoft, Twitter, and Yahoo!. These transparency reports can be found on the public websites of each company. *See* Apple, Report on Government Information Requests: January 1-June 30, 2014, http://www.apple.com/legal/privacy/transparency/requests-20140630-en.pdf (last visited Apr. 4, 2016); Apple, Report on Government Information Requests: July 1-December 31, 2014, http://www.apple.com/legal/privacy/transparency/requests-20141231-en.pdf (last visited Apr. 4, 2016); Microsoft, Law Enforcement Requests Report 2014: January-June, 2014, http://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/lerr (last visited Apr. 4, 2016) (to locate, select "2014 H1 Report" under "Download report"); Microsoft, Law Enforcement Requests Report 2014: July-December, 2014, http://www.microsoft.com

footnote continued on next page

six technology companies—Apple, Facebook, Google, Microsoft, Twitter, and Yahoo!—fielded 22,103 separate requests from the United Kingdom for customer data. On average, those requests led to some data being handed over to the British government in roughly sixty-seven percent of cases.[74]

Table 1
2014 U.K. Government Requests for
Internet Data from Major U.S. Service Providers

Internet Service Provider	Number of Requests for Data	Number of Users or Devices Affected	Percentage of Cases in Which Some Data Was Revealed
Apple (Jan.-June)	1180	19,057	51%
Apple (July-Dec.)	1052	4171	54%
Facebook (Jan.-June)	2110	2619	72%
Facebook (July-Dec.)	2366	2890	75%
Google (Jan.-June)	1535	1991	72%
Google (July-Dec.)	2080	2755	75%
Microsoft (Jan.-June)	4090	7562	78%
Microsoft (July-Dec.)	4518	8034	75%

/about/corporatecitizenship/en-us/transparencyhub/lerr (last visited Apr. 4, 2016) (to locate, select "2014 H2 Report" under "Download report"); Yahoo!, Transparency Report: Government Data Requests: January 1, 2014-June 30, 2014, https://transparency.yahoo.com/government-data-requests/index.htm (last visited Apr. 4, 2016) (to locate, select "January 1, 2014-June 30, 2014" under "Requests by Country"); Yahoo!, Transparency Report: Government Data Requests: July 1, 2014-December 31, 2014, https://transparency.yahoo.com/government-data-requests/index.htm (last visited Apr. 4, 2016) (to locate, select "July 1, 2014-December 31, 2014" under "Requests by Country"); *Countries—Google Transparency Report: January to June 2014*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/countries/?p=2014-06 (last visited Apr. 4, 2016); *Countries—Google Transparency Report: July to December 2014*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/countries/?p=2014-12 (last visited Apr. 4, 2016); *United Kingdom Requests for Data: January 2014-June 2014*, FACEBOOK, https://govtrequests.facebook.com/country/United%20Kingdom/2014-H1 (last visited Apr. 4, 2016); *United Kingdom Requests for Data: July 2014-December 2014*, FACEBOOK, https://govtrequests.facebook.com/country/United%20Kingdom/2014-H2 (last visited Apr. 4, 2016); *Information Requests (Government): January 1-June 30, 2014*, TWITTER, https://transparency.twitter.com/information-requests/2014/jan-jun (last visited Apr. 4, 2016); *Information Requests (Government): July 1-December 31, 2014*, TWITTER, https://transparency.twitter.com/information-requests/2014/jul-dec (last visited Apr. 4, 2016).

74. *See* sources cited *supra* note 73.

Internet Service Provider	Number of Requests for Data	Number of Users or Devices Affected	Percentage of Cases in Which Some Data Was Revealed
Twitter (Jan.-June)	78	220	46%
Twitter (July-Dec.)	116	371	34%
Yahoo! (Jan.-June)	1408	2037	47%
Yahoo! (July-Dec.)	1570	2240	30%
Total:	22,103	53,947	59%

It appears that only a tiny percentage of those cases—no more than a few percentage points—yielded stored contents like e-mails and other documents.[75] When U.S. technology firms hand over data to foreign governments, the data is almost entirely limited to metadata or basic subscriber information; non-U.S. law enforcement agents rarely obtain access to stored contents like e-mails and photographs, for the reasons described below.[76] This is striking: a police officer now must cross an international border in order to do her job, whereas twenty or even ten years ago, the same officer might have been able to investigate a routine crime like kidnapping without leaving her country. Just as crime has become increasingly global, evidence gathering has followed suit.[77] And yet, in order to obtain access to this crucial data, the law enforcement agent faces a seeming quagmire of unresolved jurisdictional puzzles.

B. Jurisdictional Confusion

Suppose that a woman has just been murdered in New Delhi, India. Her boyfriend, who had previously threatened to hurt her, is the primary suspect. The police get a warrant from a judge to search his apartment, but the only things in the apartment are a laptop computer cord and a phone charger; the laptop and phone are gone. Knowing that the suspect regularly uses a Gmail account, the police contact Google to get access to the account. But Google refuses to hand over the relevant data. As a company domiciled in the United States, Google must comply with ECPA, which prohibits the firm from releasing any stored communications (like e-mails) without a warrant from a

75. This data is available only from Apple, Microsoft, and Yahoo!. *See* sources cited *supra* note 73.

76. *See infra* Part I.B.

77. The trend of internationalization of law enforcement has been progressing for some time now. *See, e.g.*, PETER ANDREAS & ETHAN NADELMANN, POLICING THE GLOBE: CRIMINALIZATION AND CRIME CONTROL IN INTERNATIONAL RELATIONS (2006) (describing the trend of international cooperation in law enforcement efforts).

U.S. judge.[78] Importantly, Google contends that this statutory prohibition applies regardless of where the user data is stored.[79] However, ECPA does allow a U.S. data controller to release transactional data, such as login times, locations, and basic subscriber information, to foreign governments.[80] Google may therefore hand over this data if the request meets their internal guidelines.[81]

The result is an odd jurisdictional conflict. This case otherwise appears to be an entirely Indian matter—an Indian police officer investigating an Indian crime she suspects to have been committed by one Indian citizen against another, on Indian soil. Yet the Indian law enforcement agent must ask an American judge to sign off on her request to receive access to the data, despite the fact that an Indian magistrate has already deemed the data crucial to the investigation. Not only does this seem unfair, it has a number of unwanted consequences, as we will see in a moment.

Part of the problem is disagreement between major Internet companies about the right test for determining where data is located and whether a state's jurisdiction extends far enough to reach that data. Google and Facebook suggest that the relevant locus is the company's domicile; since they are headquartered in the United States, they argue in a number of different contexts that only the U.S. government can compel stored data content, regardless of where it is used.[82] This means that a British or Indian or Brazilian law enforcement official must request help from the United States to get evidence critical to enforcing her country's domestic laws when that data is stored by Google, even if the data is on a server outside the United States.

78. *See* 18 U.S.C. § 2703 (2014).

79. *See Transparency Report: Legal Process*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/legalprocess (last visited Apr. 4, 2016) (noting implicitly that Google responds to U.S. law enforcement requests for data regardless of the location of the server where the data is stored). Microsoft takes a different view. *See* Microsoft's Objections, *supra* note 4, at 1 (arguing that U.S. law enforcement can compel only data stored on servers in the United States, not data stored on servers abroad).

80. *See* 18 U.S.C. § 2701(c). ECPA also provides for a number of exceptions, one of which allows for voluntary disclosure of stored communications to governments without a warrant in the case of extreme emergencies. *Id.* § 2702(b)(8) (noting that an Internet service provider may divulge the contents of communications "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency").

81. *Transparency Report*, *supra* note 79 ("On a voluntary basis, we may provide user data in response to valid legal process from non-U.S. government agencies, if those requests are consistent with international norms, U.S. law, Google's policies and the law of the requesting country.").

82. *See supra* note 29 (summarizing Google and Facebook's view that they believe the relevant locus is the headquarters of the company, not the location of the data).

Microsoft, by contrast, asserts that the relevant locus ought to be the physical location of the data.[83] So if the data is resting in Redmond, Washington, when police seek access to it—whether American police or foreign police—they would need a legal instrument from a U.S. judge. If the data sits in an Irish data center, however, the Irish government may have the authority to access it while the U.S. government may not.

The Second Circuit may decide which of these tests prevails with regard to the Stored Communications Act.[84] But that will only answer the question of how far one law can reach to regulate U.S. companies. It will not solve the question of how to locate a Bitcoin account if the IRS seeks to levy it in a tax collection proceeding, for example. Nor will it resolve how a U.K. judge should decide where the data is located when a British citizen in London uploads data to the cloud, to be stored on servers controlled by a foreign company. Indeed, the far more challenging scenario—and far more common for foreign law enforcement—is when a government seeks data controlled by a foreign company, and the company disagrees with the government about who has jurisdiction to compel the data. To see how this might work from the perspective of the United States, imagine that the United States seeks data controlled by Viber, a Japanese online communication service with 711 million registered accounts.[85] If U.S. law enforcement agents sought data in connection with a crime that occurred in the United States, the data for which happened to be in Japan, would they have to ask Japan for the data? Or would they be able to compel it regardless of its location? Suppose that Viber had offices in the United States, and the U.S. government took the position that it could seize the office funds in order to compel Viber to hand over the data. How should a judge rule in this case?

---

83. *See* Brief for Appellant, *supra* note 28, at 26-27, 31-32 (concluding that the court's order would be an extraterritorial application of ECPA because the search in question would occur in Ireland, where the data is stored, suggesting that the relevant territorial question for determining ECPA's reach is where the data is stored, not where the company is domiciled).

84. *See* Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. argued Sept. 9, 2015).

85. By the end of 2015, Viber had 711 million unique customer IDs, a huge increase from the 495 million IDs reported the prior year. *See* Rakuten, Inc., FY2015 Fourth Quarter and Full Year Consolidated Financial Results, PowerPoint Presentation 70 (Feb. 12, 2016), http://global.rakuten.com/corp/investors/documents/results. Viber is owned by Rakuten, a Japanese company, but it is based in Israel and Cyprus. Chang-Ran Kim, *Japan's Rakuten Buys Chat App Viber for $900 Million to Expand Digital Empire*, REUTERS (Feb. 14, 2014, 5:10 AM EST), http://reut.rs/1jDKKEN. It is not immediately clear where Viber stores its data; the servers could be located in any of these countries, or somewhere else. Another example is Yandex, a Russian website that is fourth-largest search engine in the world and a major Internet company in Russia. Perfect 10, Inc. v. Yandex N.V., 962 F. Supp. 2d 1146, 1150 (N.D. Cal. 2013); *see* YANDEX, https://www.yandex.com (last visited Apr. 4, 2016). Yandex stores much of its data in Russia. *See Perfect 10*, 962 F. Supp. 2d at 1150-51.

There is very little precedent for such cases of cross-border government requests for data, which are soon to be commonplace. Note that this determination of when governments have jurisdiction over extraterritorial data—which the remainder of this Article is devoted to addressing—is not solely a matter of enforcement.[86] The largest American Internet companies, like Google and Facebook, have offices, staff, and other assets in foreign countries. In those cases, the question is not whether the foreign government has personal jurisdiction over the technology firm; clearly it does. Rather, the questions are: When would it be appropriate to exert that jurisdiction in order to obtain access to customer data, wherever it is held, and how should a court adjudicate a claim if another state asserts conflicting jurisdiction over the same data? Given all of this jurisdictional uncertainty, many countries find themselves asking for help from whatever government has clear authority to compel the data—typically the United States, since the world's largest Internet companies are headquartered there. Here, too, there are serious problems.

C. A Broken International System

Because it can often be hard to determine who has jurisdiction over data, and because companies and states take drastically different views about the proper scope of state jurisdiction over data, states often find that they must ask another state for help to get the data they seek. This can happen through a number of different channels. Letters rogatory—letters judicially issued across state lines requesting evidence held in another jurisdiction—are one such mechanism. But these are rarely used and extremely unreliable.[87] The more common mechanism for international cooperation regarding cloud-stored data is for one state to request mutual legal assistance from another state, a process that is guided by so-called mutual legal assistance treaties (MLATs).[88] There are hundreds of bilateral MLATs and a number of multilateral MLATs as well, such as the E.U.-U.S. agreement.[89] When one country requests mutual legal

86. Jurisdiction is classically divided into three categories: jurisdiction to adjudicate, jurisdiction to prescribe, and jurisdiction to enforce. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 401 (AM. LAW INST. 1987).

87. T. MARKUS FUNK, FED. JUDICIAL CTR., MUTUAL LEGAL ASSISTANCE TREATIES AND LETTERS ROGATORY: A GUIDE FOR JUDGES 3 (2014), http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf ("The process for letters rogatory is more time-consuming and unpredictable than that for MLATs. This is in large part because the enforcement of letters rogatory is a matter of comity between courts, rather than treaty-based. For these reasons, prosecutors typically consider letters rogatory an option of last resort for accessing evidence abroad, to be exercised only when MLATs are not available.").

88. *See* WOODS, *supra* note 46, at 3.

89. *See MLAT Index*, MLAT.INFO, https://mlat.info/mlat-index (last visited Apr. 4, 2016) (listing bilateral and multilateral MLATs).

assistance, it can take an extremely long time to complete the request—a result of the complicated nature of the process.[90]

In a typical case, law enforcement officials in a requesting state must translate their request into another language, submit it up their chain of command, and pass it along to a diplomat with the authority to communicate that request to the receiving country's central authority—which, because so many of the world's leading technology companies are based in the United States, is very often the U.S. Department of Justice's (DOJ) Office of International Affairs (OIA).[91] The OIA handles all requests of this sort and prepares the required paperwork for an MLAT request before passing it on to the U.S. Attorney in the jurisdiction of the company that controls the data.[92] The U.S. Attorney will review the submission and request a warrant under 28 U.S.C. § 1782 from a judge, who will then review the request to determine that it meets the Fourth Amendment standard of probable cause.[93] The FBI then takes the warrant to the data controller—typically an Internet company or nonprofit storing the data—and the data controller reviews the warrant. If the warrant is sufficient, and the data controller chooses to comply, they pass the data back through the chain to the requesting country.[94] The entire process has been estimated to take an average of ten months, and in some cases can take much longer.[95]

90. *See* WOODS, *supra* note 46, at 3.

91. *See* Kate Westmoreland, Process for Obtaining User Data from California Under a Mutual Legal Assistance Treaty (MLAT) 1 (n.d.), http://cyberlaw.stanford.edu/files/blogs/MLAT%20flowchart%20-%2012.19.14.pdf.

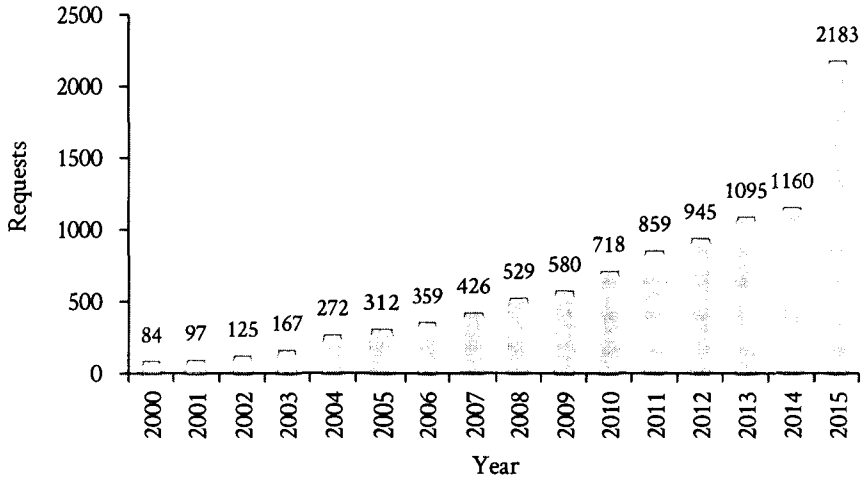
92. *See* FUNK, *supra* note 87, at 3, 6, 10.

93. *See id.* at 6, 8, 10.

94. *See* Westmoreland, *supra* note 91, at 1.

95. PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS 227 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

Figure 1
Foreign MLAT Requests for U.S.-Held Computer Records[96]



As the number of requests has skyrocketed, the DOJ has been unable to keep up.[97] The President's Review Group has recommended increased funding for the OIA specifically to handle MLAT requests,[98] and the OIA itself has asked for more funding.[99] But whether Congress will approve the funding remains to be seen.[100] Moreover, the number of requests has increased exponentially with the global spread of the Internet, and the OIA has been unable to meet the demand.[101] As the DOJ put it in its fiscal year 2017 request for funding from Congress: "Since FY 2000, the number of requests for assistance from foreign authorities handled by OIA has increased nearly 85%, and the number of requests for computer records has increased over 1,000%."[102] These trends do not appear to be slowing down. In fiscal year 2014, the OIA

96. U.S. Dep't of Justice, Foreign MLAT Request Data (on file with author).

97. WOODS, *supra* note 46, at 10.

98. PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., *supra* note 95, at 226-28.

99. U.S. Dep't of Justice, FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Reform, http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf (last visited Apr. 4, 2016).

100. *See* Peter Swire & Justin D. Hemmings, *Re-Engineering the Mutual Legal Assistance Treaty Process*, 71 N.Y.U. ANN. SURV. AM. L. (forthcoming 2016) (manuscript at 26).

101. CRIMINAL DIV., U.S. DEP'T OF JUSTICE, PERFORMANCE BUDGET: FY 2017 PRESIDENT'S BUDGET 23 (2016), http://www.justice.gov/jmd/file/820926/download.

102. *Id.* at 24.

handled 3270 MLAT requests from foreign governments, and nearly 1200 of those requests were for computer records.[103] In the fiscal year 2015, the OIA handled roughly the same number of MLAT requests from foreign governments as the prior year (3352 versus 3270), but the number of foreign requests for *computer records* nearly doubled over the prior year (2183 versus 1160).[104] The OIA's resources have not increased to meet this new demand, and as a result a growing number of MLAT requests go unanswered: the current backlog of unanswered foreign requests for assistance—both MLAT requests and extradition requests—has grown to over 12,000.[105] These numbers, though alarming, do not reflect the true scale of foreign government interest in data controlled by U.S. companies, however; because the MLAT process is so slow, many law enforcement agents never even bother to file MLAT requests.[106]

D. Government Response

Because the data that states seek may be under another jurisdiction's control and international cooperation is so cumbersome, law enforcement officers may sometimes resort to other, less wholesome tactics to get access to the data. These tactics range from demanding that data be stored locally—a hugely costly requirement—to raiding the company offices, to engaging in surveillance. Each of these actions has costs—from raising the cost of doing business on the Internet to threatening Internet users' privacy.[107] Mitigating these harms is one of the best motivations for resolving jurisdictional conflicts over Internet data and devising a more efficient regime for sharing cloud-based evidence across borders.[108]

As noted, because some companies and countries have decided that the location of the data is determinative of jurisdiction, a number of states have moved to require that Internet companies store all relevant data locally. For example, Brazil considered passing a bill that would give the executive branch the power to force Internet companies "to install or use structures for storage,

103. CRIMINAL DIV., U.S. DEP'T OF JUSTICE, FY 2016 PRESIDENT'S BUDGET 23 (2015), https://edit.justice.gov/sites/default/files/jmd/pages/attachments/2015/02/02/10._criminal_division_crm.pdf; E-mail from Ian Musa, Bus. Process Manager, Office of Int'l Affairs, U.S. Dep't of Justice, to author (Feb. 19, 2016) (on file with author).

104. CRIMINAL DIV., *supra* note 101, at 24.

105. *Id.* at 25.

106. Skype Interview with Anonymous Officer, United Nations Office on Drugs & Crime (Sept. 8, 2014).

107. *See* Matthias Bauer et al., *The Costs of Data Localisation: Friendly Fire on Economic Recovery* 2 (Eur. Ctr. for Int'l Political Econ., Occasional Paper No. 3, 2014), http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf (attempting to quantify the costs of data localization requirements and related privacy laws).

108. The Article turns to the more practical aspects of these reforms in Part V below.

management and dissemination of data in the country."[109] Russia went further, passing a localization law that it is now enforcing.[110] Data localization has been described as a threat that might "break" the Internet.[111] This is somewhat of an exaggeration: the Internet has long appeared different in different countries, reflecting each state's considerable and enduring power to regulate electronic content within its borders; this is unlikely to stop any time soon.[112] But data localization measures can nonetheless impose a number of considerable costs.

First, perhaps most obviously, localization requirements create significant efficiency costs.[113] The very point of a distributed network is to be able to store and move data through the network—including data load balancing—in ways that maximize efficiency.[114] If an Internet user flies from New York to Sao Paolo and accesses the same Internet services in both cities, it may make sense for her Internet companies to cache some of her data in servers closer to Sao Paolo than New York. But it may not. What if she is in Brazil for two days—should the service provider be forced to port all of her data into the country just because she accessed the service while on vacation there? It would

109. Lei No. 12.965, de 23 de Abril de 2014, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 24.4.2014 (Braz.), *translated in Macro Civil Brazilian Internet Bill of Rights: English Translation*, ASS'N FOR PROGRESSIVE COMM., https://www.apc.org/en/blog/marco-civil-brazilian-internet-bill-rights-english (last visited Apr. 4, 2016); *see also* Arthur Rodrigues do Amaral et al., *Marco Civil da Internet: Brazil's New Internet Law Could Broadly Impact Online Companies' Privacy and Data Handling Practices*, HOGAN LOVELLS (May 5, 2014), http://www.hoganlovells.com/marco-civil-da-internet-brazils-new-internet-law-could-broadly-impact-online-companies-privacy-and-data-handling-practices-05-05-2014 (describing the possible effects of Brazil's localization bill on global Internet companies).

110. *See* Sergei Blagov, *Russia to Twitter: Comply with Data Localization*, BLOOMBERG BNA (Jan. 25, 2016), http://www.bna.com/russia-twitter-comply-n57982066518 (describing Russia's demands that Twitter store data collected about Russian citizens locally on Russian soil in accordance with the recently passed data localization law).

111. Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 713 (2015) (describing data localization bills as efforts that "break the World Wide Web").

112. *See* GOLDSMITH & WU, *supra* note 26, at 180-81 (describing how states have significant control over the Internet's appearance and behavior within a particular country, contrary to the predictions of a number of scholars that the Internet would behave as a transnational space beyond state control).

113. *Cf.* Ned Schultheis, Note, *Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry*, 9 BROOK. J. CORP. FIN. & COM. L. 661, 663 (2015) (describing how "Microsoft and other U.S. cloud companies risk losing large sums of business to either foreign data storage companies or data localization movements" as a result of the SCA's unclear requirements).

114. *See Elastic Load Balancing*, AMAZON WEB SERVS., http://aws.amazon.com/elasticloadbalancing (last visited Apr. 4, 2016) (describing load balancing services as a way to distribute data in order to accommodate numerous requests for that data, so that each request is handled promptly).

certainly be a drag on the service's efficiency if every bit of data created by that user had to be stored wherever the service was accessible.[115]

Second, localization requirements impose considerable monetary costs on Internet companies, leading to increased user fees or reduced services.[116] Many Internet companies offer users a staggering array of no-fee services—things like e-mail, photo storage, and online banking. Many of these things are not free, of course—they are paid for with advertisements. But if the service costs go up for Internet companies, as they would under localization requirements, advertising costs would likely go up as well, possibly to the point where advertising will no longer pay for the free services.

Finally, and perhaps most importantly, data localization rules have significant implications for privacy. In states where data localization is mandated, it is considerably easier for states to surveil their citizens.[117] Moreover, data localization is unlikely to limit the U.S. National Security Agency's (NSA) ability to surveil Internet traffic; if anything, gathering all of a country's data in one place—and off U.S. soil—may make it easier for the NSA to surveil.[118]

Another tactic that states use to get the data that they cannot get through lawful channels, such as MLAT, is to bully or threaten companies to coerce them into handing over the data. For example, South Korean officials raided Google's offices in Seoul and seized digital evidence after it was alleged that Google had inappropriately collected users' data.[119] These sorts of tactics are often hard to document because, while some employee arrests and office raids make the headlines, law enforcement officers far more often use subtler means of intimidating Internet companies into cooperating with their requests for data.[120]

Yet another tactic deployed by states when they cannot get data with the company's assistance is covert surveillance.[121] This is problematic for obvious

115. *See* Bauer et al., *supra* note 107, at 3.

116. *See* Chander & Lê, *supra* note 111, at 721.

117. *See id.* at 735-38.

118. *See id.* at 714-18.

119. Song Jung-a, *South Korean Police Raid Google Offices*, FIN. TIMES (Aug. 10, 2010, 5:53 PM), http://on.ft.com/1MmoRcs.

120. *See* Andrew K. Woods, *Why Does Microsoft Want a Global Convention on Government Access to Data?*, JUST SECURITY (Feb. 19, 2014, 9:45 AM), https://www.justsecurity.org/7246/microsoft-global-convention-government-access-data.

121. *Cf.* Richard Salgado, Dir. Law Enf't & Info. Sec., Google Inc., Is the Internet Starting to Fracture?, Remarks at Brookings Institution Panel (Sept. 25, 2014), http://www.brookings.edu/events/2014/09/25-internet-starting-to-fracture (suggesting implicitly that countries may resort to covert surveillance due to temptation "to try to build their own surveillance infrastructure to match what they view . . . as being the capabilities of the NSA").

reasons, and it is beyond the scope of this Article to catalog all of the problems with Internet surveillance.[122] It should be self-evident that a regime in which government can lawfully access data in the cloud when that data is necessary for law enforcement is preferable to a regime in which government accesses the same data through covert surveillance.

The current state of affairs in cross-border data requests is suboptimal from nearly every perspective. Clearly, from the state's perspective, the inability to access data that is needed for law enforcement operations is a problem. From the perspective of Internet companies, being caught in the middle of two countries' dispute over jurisdiction may make it hard to establish clear and consistent policies. Finally, from the perspective of the user, the current regime is problematic because it encourages states to take extraordinary—and perhaps even illegal—measures to obtain data necessary for law enforcement. Some may look at the problem described here and ask, "What's the problem? States have too much access to data as it is—we should not make it easier for them." But a regime in which law enforcement officials can get access to digital evidence in which they have a legitimate interest is less of a threat to privacy than the regime we have now—one in which law enforcement officials cannot get the data they seek through lawful channels and, as a result, may resort to other tactics.[123] This is an underappreciated point: regardless of whether one's normative goals are to maximize user privacy, to maximize law enforcement capabilities, or to maximize the efficiency of the Internet, the equilibrium point is likely the same. More privacy can be achieved by giving governments greater lawful access to data in the cloud when that access is justified. As we will see, that requires a mechanism for determining under what circumstances governments have jurisdiction over data stored in the global cloud.

II. Is Data Different?

The growth of cloud-stored data presents a number of jurisdictional questions, which the next Part will address. But before asking whether data presents novel jurisdictional questions, it may make sense to ask whether data itself is conceptually exceptional. This Part attempts to show why claims about data's unique nature—as a mobile, divisible, location-independent asset—are largely overstated. Rather, data has analogues in both physical and intangible

122. For a nice overview of the subject, see BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015).

123. *See* Andrew K. Woods, *You Should Care About Mutual Legal Assistance More than You Do*, JUST SECURITY (Jan. 28, 2015, 12:13 PM), https://www.justsecurity.org/19449/care-mutual-legal-assistance.

assets, both of which provide useful precedents for courts attempting to determine the scope of law's reach into the cloud.

A. The Claim: "Data Is Different"

Given the radical change that the cloud represents—to the health sector, to the financial sector, and to everyday life—the claim that the rise of big data calls for new legal principles has intuitive appeal.[124] The digitization of once-physical experiences like communications and commerce represents a profound shift in the course of everyday life—a shift that has repercussions for social norms, the economy, and of course, the law.[125] So it is natural to think that this novel activity calls for novel legal principles.[126] This is the data exceptionalist view, and it turns on a number of claims about cloud-based data.

To be clear, these claims are not solely about the nature of data, but rather about the role of data in the cloud. For example, the mobility of data is not a jurisdictional problem unless that data is transmitted in a network that spans across borders, as the Internet does. If a French person writes in her diary while she is in France, her diary is in France. If she jots down her thoughts on an iPad while in France, that digital data is in France and the situation is functionally the same. The move from a paper diary to a digital one does not raise novel jurisdictional concerns. However, if the same person backs up her iPad to iCloud, her thoughts may be stored on servers in another country, and here we get into potentially novel territory.

Not only can the data be moved around quickly, but it also can be divided into many different pieces and flung into different jurisdictions. While a paper letter can be in only one place at one time, a digital letter might be divided up into many different component parts and distributed around the world, such that the data can be in more than one place simultaneously, and neither location needs to be the same as the location of the user.[127] The argument that data is unique and cannot be treated as territorial thus stems from the fact that it is mobile and divisible and commingles with other data.[128] Furthermore,

124. *See, e.g.*, Andrews & Newman, *supra* note 20, at 318 ("As with any disruptive leap forward in technology that ultimately alters real-space behavior, the move to the cloud carries with it implications for the administration of legal systems . . . .").

125. *See generally* 1 MANUEL CASTELLS, THE INFORMATION AGE: ECONOMY, SOCIETY, AND CULTURE; THE RISE OF THE NETWORK SOCIETY (2d ed. 2000) (describing the Internet's fundamental influence on nearly every aspect of daily life).

126. *See, e.g.*, David Friedman, *Does Technology Require New Law?*, 25 HARV. J.L. & PUB. POL'Y 71, 72, 85 (2002) (describing how the Internet and related technologies changed many aspects of life and explaining how some of this new activity will require new regulations).

127. *See* Transcript of July 31, 2014 Hearing, *supra* note 72, at 20.

128. Daskal, *supra* note 20, at 365-76.

because data is not tangible, it need not be tied to a particular location, giving data "location independence" between the user of the data and the location of the data.[129] But as the next subparts will illustrate, none of these features is entirely novel.

B. The Reality: Data Is Not So Different

Many of the features that are cited as evidence of data's unique properties are in fact neither novel nor unique to data. Indeed, for as long as global trade has existed, people have been commingling and moving their assets in and out of different jurisdictions and courts have managed to adapt their old, territorial rules to assets that cross territories.[130] This Subpart addresses each of the features of data that could potentially make data uniquely challenging from the standpoint of a legal regime rooted in territorial notions of jurisdiction. Because courts can choose to treat data as either an intangible or tangible asset, the analysis is divided into two categories.

1. Data as an intangible asset

a. Intangibility

One aspect of data that might lead one to believe that old, territorial rules will not easily apply is its intangible nature: the fact that we cannot hold digital ones and zeros in our hands. This intangibility, however, is not on its own a novel problem because courts have adjudicated disputes over intangible assets like stock and debts for many years.[131] Indeed, courts have come up with a

---

129. *Id.* at 369-70.

130. *See, e.g.*, United States v. First Nat'l City Bank, 396 F.2d 897, 900 (2d Cir. 1968) ("The basic legal question confronting us is not a total stranger to this Court. With the growing interdependence of world trade and the increased mobility of persons and companies, the need arises not infrequently, whether related to civil or criminal proceedings, for the production of evidence located in foreign jurisdictions.").

131. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 412 cmt. f (AM. LAW INST. 1987) ("Intangible property, regardless of where physical evidence of ownership may be, is ordinarily considered to be located in a state if the property consists of: (i) shares of a corporation or comparable juridical entity domiciled in the state; (ii) debt obligations of the state or subdivision of the state, or of a person (natural or juridical) resident or domiciled in that state; or (iii) rights created or protected by the laws of the state, such as patents, copyrights, and trademarks."). It is true that debt may be written up in a tangible paper instrument, but the physical location of that instrument does not control the location of the debt. The same is true for stocks, which are paper manifestations of an equity stake in a company. The paper stock certificates are not treated as tangible property except where the stock has been certificated. *See* Simowitz, *supra* note 24, at 13 n.36.

number of different approaches to locating intangible assets.[132] For example, intellectual property rights like trademarks are typically found to be located wherever they were created or registered.[133] Debts are typically located where the debtor resides[134]—as that is typically, though not always, where steps can be taken to ameliorate the debt. As early as the nineteenth century, shares of stock have been treated like mortgages, bonds, and promissory notes for the purposes of taxation: both the stock owner's domiciliary state and the issuer's state of incorporation are legally able to tax capital gains made from the sale of stock.[135] In property claims, corporate shares are typically found to be located in the state where the corporation was incorporated—not the location of the piece of paper that grants the holder stock ownership.[136]

As the *Restatement (Third) of the Foreign Relations Law of the United States* cautions, "intangible property may have different situs for different purposes, and none at all for some purposes."[137] The appropriate test for a court to apply when determining the location of data that is sought in connection with a criminal investigation may very well be different than the appropriate test for determining location for tax purposes or civil disputes. In fact, in many cases it will not matter where the intangible asset is located as long as the court has jurisdiction over a defendant who can command the asset's production.[138] But before turning to the jurisdictional grounds upon which a state might assert its

132. *See* Simowitz, *supra* note 24, at 13-20 (describing how courts have deployed a number of different fictions to give an intangible asset a physical location for jurisdictional purposes).

133. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 455 reporters' note 2 ("Intangible property rights created or protected by a state, such as patents, trademarks, and copyrights, are generally considered to have their situs in the state that created them—regardless of the location of the physical evidence of ownership.").

134. *Id.* ("[D]ebt obligations are generally considered located at the domicile or place of incorporation of the debtor but may have been contractually fixed by the parties at some other place, such as the head office of a bank or trustee.").

135. *See, e.g.*, Comment, *Conflict of Laws: Situs of Shares of Corporate Stock for Purposes of Taxation*, 7 CALIF. L. REV. 117, 119 & n.15 (1919) (noting the principle of *mobilia sequuntur personam* and citing a number of early cases that support the principle).

136. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 455 reporters' note 2 ("Ordinarily the shares of a corporation (or comparable juridical entity) are considered to have their situs at the corporation's place of incorporation....").

137. *Id.*

138. *See, e.g.*, United States v. Bank of N.S., 740 F.2d 817, 826-28 (11th Cir. 1984) (finding that bank records located abroad could be compelled in the United States, even where doing so would violate foreign law). Simowitz endorses applying this rule to all intangible assets. *See* Simowitz, *supra* note 24, at 316 (arguing that giving intangible assets a fictional situs is unhelpful and suggesting instead that courts can seize an asset in order to enforce a judgment where the court has personal jurisdiction over a party).

authority over cloud data, it is worth noting that there is a great deal of similarity between data and intangible assets, and courts have considerable experience negotiating claims involving those assets—either by giving them a fictional situs, or by ignoring the situs and granting jurisdiction nonetheless.[139]

b. Mobility

The data exceptionalists also suggest that jurisdiction based on location makes little sense when the subject is data because data is so mobile: it is easy to move data from one location to another at the speed of light.[140] But mobility, as a feature of an asset class, is hardly unique to data. Consider money, which can be wired from one location to another in an instant. Courts have little trouble determining the location of money for the purposes of asserting jurisdiction over the asset. The same is true for nearly everything, given the speed of modern communications and transportation networks. Courts have no special difficulty determining jurisdiction over people, goods, or any of the other highly mobile assets that regularly flow across jurisdictional lines. So data's mobility cannot be enough on its own to make us worry that territorial jurisdiction rules will be especially problematic.[141]

One feature of data that is not shared by debt, money, or other assets is how easy it is to copy and store in multiple locations at once. But this does not necessarily change the core of the territoriality analysis. Indeed, courts have inquired whether the act of moving data is meaningfully different from the act of moving material information. In an ongoing dispute regarding patent infringement, the U.S. International Trade Commission (ITC) found that it had jurisdiction, under section 337 of the Tariff Act of 1930,[142] over a patent dispute involving a Texas company that received digital files from a Pakistani company and then printed them, creating the infringing product.[143] On appeal, the Texas company, as well as a number of amici including industry groups representing Google and Apple, argued that the ITC did not have authority over the dispute because the e-mailed files did not constitute "importation of

139. *See* Andreas F. Lowenfeld, *In Search of the Intangible: A Comment on* Shaffer v. Heitner, 53 N.Y.U. L. REV. 102, 108 (1978) (describing how intangible assets at times have no situs at all).

140. *See, e.g.*, Daskal, *supra* note 20, at 366.

141. Data's mobility may mean that it passes through a number of jurisdictions and as a consequence is subject to a number of different authorities, but this is neither a novel problem nor one unique to data.

142. 19 U.S.C. § 1337 (2014).

143. *See* Certain Digital Models, Digital Data & Treatment Plans for Use in Making Incremental Dental Positioning Adjustment Appliances, the Appliances Made Therefrom & Methods of Making the Same, Inv. No. 337-TA-833, USITC Pub. 4555, at 2 (Mar. 30, 2012) (notice of institution of investigation).

'articles.'"[144] The Federal Circuit agreed, noting that when the Tariff Act was passed, the word "articles" did not refer to digital information.[145] The case seems to suggest that while data's mobility creates novel market arrangements, it does not present a fundamental theoretical challenge to the way we think about jurisdiction in the physical, territorial world.

c. Divisibility and fungibility

Another feature of data that some see as problematic for territoriality is its divisibility and, relatedly, its interchangeability.[146] That is, one user's data might be divided into several different parts and distributed on servers in different locations or jurisdictions. When an Internet user visits Flickr to view the photos he uploaded, for example, he does not have a claim over particular ones and zeros. Rather, the user asks the data holder (in this case, Yahoo!) to present him with a particular configuration of ones and zeros that will allow him to see what he deposited in the cloud.[147] The ones and zeros are divisible and interchangeable; the user does not care if they are the same ones and zeros that were initially uploaded to Flickr, or if they have been divided among or commingled with other ones and zeros, as long as they are configured in a certain, recognizable way when he calls upon them.

But these features are neither novel nor unique to data. Consider money in a bank account. When customers deposit two $5 bills with a bank, they do not expect the bank to hold that money in its exact form; indeed, they expect that the bank may divide that money up and distribute it widely around the bank's many branches (or with the bank's many other customers). But they expect that when they call upon the bank to make a withdrawal, the bank will give them $10—made up of some combination of $10 bills, $5 bills, and $1 bills.

144. Brief of Appellants ClearCorrect Operating, LLC, ClearCorrect Pakistan (Private), Ltd. at 7, ClearCorrect Operating, LLC v. Int'l Trade Comm'n, 2015 WL 6875205 (Fed. Cir. Nov. 10, 2015) (No. 2014-1527), 2014 WL 5318047; Brief of the Internet Association as Amicus Curiae in Support of Appellants and Urging Reversal at 2, *ClearCorrect Operating*, 2015 WL 6875205 (No. 2014-1527), 2014 WL 5427858; Brief for Business Software Alliance as Amicus Curiae in Support of Appellants in Favor of Reversal at 6, *ClearCorrect Operating*, 2015 WL 6875205 (No. 2014-1527), 2014 WL 5427859.

145. *ClearCorrect Operating*, 2015 WL 6875205, at *1 (stating that "articles" is defined as "material things," and thus does not extend to electronic transmission of digital data); *see also* Sapna Kumar, *Regulating Digital Trade*, 67 FLA. L. REV. 1909, 1912-13 (2015) (describing the debate over the *ClearCorrect* case); Editorial, *Keep the Internet Free of Borders*, N.Y. TIMES (Aug. 10, 2015), http://nyti.ms/1WcOwrE (arguing the ITC's ruling should be overturned given that it is not clear that the ITC has the authority to consider digital information to be "articles" within the meaning of the Tariff Act).

146. Daskal, *supra* note 20, at 368.

147. *See* FLICKR, https://www.flickr.com (last visited Apr. 4, 2016) ("Flickr, a Yahoo company.").

These are not the same paper bills the user deposited—those have been divided and distributed—and they may not even be the same dollar configuration of bills—the customer may have deposited two $5 bills and received a $10 bill—but customers do not care because they recognize that money is divisible and fungible. Once the money is deposited, it will be divided up and it will commingle with other money; the user's only concern with the money is that it be there when the user visits the bank. Ones and zeros are fungible, too. What matters to the user is how those ones and zeros are reconfigured so that they appear familiar when the user calls the data up on their screen.

What about ones and zeros that are improperly displayed—ones and zeros that in a given configuration do not reflect the file or image that the user initially uploaded? Here, too, there is an analogue in the financial world. Suppose that a user deposits a single $100 bill of U.S. currency in a bank account. The bank might turn around and exchange that money for some amount of Mexican pesos or Japanese yen. If the account holder were to call upon the bank and receive pesos or yen, he may be disappointed—not unlike the Flickr user who may be disappointed to find his account filled with someone else's photographs (or worse, a configuration of ones and zeros that does not depict an image at all). The ones and zeros do not matter to the user, just as the particular $100 bill does not matter to the banker; what matters is what the data controller, like the bank, produces when the user comes calling.

d. Distance between the asset holder and the asset

The fact that users may not be in the same location as their data, and may not know where it is, has led some to suggest that data is incompatible with territorially bound legal rules.[148] But this separation is not unique to data. Money can be stored in an offshore bank account; debts can be held against someone in another jurisdiction; and someone might hold stock in a mutual fund that is located in another jurisdiction, and the mutual fund might hold stocks in companies distributed around a huge number of jurisdictions. In each of these scenarios, there is a jurisdictional barrier between the asset holder and the asset, and yet courts have simple rules to establish a location for the asset and to determine their jurisdiction over the dispute in question.[149] Data should be no different.

2. Data as a physical asset

All of the features that are thought to make data difficult to square with a territorial conception of jurisdiction are premised on the idea that data is hard

148. Daskal, *supra* note 20, at 369-73.

149. *See supra* notes 133-36 and accompanying text.

to locate. But in many ways, it is easier for courts to assert jurisdiction over data than over intangible assets because, unlike debts or stock, data has a physical and therefore territorial presence wherever it is stored. Unlike stocks, debts, and bank wires, data resides on physical drives that can be seized.[150] In fact, while it may feel to the casual Internet user as if data floats around in a transnational ether, it is in fact stored in a physical location, usually one near the user. Microsoft's own affidavits in the *Microsoft Corp.* case suggest that data centers are located as near as possible to the end user.[151] Moreover, as a number of network engineers and computer scientists attested in that case, it is in fact impractical for companies handling massive amounts of data to parse individual accounts and spread the accounts across different jurisdictions if they do not need to do so.[152] If the user stays put in a particular location, it makes sense for the data to stay put as well.

This suggests that data is in fact much more tangible than classic intangibles like debts or stock. It may not matter to typical banking customers whether their money is held in Switzerland, Japan, or the Cayman Islands, as long as it is available when they need it. Yet it does matter to typical cloud users where their data is stored because where it is stored affects how quickly they can access it and—crucially—which governments can access it. For example, when Google did not want China to have access to its customers' data, Google felt it necessary to move to Hong Kong.[153] Google stores customer data on servers in nearby Taiwan and Singapore, rather than in Hong Kong or China.[154] By doing this, Google can offer some of its services to customers in China but keep the data out of the reach of the Chinese authorities[155]—an

150. *See, e.g.*, Verne G. Kopytoff, *F.B.I. Seizes Web Servers, Knocking Sites Offline*, N.Y. TIMES: BITS (June 21, 2011, 5:54 PM), http://nyti.ms/RBVouW.

151. *See Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014) ("[B]ecause the quality of service decreases the farther a user is from the datacenter where his account is hosted, efforts are made to assign each account to the closest datacenter."), *appeal docketed sub nom.* Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. argued Sept. 9, 2015).

152. *See* Brief for Amici Curiae Computer and Data Science Experts in Support of Appellant Microsoft Corp. at 21, *Microsoft Corp.*, No. 14-2985-cv ("[T]he impracticalities of . . . partitioning very small segments of data across geographically dispersed data centers mean that a given individual's email will generally be isolated to a particular region, if not a particular datacenter and server, regardless of the vendor.").

153. *See* Miguel Helft & David Barboza, *Google Shuts China Site in Dispute over Censorship*, N.Y. TIMES (Mar. 22, 2010), http://nyti.ms/xHQBAt (describing Google's decision to leave China and its hope to retain some customers there by routing web users to its Chinese-language site based in Hong Kong).

154. Roland Lim, *Goodbye Google Data Center in Hong Kong*, ZDNET (Dec. 11, 2013, 9:14 AM GMT), http://zd.net/1kybGkX.

155. *See* Helft & Barboza, *supra* note 153.

arrangement that implicitly acknowledges the importance of data's physical location.

Courts have acknowledged data's physical properties in a number of different contexts. Some of the earliest cases were insurance claims where courts had to decide whether data losses were covered by a standard commercial insurance contract that protects against direct physical loss or damage. Most courts that considered the question answered in the affirmative.[156] The Fourth Circuit, the first federal appellate court to address the issue, found that data loss constitutes direct physical damage in *NMS Services, Inc. v. Hartford*.[157] In that case, one of the plaintiff's former employees used a backdoor program that he had installed while still at the company to remotely log in and delete important files and databases.[158] The defendant had insured the plaintiff for business income lost due to suspension of operations where that suspension was caused by "direct physical loss of or damage to property."[159] The court found that there was "no question that [the plaintiff] suffered damage to its property" and that it was physical damage.[160] As Judge Widener noted in his concurrence:

> [A] computer stores information by the rearrangement of the atoms or molecules of a disc or tape to effect the formation of a particular order of magnetic impulses, and a meaningful sequence of magnetic impulses cannot float in space. It is the fact that the erasure was a 'direct physical loss' that enables [plaintiff] to recover under the policy . . . .[161]

In a similar case, a district court found that under Louisiana law, data can be subject to "direct, physical 'loss or damage.'"[162]

Not all courts have found that data losses of this kind were tangible losses, however.[163] A California court found that where hard drives were erased but

156. *See, e.g.*, Se. Mental Health Ctr., Inc. v. Pac. Ins., 439 F. Supp. 2d 831, 839 (W.D. Tenn. 2006) (finding that data lost due to a power outage constituted direct physical loss under the insurance policy); Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc., No. 99-185, 2000 WL 726789, at *3-4 (D. Ariz. Apr. 18, 2000) (holding that data loss suffered due to a power outage was "physical damage" because without the data, the machines had little functionality); Lambrecht & Assocs. v. State Farm Lloyds, 119 S.W.3d 16, 26 (Tex. App. 2003) (finding that insurance company's own policy coverage for data stored electronically dictated that "such property is capable of sustaining a 'physical' loss," and therefore holding that the plaintiff's insurance coverage included data lost due to a virus).

157. 62 F. App'x 511, 514-15 (4th Cir. 2003).

158. *Id.* at 512-13.

159. *Id.* at 514 (emphasis omitted).

160. *Id.*

161. *Id.* at 515 (Widener, J., concurring) (citation omitted).

162. Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs., Inc., Civ. No. 10-809, 2012 WL 1094761, at *4 (M.D. La. 2012).

unharmed, there was no tangible loss.[164] And the Fourth Circuit—the same court that decided *NMS Services*—found that data is not tangible because it cannot be touched.[165] One explanation for this split is that courts are struggling with data's dual nature—at once physical and intangible. As we will see, both of these features may be grounds for a state to assert jurisdiction.[166]

C. Summary

At a deep conceptual level, data is not as novel as the data exceptionalists suggest. None of the features that are thought to make data novel are in fact novel—whether the features are considered individually or as a whole—and in fact, data is an easier case than some other assets because data has a physical location wherever it is stored. Courts have at least two lines of inquiry for determining when a state ought to be able to properly assert jurisdiction over data in the cloud. First, courts can treat data as an intangible asset, much the way they treat money, debts, stock, and other similar items. Intangible assets constitute a significant strand of conflicts-of-laws jurisprudence, and courts have long negotiated jurisdictional claims for assets that have no physical presence in a given jurisdiction.[167] Second, courts can treat data as the physical object that it is—electronic, magnetic, and physical switches that sit on servers that are bolted to the ground. To be sure, cloud-stored data raises a number of complex jurisdictional problems, but efforts to solve these problems need not begin from the premise that data changes the way that courts currently think about jurisdiction and location.

---

163. *See* John N. Love & Ann F. Ketchen, *Physical but Not Tangible: Electronic Data Losses*, LAW360 (Nov. 30, 2010), http://www.robinskaplan.com/~/media/pdfs/physical%20but%20not%20tangible%20electronic%20data%20losses.pdf?la=en (suggesting that data loss has been largely found to be direct physical loss, but there are some exceptions, especially in the third-party insurance context where the loss must be tangible as well as physical).

164. Ward Gen. Ins. Servs. Inc. v. Emp'rs Fire Ins. Co., 7 Cal. Rptr. 3d 844, 851 (Ct. App. 2003) ("Here, the loss suffered by plaintiff was a loss of information, i.e., the sequence of ones and zeros stored by aligning small domains of magnetic material on the computer's hard drive in a machine-readable manner. Plaintiff did not lose the tangible material of the storage medium. Rather, plaintiff lost the stored information. The sequence of ones and zeros can be altered, rearranged, or erased, without losing or damaging the tangible material of the storage medium." (emphasis omitted) (footnote omitted)).

165. Am. Online, Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp. 2d 459, 462 (E.D. Va. 2002) ("[C]omputer data, software and systems are not 'tangible' property in the common sense understanding of the word. The plain and ordinary meaning of the term 'tangible' is property that can be touched. Computer data, software and systems are incapable of perception by any of the senses and are therefore intangible.").

166. *See infra* Part III.

167. *See* Simowitz, *supra* note 24, at 7.

III. Jurisdiction over Data in the Cloud

The previous Part showed that data is not conceptually exceptional; this Part shows that even if data had unprecedented features, it would not shake "territoriality at its core,"[168] nor would it erode state jurisdiction.[169] Jurisdiction is and likely always will be rooted in territoriality. States are the sovereigns of their territory and their citizens.[170] Accordingly, they can regulate acts taking place on their soil as well as acts that affect their citizens, regardless of the location of those acts. This means that a state might legitimately assert its jurisdiction over a piece of data because that data or its controller is located in the state's territory, or simply because the data is needed for law enforcement there, regardless of where the data is stored or where the company is headquartered. It also means that Microsoft is wrong when it suggests that the territorial location of the physical drives is the sole determinant of which state's laws apply,[171] just as Google is wrong when it suggests that the sole determinant is the domicile of the company.[172]

According to longstanding international law jurisprudence, there are three general categories of jurisdiction: jurisdiction to prescribe, to enforce, and to adjudicate.[173] This Part will discuss the first two.[174] The importance of the

168. Daskal, *supra* note 20, at 397.

169. *Contra* Teresa Scassa & Robert J. Currie, *New First Principles?: Assessing the Internet's Challenges to Jurisdiction*, 42 GEO. J. INT'L L. 1017, 1063 (2011) ("Not only does the Internet pose new challenges for states in terms of how to determine when and how they should exercise their jurisdiction, the Internet and the related phenomenon of globalization also have an eroding effect on jurisdiction.").

170. This is quite an old principle. For a relatively recent treatment, see Joseph H. Beale, *The Jurisdiction of a Sovereign State*, 36 HARV. L. REV. 241, 252 (1923). *See also* JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS § 18, at 21 (Boston, Little, Brown & Co. 8th ed. 1883) (1834).

171. Brief for Appellant, *supra* note 28, at 31-33 (arguing that the territorial location of its servers is the relevant location for the purposes of the territoriality provisions of ECPA); *see also* Transcript of Oral Argument, *supra* note 12, at 4-5 (counsel for Microsoft agreeing with Judge Lynch's characterization of Microsoft's claim that it can choose where to store data, and that it must follow the laws of the state where the data physically rests, seemingly to the exclusion of other state laws).

172. *See* Vidal-Hall v. Google Inc, [2014] EWHC (QB) 13 (rejecting Google's contention that the court lacked jurisdiction to hear a case because the relevant activity occurred, in Google's view, in California).

173. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 401 (AM. LAW INST. 1987). Adjudicative jurisdiction represents the same concept as personal jurisdiction. This conversation assumes that personal jurisdiction is not a question because without personal jurisdiction, there is little to litigate.

174. In many of the scenarios discussed here, like that being litigated in *Microsoft Corp.*, the court's personal jurisdiction over the parties is simply not in question. Many of the earliest Internet jurisdiction cases were concerned exclusively with personal jurisdiction. In those cases, courts largely adopted one of two approaches: the *Calder*

footnote continued on next page

distinction between prescriptive and enforcement jurisdiction for the Internet was first identified by Jack Goldsmith, who noted that while states might have a number of reasons to regulate extraterritorial Internet activities, they may struggle to enforce them, a question explored in the second section of this Part.[175] Ultimately, the data exceptionalists are wrong to suggest that the cloud changes anything fundamental as a matter of prescriptive jurisdiction or enforcement jurisdiction; the same old (territorial) rules apply to this new Internet technology.

A. Prescriptive Jurisdiction

States have essentially five bases to assert the jurisdiction necessary to prescribe conduct. A state can prescribe law with regard to: (1) conduct that takes place within its territory; (2) persons or things within its territory; (3) extraterritorial conduct that has or is intended to have substantial effects within its territory; (4) the activities of its nationals regardless of location; and (5) conduct outside the state that is directed against the security of the state or its interests.[176] These categories are drawn from international law, and as such, they do not bind Congress,[177] but they do impact U.S. law in at least two ways. First, the categories influence judicial interpretation of statutes via the *Charming Betsy* principle, which holds that "an act of Congress ought never to be construed to violate the law of nations if any other possible construction remains."[178] Second, the categories find rich support in U.S. case law.[179] Translating these categories to the context of the *Microsoft Corp.* case, there are five—and possibly more—potential jurisdictional hooks that a state might use to assert jurisdiction over cloud-based data: (1) the location of the data; (2) the location of the harm; (3) the citizenship of the suspect; (4) the citizenship of the

"effects" test or the *Zippo* "sliding scale" test. *See* CTR. ON LAW & INFO. POLICY AT FORDHAM LAW SCH., INTERNET JURISDICTION: A SURVEY OF LEGAL SCHOLARSHIP PUBLISHED IN ENGLISH AND UNITED STATES CASE LAW 58 (2013), http://www.fordham.edu/downloads/file/1826/clip_internet_jurisdiction_-_united_states; *see also* Calder v. Jones, 465 U.S. 783 (1984); Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).

175. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1216-17 (describing the limits of enforcement jurisdiction).

176. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402.

177. *See* United States v. Yousef, 327 F.3d 56, 86 (2d Cir. 2003) (noting that "Congress is not bound by international law" and "may legislate with respect to conduct outside the United States, in excess of the limits posed by international law," but that Congress must explicitly state that they intend to do so).

178. Murray v. Schooner Charming Betsy, 6 U.S. (2 Cranch) 64, 118 (1804).

179. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 case citations.

victim; and (5) the citizenship of the data controller.[180] As a matter of prescriptive jurisdiction, a state might assert jurisdiction over the crime based on any of these elements.[181]

These bases for jurisdiction suggest that states have extremely broad latitude to prescribe laws that regulate overseas conduct, as long as that conduct touches the state's territory or its citizens through its effects.[182] One of the lessons of this analysis is that a single test for jurisdiction—the location of the data, as Microsoft urges,[183] or the location of the company headquarters, as Google and others urge[184]—is unlikely to dictate a state's ability to assert jurisdiction over data.[185] Rather, the last century of conflicts of laws shows courts embracing a mosaic of different grounds for asserting jurisdiction over a particular act, depending on the act's location, its effects, and the citizenship of the parties involved.[186] What follows is a brief discussion of only five potential grounds for asserting prescriptive jurisdiction over data in the cloud.

1. Location of the data

The first and perhaps most obvious basis for jurisdiction is the location of the data.[187] As the previous Part demonstrated, data is both territorial and intangible. The territorial aspect of data is unlikely to go away: as long as states can seize physical hard drives that are bolted down on their sovereign soil, it seems unlikely that they will accept—absent a voluntary waiver of sovereignty via treaty—limits to their jurisdiction over the physical evidence within their territory. Servers are tangible, physical evidence bolted to a particular

180. There are others, such as the location of the criminal and the victim, but the arguments for or against these bases are largely repetitive of the arguments for asserting jurisdiction over the activities in the state's territory, so they are omitted here.

181. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403.

182. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1208 ("[A] transaction can legitimately be regulated by the jurisdiction where the transaction occurs, the jurisdictions where significant effects of the transaction are felt, and the jurisdictions where the parties burdened by the regulation are from.").

183. Microsoft's Objections, *supra* note 4, at 21; *see also supra* note 171 and accompanying text.

184. *See supra* note 29.

185. Congress might nonetheless elect to pick a single test and voluntarily narrow the state's ability to reach data abroad, but as a matter of jurisdictional scope, international transactions are increasingly regulated by more than one jurisdiction.

186. Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1208 ("The earlier belief in a unique governing law for all transnational activities has given way to the view that more than one jurisdiction can legitimately apply its law to the same transnational activity.").

187. This is the only jurisdictional hook that Microsoft suggests should dictate which states have the ability to compel data. *See supra* note 171 and accompanying text.

territory, and they can be seized.[188] This fact will not disappear at the urging of legal scholars.[189] This will likely not come as a surprise to the general counsels of the leading Internet companies, who have chosen the locations of their servers with a number of concerns in mind.[190] There is no reason to think that regulatory arbitrage—which is already widely practiced on a global scale[191]—should not also extend to the world of Internet data.

2. Location of the harm

States have a considerable interest in ensuring that their laws are enforced. For this reason, one sound basis for jurisdiction would be to say that the state where the crime occurred has a compelling interest in gaining access to digital evidence necessary to enforce its laws. Suppose, for example, that law enforcement agents at Scotland Yard are investigating a string of bank robberies in London, and they decide that critical evidence likely resides on one of the suspect's Dropbox accounts. Dropbox has its headquarters in California, but until recently it relied on Amazon Web Services for its data storage, and Amazon stores data on servers around the world.[192] No one doubts

188. *See supra* note 23 and accompanying text.

189. As Goldsmith notes, enforcement jurisdiction very often ends up being a greater limitation on a country's ability to enforce its laws on the Internet than prescriptive jurisdiction or choice of law. This problem is considerably easier to solve when the data sit on servers within the state's territory that can be seized. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1217 ("A defendant's physical presence or assets within the territory remains the primary basis for a nation or state to enforce its laws.").

190. Henry McDonald, *Ireland Is Cool for Google as Its Data Servers Like the Weather*, GUARDIAN (Dec. 22, 2012, 7:08 PM EST), http://gu.com/p/3cy4p/sbl (describing how many of the world's leading technology companies have chosen to house much of their data in Ireland for a number of reasons, including a well-educated, English-speaking workforce; extremely low corporate taxes; and cool weather); *see also* Chertoff Grp., Law Enforcement Access to Evidence in the Cloud Era 8-9 (2015), http://www.chertoffgroup.com/cms-assets/documents/209798-892097.law-enforcement-access-to-evidence-in (noting how companies have an incentive to store data in the jurisdiction with the most favorable data access rules).

191. *See, e.g.*, Victor Fleischer, *Regulatory Arbitrage*, 89 TEX. L. REV. 227, 229-30, 275-76 (2010) (describing how legally sophisticated actors move their assets to different locations in order to take advantage of the different regulatory systems in place); Annelise Riles, *Managing Regulatory Arbitrage: A Conflict of Laws Approach*, 47 CORNELL INT'L L.J. 63, 64, 96-97 (2014) (describing how companies such as AIG conduct some transactions overseas in an effort to take comparative advantage of different legal regimes).

192. *See* Sebastian Anthony, *Amazon Launches Cut-Price Dropbox Competitor Zocalo, Takes a Page from Microsoft's Monopolistic Playbook*, EXTREMETECH (July 11, 2014, 8:06 AM), http://www.extremetech.com/computing/186150-amazon-launches-cut-price-dropbox-competitor-zocalo-takes-a-page-from-microsofts-monopolistic-playbook (describing how Dropbox has long used Amazon's servers to host its cloud service). Amazon's web servers are located around the world, so the data in this hypothetical could be in Germany, Ireland, or the United States. *See Region Table*, AMAZON WEB

footnote continued on next page

that the U.K. Parliament has the legislative jurisdiction to pass a law criminalizing bank robbery. Indeed, it has a rock-solid jurisdictional basis for doing so—namely, controlling the activities that occur on its soil.[193] Getting access to digital evidence related to a U.K. crime—evidence that may or may not be in the United Kingdom's territory—is a question of enforcement jurisdiction, which will be discussed in more detail below.

3. Citizenship of the suspect

Another possible nexus for jurisdiction is the citizenship of the user whose data is being sought. States have an interest in protecting their citizens, and so it makes good sense that courts would strive to allow states to define when and under what conditions law enforcement should be able to access a citizen's data, wherever it is stored. Of course, one of the problems with this test is that the citizenship of the user is not always clear. (Though between the state and the Internet service provider, one would presume that citizenship can often be determined.) A second, and perhaps more troubling, problem is that such a test could encourage gaming. Criminals seeking to keep their data at bay from law enforcement in a particular state may self-identify online as having citizenship in whatever country will make law enforcement's job the most difficult—presumably a country with a blocking statute.

4. Citizenship of the victim

Likewise, states have a considerable interest in protecting their citizens from harm. Regardless of where a crime has been committed, a state may have an interest in seeking evidence related to the crime in order to get justice for their citizen, the victim. This basis for jurisdiction raises similar concerns to those raised by a test that turns on the location of the user. First, it may be difficult to identify the citizenship of the victim, though again the data controller and law enforcement might work together to identify the user's citizenship. Second, citizens seeking extra privacy from their own government may self-identify as being from a foreign country precisely in order to limit

---

SERVS., http://aws.amazon.com/about-aws/global-infrastructure/regional-product-services (last visited Apr. 4, 2016). There is some evidence that Dropbox is moving away from Amazon Web Services, and this hypothetical might play out differently if Dropbox stores its data in-country. *See* Barb Darrow, *AWS in Fight of Its Life as Customers like Dropbox Ponder Hybrid Clouds and Google Pricing*, GIGAOM (July 25, 2014, 11:19 AM PST), https://gigaom.com/2014/07/25/aws-in-fight-of-its-life-as-customers-like-dropbox-ponder-hybrid-clouds-and-google-pricing.

193. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (AM. LAW INST. 1987) ("Subject to § 403, a state has jurisdiction to prescribe law with respect to . . . conduct that, wholly or in substantial part, takes place within its territory . . . .").

their home state's ability to access their data,[194] which could perversely make it difficult for their home state to help them in the event that they are victimized.

5. Citizenship of the data controller

Finally, states have a considerable interest in regulating the commercial activity that takes place on their soil, including transnational data storage and cloud computing services. For example, the U.S. government has the authority to dictate the activity of its citizen corporations abroad, including prohibiting the payment of bribes.[195] It should not matter that the activities of that company are felt around the world via the Internet, rather than by some other means. The U.S. government's interest in regulating the foreign behavior of an oil company and the foreign behavior of an Internet company ought to be the same. The government might have different substantive reasons for regulating one as opposed to the other, but its fundamental interest in regulating the corporation should not change.

Ultimately, there are a number of ways that states might assert prescriptive jurisdiction over cloud-based data. That data might be mobile, divisible, and stored on different servers around the world—those facts do not fundamentally change the state's ability to regulate things and people that touch its soil.[196] The harder question, especially in cases where the underlying crime is domestic but the data is stored in the cloud, is how to determine limits on the state's enforcement jurisdiction.

B. Enforcement Jurisdiction

The rule for enforcement jurisdiction is quite simple: "a nation can exercise enforcement jurisdiction only against persons or entities with a presence or

194. *See, e.g.*, Sealed Indictment at 1, 7, United States v. Paunescu, No. 13 Cr. 41 (S.D.N.Y. Jan. 17, 2013) (alleging that an Internet service provider violated the Computer Fraud and Abuse Act when it provided a hosting service that allowed people to mask their location and identity online in order to evade law enforcement detection).

195. *See* Foreign Corrupt Practices Act of 1977 §§ 103(a), 104, 104A, 15 U.S.C. §§ 78dd-1 to -3 (2014). The only federal appellate case to examine the scope of the Foreign Corrupt Practices Act (FCPA) is *United States v. Kay*, 513 F.3d 432, 440-43 (5th Cir. 2007) (endorsing the SEC's broad view that the FCPA covers not only payments made to foreign officials to obtain or retain business, but also any improper payments that facilitate general business activities).

196. Indeed, neither side in the *Microsoft E-mail Search Warrant Case* disputes the state's authority to proscribe the underlying conduct. *See* Government's Brief in Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within Its Custody and Control, *Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014), *appeal docketed sub nom.* Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. argued Sept. 9, 2015) (No. 13 Mag. 2814); Microsoft's Objections, *supra* note 4.

assets within its territory."[197] If an Internet company has an office or bank account in a country, those assets are liable to being seized in order to compel the company to hand over data held by the company, wherever it might happen to be stored.[198] In such a case, concerns about data's incompatibility with notions of territoriality are largely irrelevant. As Goldsmith wrote over fifteen years ago, "A defendant's physical presence or assets within the territory remains the primary basis for a nation or state to enforce its laws."[199]

Indeed, courts regularly enforce foreign judgments when they are able to assert personal jurisdiction over the defendant, even if the assets are not within the jurisdiction, as long as doing so would not subject the parties to double liability or egregiously violate foreign law.[200] This is well supported by case law in the United States and abroad. Ireland's own amicus brief in the *Microsoft Corp.* case asserts as much: "It appears that in certain circumstances, an Irish court is prepared to order the disclosure by an Irish corporation of information in its possession, notwithstanding that the information is physically located in another jurisdiction . . . ."[201] And over a half-century ago, the Second Circuit ruled that, "It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has in personam jurisdiction of the person in possession or control of the material."[202] This is true in criminal cases as well.[203] U.S. courts have been clear: global companies that publicly avail themselves of business opportunities in the United States are subject to this country's criminal laws, and they can be

197. Goldsmith, *Unilateral Regulation*, *supra* note 26, at 139.

198. Servers can be seized too, of course, which is one reason why the suggestion that data is not territorial makes little sense.

199. Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1217. This is largely the approach taken by courts evaluating American surveillance law, which places greater constitutional scrutiny on government action addressed towards both people and data within the United States. *See* Daskal, *supra* note 20, at 345.

200. Simowitz, *supra* note 24, at 7.

201. Brief of Amicus Curiae Ireland, *supra* note 11, at 7.

202. United States v. First Nat'l City Bank, 396 F.2d 897, 900-01 (2d Cir. 1968) (emphasis omitted).

203. While the *Restatement* claims that extraterritorial enforcement of criminal laws is universally condemned, it is generally allowed for discovery purposes. *Compare* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432 cmt. b (AM. LAW INST. 1987) ("It is universally recognized, as a corollary of state sovereignty, that officials of one state may not exercise their functions in the territory of another state without the latter's consent."), *with id.* § 442(1)(a) ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.").

compelled to bring assets and evidence from abroad into the United States.[204] U.S. courts will not issue warrants for extraterritorial searches.[205] But extraterritorial subpoenas are generally available, subject to a reasonableness test that balances the privacy interests of the person whose data is being searched with the government's interest in the data.[206] So even if the United States cannot send agents to another country to seize data held abroad, the United States can compel a company that operates in the United States and has violated U.S. law to produce those same documents if they relate to the crime.[207]

The crucial question in enforcement cases is not where the data is stored—or how mobile, interchangeable, or tangible it is—but rather whether the court can assert personal jurisdiction over a defendant with the ability to access that data.[208] This fact matters today in a way that it did not fifteen years ago because courts increasingly have personal jurisdiction over global Internet companies. When Goldsmith wrote about enforcement jurisdiction, he noted that enforcement jurisdiction serves as a significant limitation on states exercising jurisdiction over online actors, despite the fact that the activity is well within the state's prescriptive jurisdiction.[209] That is less true today. The major technology firms that have significant global Internet user bases also have significant assets and offices around the world. In 2004, Google had one office

204. *See, e.g.*, United States v. Bank of N.S., 740 F.2d 817, 828 (11th Cir. 1984) (noting that the cost of business in different foreign jurisdictions includes taking the risk that a conflict of laws may arise); *In re* One Grand Jury Subpoena Returnable January 11, 1989, No. N-89-7, 1989 WL 49165, at *3 (D. Conn. Mar. 22, 1989) ("[B]anks involved in international commerce must often face the risk of inconsistent government actions. That risk is an incident of international banking, and with the decision to enter that field of commerce comes such a risk.").

205. *See In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 171 (2d Cir. 2008) (noting that warrants do not have extraterritorial reach).

206. Orin Kerr, *What Legal Protections Apply to E-mail Stored Outside the U.S.?*, WASH. POST: VOLOKH CONSPIRACY (July 7, 2014), http://wpo.st/U5i91.

207. *See Bank of N.S.*, 740 F.2d at 828, 832.

208. Microsoft implicitly acknowledged this point when it set up a data center in Germany through an unusual trustee relationship with Deutsch Telekom that would give Microsoft no ability to control the data held there. *See* Glyn Moody, *Microsoft Building Data Centers in Germany that US Government Can't Touch*, ARS TECHNICA (Nov. 12, 2015, 10:07 AM PST), http://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch. This was likely designed so that customers storing their data there could be sure that the United States could not compel Microsoft to hand over that data using a *Bank of Nova Scotia*-type subpoena—a subpoena for foreign records—of the sort the government seeks to use in the *Microsoft Corp.* case.

209. Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1216.

with around 800 employees.[210] Today, the company has nearly 60,000 employees,[211] working in 70 offices in more than 40 countries.[212] If a country feels it has a legitimate interest in accessing data stored by Google, the critical question may not be where the data is stored, but rather whether the country can assert personal jurisdiction over Google's assets in the country.[213]

C. Integrated Analysis

Taken together, these grounds for jurisdiction provide the beginnings of a flow chart for thinking through the jurisdictional problems that arise when the state attempts to access data in the cloud. What if someone is kidnapped from Manhattan and the New York police has good reason to think that critical evidence might be in the Viber account of the victim's boyfriend, who is also missing? If the law enforcement agents ask Viber for the data, and Viber insists that they seek a warrant from a judge in Cyprus or Israel, how should a court approach the case?[214] The first question, of course, is whether the court has personal jurisdiction over the matter before it—what is classically referred to as adjudicatory jurisdiction.[215] Assuming that it does, the next question would be how existing law applies to the conflict.

The court would have to ask how the Fourth Amendment and the SCA apply to the Viber account and whether the Viber account is "extraterritorial." If the account is extraterritorial, it likely does not enjoy Fourth Amendment

---

210. *Our History in Depth*, GOOGLE, http://www.google.com/about/company/history (last visited Apr. 4, 2016).

211. Google Inc., Quarterly Report (Form 10-Q), at 32 (Sept. 30, 2015), http://www.sec.gov/Archives/edgar/data/1288776/000128877615000046/goog10-qq32015.htm ("Headcount increased to 59,976 as of September 30, 2015.").

212. *Google Locations*, GOOGLE, http://www.google.com/about/company/facts/locations (last visited Apr. 4, 2016).

213. This is consistent with the view of the United States in the Microsoft litigation. *See* Brief for the United States of America at 5, Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. Mar. 9, 2015) (citing with approval the magistrate judge's decision that Microsoft must produce the data sought, "regardless of the location of that information," given the issuance of the warrant). This analysis may become more complicated if the Internet service provider in question is incorporated as a subsidiary. The Supreme Court has recently narrowed the ability of courts to assert personal jurisdiction over a parent corporation based solely on its subsidiary, and vice versa. *See* Daimler AG v. Bauman, 134 S. Ct. 746, 761-62 (2014).

214. *See supra* text accompanying note 85.

215. This distinction is commonly taught in civil procedure courses as one between personal and subject matter jurisdiction. *See* JACK H. FRIEDENTHAL ET AL., CIVIL PROCEDURE: CASES AND MATERIALS 26 (10th ed. 2009) ("A court must be chosen that has jurisdiction over the subject matter of the suit and in which jurisdiction over the person of the defendant may be obtained.").

protections.[216] Whether and how the SCA applies is, of course, the core concern in the *Microsoft Corp.* case: Did Congress intend for ECPA to reach a criminal suspect's data where the data is stored on foreign servers?[217] If it is at all unclear, the court would have to inquire whether the legislature had the authority to reach the data in question. This is a prescriptive jurisdictional analysis, and as we have seen there are a number of legitimate grounds for asserting prescriptive jurisdiction over data. Finally, even if Congress has the prescriptive jurisdiction to reach the data, there is a remaining question about the scope of the state's enforcement powers over that data. The next question, of course, is whether exercising that jurisdictional authority would create a conflict of laws.

This analysis is deeply territorial and not fundamentally different from an analysis of jurisdiction over foreign-held intangible assets. The fact that the subject of the dispute is ones and zeros does not ultimately change very much about how the court asserts personal jurisdiction over the defendant, interprets existing constitutional and statutory law, or examines international law and common law limits on jurisdiction.

This may explain why a number of jurisdictions have asserted something akin to a minimum contacts test similar to that articulated in *International Shoe Co. v. Washington* to determine jurisdiction over Internet companies.[218] In the *Google Spain* case, for example, the European Court of Justice found that Google was properly subject to European regulation as a result of its Spanish subsidiary's "exercise of activity through stable arrangements in Spain."[219] And under the sweeping European Data Protection Directive, a firm can be bound by European law where the processing of personal data happens "in the context of the activities of an establishment of the controller on the territory of the Member State."[220] It may not be an easy task to identify a simple test for determining when sufficient contacts exist in the Internet space, but it is not conceptually as novel as it seems.

---

216. *See* Kerr, *supra* note 15, at 301.

217. *Microsoft E-mail Search Warrant Case*, 15 F. Supp. 3d 466, 467-68 (S.D.N.Y. 2014), *appeal docketed sub nom.* Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. argued Sept. 9, 2015). As Kerr notes about the case, this is essentially an open question: "[T]he Stored Communications Act just wasn't drafted with the problem of territoriality in mind. It assumed a U.S. Internet with U.S. servers and U.S. users." Kerr, *supra* note 206.

218. 326 U.S. 310, 316, 320 (1945) (finding a shoe company to have sufficient contacts for personal jurisdiction in the state of Washington because its sales efforts there were systematic and continuous).

219. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. para. 49, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.

220. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 4, 1995 O.J. (L 281) 31.

IV. Conflicts of Laws over the Cloud

Because there are many different grounds for states to assert jurisdiction over the same piece of data, cloud-based data will regularly be subject to overlapping jurisdictions.[221] Where two states' laws do conflict, courts have a suite of tools at their disposal. None of these tools change as a result of the fact that the subject of the conflict is data stored in the cloud. Ultimately, the conflicts-of-laws questions presented by cloud-based data are conceptually no different than other transnational activities, even if their consequences are more profound. This Part explains how basic conflicts-of-laws principles apply to disputes involving data stored in the cloud.

Before going any further, a clarification is in order. One could imagine objections to this proposal on the grounds that conflicts-of-laws principles derive from private law and this proposal applies them to public law disputes. But, this view leans too heavily on a simplistic distinction between public and private law. As Goldsmith noted over a decade ago when applying conflicts principles to early questions of Internet jurisdiction, some of the most influential conflicts principles were developed as a result of public law initiatives to control a globalizing world.[222] The history of conflicts cases—and indeed jurisdiction theory more broadly—involves a heavy dose of both private and public law cases. Moreover, as William Dodge has shown, there is a growing need for conflicts principles to be applied to public law subjects.[223] This is underscored by the fact that as the regulatory state has grown, so has the need for greater flexibility among conflicts rules. Indeed, "many of the transformative midcentury constitutional choice-of-law decisions involved public regulations rather than private law."[224]

A. A Conflicts Approach to Evidence in the Global Cloud

When should a country be able to get access to data stored in the cloud and possibly subject to another country's laws? The answer provided by conflicts of laws is simple: when the state has an interest in that data that outweighs competing state interests. Any single test for location of data would be overly narrow. Accordingly, it is wrong to say that the test is or even ought to turn exclusively on the location of the data or the domicile of the company. Rather, there are many different ways for a state to legitimately assert its jurisdiction

221. Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1208.

222. *Id.* at 1206 n.27.

223. William S. Dodge, *Breaking the Public Law Taboo*, 43 HARV. INT'L L.J. 161, 163 (2002).

224. Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1206 n.27 (citing a number of antitrust and workers' compensation cases).

over a given piece of data.[225] That is not to say that location is irrelevant. Rather, the state where the data is located will have an interest in the data. Given these various jurisdictional hooks, the next question is how courts ought to conclude that one state's interest in the data trumps another state's interest. The first challenge is to identify whether a conflict exists at all; if a conflict does exist, a court would then attempt to weigh the two states' interests in enforcing their laws, an analysis that may depend on the principle of reciprocity.

1. Identifying true conflicts

Regardless of how states define their jurisdiction over cloud-based data, conflicts are likely to arise. For example, we should expect that states will assert jurisdiction over data based on its tangible properties as well as its intangible properties. If some piece of data gives rise to jurisdiction in one location based on its intangible properties, and the data is stored in another location—one that might claim jurisdiction over it as a tangible asset—a conflict may arise.[226] But a true conflict of laws only exists where two states both have: (1) jurisdiction to prescribe certain conduct; (2) jurisdiction to enforce their laws such that there is a conflict about which state should have access to the relevant data; and (3) an interest in having their laws applied. That is, conflicts can only arise where state jurisdiction over a piece of data overlaps, and even then not all cases of jurisdictional overlap will produce a true conflict of laws.[227] The question is not whether one state's laws are incompatible with another state's laws; rather, the question is whether both states can apply their laws and have a compelling interest in doing so. If they do not have such an interest, there is merely a false conflict and the problem is resolved.[228]

It turns out that many potential conflicts are not, upon further inspection, conflicts at all.[229] By identifying the interest that a state has in regulating a particular piece of data, and the purpose the state has in regulating it, courts

225. As Goldsmith noted about Internet jurisdiction over a decade ago, this is consistent with the overall trend in conflicts jurisprudence. *See id.* at 1208 ("Any number of choice-of-law regimes are now consistent with constitutional and international law. The earlier belief in a unique governing law for all transnational activities has given way to the view that more than one jurisdiction can legitimately apply its law to the same transnational activity.").

226. This fairly describes the scenario in the *Microsoft Corp.* case, although Ireland has not explicitly argued that a conflict of laws exists. *See* Brief of Amicus Curiae Ireland, *supra* note 11, at 3.

227. *See* Kramer, *supra* note 31, at 292-93.

228. *Id.* Note that a true conflict can exist even if ruling that state *A*'s laws apply would put a party in the position of violating the laws of state *B*.

229. *See id.* at 291-304.

can often easily decide which state's interest should prevail in a given conflict. Suppose, for example, that the United States passes a law designed to promote entrepreneurship online. The law has provisions calling for, among other things, cybersecurity standards and data integrity standards. Now suppose that the U.K. law enforcement agents investigating a crime discover that they need access to a drug smuggler's e-mail account, an account that is managed by an Internet service provider that is subject to the U.S. law. In theory, this is a potential conflict because there is at least an overlap in jurisdiction. But in reality, there is no conflict at all: as long as giving the data to the U.K. law enforcement will not affect the U.S. goal of promoting entrepreneurship online, as it seems unlikely to do, there is no true conflict of laws.

2. Weighing state interests

A longstanding feature of conflicts jurisprudence—as the *Restatement* reflects in its reasonableness analysis—is the notion that courts could determine choice-of-law matters by balancing the competing state interests rather than relying solely on the location of the relevant activity.[230] Rather than ask simply where the harm occurred, courts ask which state has an interest in seeing its laws enforced in the case.[231] As Larry Kramer points out, this is not just a matter of tallying interests on one side and balancing them against the interests on the other side; rather, the interest analysis requires an inquiry into the purpose of the relevant law.[232] This is not the only approach courts have adopted—courts also use the vested rights approach, a comparative impairment approach, a better-law approach, and more.[233] But the Supreme Court in *Société Nationale Industrielle Aérospatiale v. U.S. District Court* largely endorsed the *Restatement*'s balancing of government interests approach in foreign affairs cases.[234]

This can be seen in a number of different areas of U.S. conflicts jurisprudence, but the area most relevant for this inquiry is the way that U.S. courts evaluate competing state interests in cases where evidence resides overseas, the production of which may violate another nation's sovereignty and or its substantive laws.[235] For example, in *United States v. Vetco Inc.*, a court

230. BRAINERD CURRIE, SELECTED ESSAYS ON THE CONFLICT OF LAWS 183-84 (1963).

231. *Id.*

232. *See* Kramer, *supra* note 31, at 285 (describing the first step of his two-step process for identifying conflicts).

233. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1207 n.32).

234. 482 U.S. 522, 543-44, 544 n.28 (1987) (endorsing the factors listed in the RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 437 (AM. LAW INST. 1987)).

235. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 reporters' note 7 ("Numerous decisions of United States courts have engaged in a

footnote continued on next page

weighed the interest of the United States in prosecuting tax fraud against Switzerland's interest in preserving business secrets and found for the United States, ordering the production of bank documents held abroad.[236] In that case, the records were held by a U.S. corporation's subsidiary in Switzerland,[237] which U.S. courts have generally found to be responsible for the production of documents held outside the United States.[238]

More recently, in *Linde v. Arab Bank, PLC*, the Second Circuit affirmed a district court decision to sanction a bank for failing to comply with an order to compel bank records held abroad in jurisdictions where their disclosure was illegal.[239] There are many similar cases.[240]

In these cases, courts must ask not only whether it is acceptable to compel a defendant to bring data into the state's territory, but also whether doing so would affect another state's interest.[241] This is a distinct question from whether the data is within the state's jurisdictional reach; rather, this is about whether compelling a defendant to bring into the state's jurisdiction documents that it could otherwise not produce would offend the sovereignty of another state. And the approach courts use in these cases is balancing the two states' interests in the data.

This approach is not without costs.[242] Indeed, one of the risks of this approach is that courts, somewhat unpredictably, rely on the notoriously

---

balancing of interests, both in determining the appropriateness of discovery orders in the face of foreign nondisclosure laws, Subsection (1)(c), and in considering sanctions for noncompliance, Subsection (2)(c).").

236. 691 F.2d 1281, 1289-91 (9th Cir. 1981).

237. *Id.* at 1284.

238. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 reporters' note 10.

239. 706 F.3d 92, 95-96 (2d Cir. 2013).

240. *See, e.g.*, United States v. Field, 532 F.2d 404, 407-09 (5th Cir. 1976) (holding that the United States' interest in investigating crime outweighed the Cayman Islands' interest in bank secrecy); United States v. First Nat'l City Bank, 396 F.2d 897, 902-05 (2d Cir. 1968) (requiring bank to produce documents in response to federal grand jury subpoena, despite the bank's insistence that removing the documents from Germany would expose the bank to civil and other penalties).

241. *Linde*, 706 F.3d at 98 (noting that courts must balance "(on the one hand) the interests of foreign governments in enforcing their laws and the potential hardship created for the Bank by its conflicting legal obligations, with (on the other hand) the interests of the United States in enforcing its laws and plaintiffs' need for the material in pursuing their claims").

242. Diplomatic tensions are one possible cost. *See* OFFICES OF THE U.S. ATTORNEYS, CRIMINAL RESOURCE MANUAL § 279(B) (1997) ("[T]he use of unilateral compulsory measures can adversely affect the law enforcement relationship with the foreign country.").

malleable concept of international comity[243] to decide whether another jurisdiction's interests weigh in favor of not compelling the evidence. For example, in *Ings v. Ferguson*, the Second Circuit found that "fundamental principles of international comity" dictated that two New York agencies seeking records held by a Canadian bank were required to file letters rogatory with a Canadian judge in order to determine whether the disclosures might violate Canadian law.[244] But unpredictability in the application of comity may 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. Such a system, as the next Part shows, offers a number of advantages over a top-down, uniform set of limits for state access to cloud data.[245]

3. Reciprocity

Finally, one of the fundamental principles of conflicts jurisprudence is the idea of reciprocity in the recognition and enforcement of foreign judgments.[246] When one state enforces another state's judicial decision, it sometimes does so on the condition that the first state would have done the same thing.[247] For states that regularly manage conflicts of laws, a reciprocity rule can work to both states' advantage over time.[248] This could easily be applied to the context of cloud data. For example, American courts could agree to respond to foreign law enforcement requests for data on an expedited basis if and only if the request comes from a country that processes American government requests for data expeditiously, a fact that could be established by affidavit from the State Department or the Office of International Affairs at the DOJ. Moreover, Congress could revise ECPA to allow for explicit reciprocity by allowing U.S. companies to respond directly to foreign government requests for information if and only if those requests come from countries that also allow their

243. For a summary of comity's malleability and unpredictability, see Michael D. Ramsey, *Escaping "International Comity,"* 83 IOWA L. REV. 893 (1998).

244. 282 F.2d 149, 152-53 (2d Cir. 1960).

245. *See infra* Part V.D.

246. *See* John F. Coyle, *Rethinking Judgments Reciprocity*, 92 N.C. L. REV. 1109, 1111 (2014) (describing the longstanding debate over reciprocity in enforcement of foreign judgments).

247. *See* Katherine R. Miller, *Playground Politics: Assessing the Wisdom of Writing a Reciprocity Requirement into U.S. International Recognition and Enforcement Law*, 35 GEO. J. INT'L L. 239, 244-46 (2004).

248. *See* Kramer, *supra* note 31, at 343 ("[W]here the same conflict of interest arises continuously, the parties can learn from one another—the long term costs of failing to do so are simply too great.").

companies to respond directly to U.S. government requests for data.[249] This may in fact be one way of discouraging blocking statutes.

B. Blocking Statutes

Suppose that an Internet company is incorporated in country *A*, but it operates worldwide. The company stores customer data in a handful of different countries, according to where customers happen to be, where storage is cheaper, and so on. Suppose also that country *A* has passed two laws: one that authorizes the government to seek warrants regarding customer data, regardless of the data's location; and one that prohibits technology companies from releasing data to other governments. Now suppose that country *B* passes the same two laws. This is what happens when countries pass a law like ECPA, which operates as both a shield and a sword.[250] It is a shield insofar as it prevents foreign governments from compelling data controlled by U.S. companies,[251] and a sword insofar as it forces companies to hand over data to the U.S. government in accordance with certain procedures.[252] The trick, as it were, is determining how one country's ECPA can play nicely with another's. Conflicts rules help. If courts can assert personal jurisdiction over a defendant, they can enforce a judgment against that defendant's assets, wherever they are located, unless doing so would lead to a gross violation of another country's laws.[253] This caveat ends up being important because a number of countries have passed so-called "blocking statutes," which are intentionally designed to prevent the production of evidence.[254]

Courts consider blocking statutes as part of their interest analysis, but relying on a blocking statute will not always help a litigant. In *Societe Internationale*, a Swiss holding company had an adequate excuse for not complying with an order to produce records where their production would

249. *See* Greg Nojeim, Ctr. for Democracy & Tech., MLAT Reform: A Straw Man Proposal (2015), https://cdt.org/files/2015/09/2015-09-03-MLAT-Reform-Post_Final-1.pdf.

250. *See* Kerr, *supra* note 206 (noting that the SCA, as part of ECPA, "acts as both a shield and a sword").

251. 18 U.S.C. § 2702(a)(3) (2014).

252. *Id.* § 2703(a)-(c).

253. *See* Simowitz, *supra* note 24, at 7 (noting that when a defendant's assets are located outside the jurisdiction but the court has personal jurisdiction over the defendant, "courts will generally restrain assets located elsewhere, unless the parties would be subjected to a substantial risk of double liability or the restraint would so egregiously violate foreign law that the asset would be rendered valueless").

254. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 reporters' note 4 (AM. LAW INST. 1987) ("Blocking statutes are designed to take advantage of the foreign government compulsion defense by prohibiting the disclosure, copying, inspection, or removal of documents located in the territory of the enacting state in compliance with orders of foreign authorities." (citation omitted)).

violate Swiss law, but the Supreme Court noted: "This is not to say that petitioner will profit through its inability to tender the records called for.... It may be that in the absence of complete disclosure by petitioner, the District Court would be justified in drawing inferences unfavorable to petitioner...."[255] Thirty years later, in *Société Nationale*, the Court held that a U.S. district court could compel a French company to produce documents related to an airplane accident despite the contention that doing so would violate a French blocking statute.[256] As the *Restatement* suggests, the case represents the view that when a court has prescriptive and adjudicatory jurisdiction, and blocking statutes frustrate the goal of enforcement, they "need not be given the same deference by courts of the United States as differences in substantive rules of law."[257]

This is instructive because the real challenge to the smooth functioning of conflicts principles as they apply to the cloud is not overlapping or conflicting jurisdictions, but rather the existence of blocking statutes and in particular—since the vast majority of the world's Internet users store their data with U.S. firms—the U.S. blocking statute, ECPA. American technology firms are prevented from releasing American-held content to foreign governments by the clear requirements of the SCA.[258] Interest analysis and other conflicts-of-laws rules will have little effect in this scenario, as long as the statute prevents U.S. data controllers from cooperating with foreign governments (or foreign judgments in conflicts cases). ECPA, therefore, must be reformed, and this should be done with conflicts principles in mind.[259]

This discussion hopefully shows that a number of conflicts principles give courts adequate tools to resolve jurisdictional disputes over data. Despite the multiple grounds states have for asserting jurisdiction over data, fears about overlapping and even conflicting jurisdictions are overblown. The real concern is not jurisdictions that conflict, or even substantively inconsistent laws, but rather blocking statutes that make it difficult for courts to find the appropriate equilibrium point between one state's interest in law enforcement and another state's interest in data privacy.

---

255. Societe Internationale pour Participations Industrielles et Commerciales, S.A. v. Rogers, 357 U.S. 197, 212-13 (1958).

256. Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court, 482 U.S. 522, 539-40, 544 n.29 (1987).

257. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 reporters' note 5.

258. 18 U.S.C. § 2702(a)(3) (2014).

259. *See infra* Part V.A.

V. Implications for Law and Policy

The preceding parts suggest that cloud data is not so conceptually different from other intangible assets, and that in any case, the distinction is one without a difference as a matter of enforcement jurisdiction: states have wide latitude to regulate their core interests—acts affecting their territory and their citizens—and courts have wide latitude to balance state interests when they conflict. But showing that cloud data is not conceptually novel does not resolve the very real jurisdictional puzzles raised by the cloud. So what should be done? The conflicts analysis above suggests that first, and perhaps most importantly, Congress should modify any blocking statutes that prevent U.S.-based Internet companies from cooperating with foreign law enforcement requests for data. This means that the United States should revise ECPA so that it no longer acts as a blocking statute, forcing all requests for data from U.S. companies through the MLAT process. Second, courts should interpret ECPA's territoriality requirements in light of the U.S. interest in cloud data—that is, by holding that Congress intended ECPA to apply to information stored by U.S.-based firms about U.S. persons—and balance competing state interests in cloud data accordingly. Third, the United States should revise its MLAT procedures and encourage other countries to do the same. Finally, the conflicts analysis above suggests that the United States should adopt a decentralized, state-by-state approach to state access to data in the cloud, rather than push for an international treaty forged out of pixie dust.

A. Reforming ECPA

As the conflict in the *Microsoft Corp.* case shows, Congress must reform ECPA to clarify its jurisdictional reach. But there is still the question of how to strike the right balance between U.S. governmental interests in the data and foreign governmental interests in that same data. That is, viewed from a conflicts perspective, what set of reforms is optimal? First, the foregoing suggests that a state's jurisdiction to regulate a particular piece of data flows from its legitimate interest in that data, so any jurisdictional test ought to reflect that fact. Second, in order to allow countries to enforce the law in cases that affect their interests, and in order for courts to adjudicate freely any jurisdictional disputes, ECPA must no longer act as a blocking statute. Specifically, ECPA should be reformed to allow U.S. companies to hand over to foreign governments their U.S.-stored electronic content when: (1) the data belongs to a non-U.S. citizen, (2) it is being requested in connection with a law enforcement or counterterrorism operation in which the state has a legitimate interest, and (3) an independent third party (e.g., a judge, magistrate, commission, etc.) has approved the request, (4) in reasonable accordance with shared standards of due process and human rights.

To be clear, the aim of these requirements is not to dictate as a normative matter how such requests for data ought to be processed, but rather to design the system to maximize appreciation of state interests and minimize conflicts. Consider each of these elements in turn. The first requirement turns on the nationality of the suspect whose data is being sought. It makes sense from a conflicts-of-laws perspective both that the British government has an interest in regulating the activity of its citizens, and that the American government has much less of an interest doing so. To be sure, the United States has an interest in regulating the global activities of American companies, but that can be done without impeding fair and just attempts to enforce local laws. Of course, the nationality of the suspect is not always clear to the Internet service provider, so they can refuse to cooperate if law enforcement is unable to determine the suspect's nationality.

Second, the requesting officers must be seeking the data as part of a criminal or counterterrorism investigation in which the state has a legitimate interest. The United States is well within its prescriptive jurisdiction to insist that technology companies headquartered in the United States only comply with another country's laws when those laws are legitimate; this is akin to Congress mandating that U.S. firms not accept bribes, even where doing so is legal or accepted practice.[260] U.S. interests in dictating the conduct of American firms should only be outweighed when there is some compelling countervailing foreign government interest. Accordingly, U.S. firms ought to be free to hand over data where the data is being requested by a state that has a meaningful interest in that data. This may mean that the state must show that the data relates to a crime that occurred or had significant effects on its soil, or involved one of its citizens. This codifies the conflicts principle that jurisdiction ought to track state interests.[261]

Third, when law enforcement agents attempt to gain access to private data, this request should be verified by an independent party—meaning someone outside of the direct line of command of the law enforcement agents requesting the data, whether that person is a judge, magistrate, or a commission. This is not a normative claim about due process but rather a conflicts point. Without this step, companies will be forced into the role of evaluating the urgency and legitimacy of law enforcement requests, which no one wants—not companies, not their users, and not law enforcement officials. Rather than delegate the evaluation of the legitimacy of each request to the legal and policy teams at U.S.

260. *See supra* text accompanying note 195.

261. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES pt. IV, ch. 1, intro. note ("Territoriality and nationality remain the principal bases of jurisdiction to prescribe, but in determining their meaning rigid concepts have been replaced by broader criteria embracing principles of reasonableness and fairness to accommodate overlapping or conflicting interests of states . . . .").

firms, that analysis should be done by an independent official in the requesting state. This gives firms a clear rule to apply around the world, rather than asking firms to evaluate requests on an ad hoc, country-by-country basis. This is not to say that company review should not play a role in these requests; to the contrary, it is absolutely critical, as outlined below. But companies should review to ensure that the request meets the process requirements laid out in ECPA and by local law, not determine the legitimacy of the request as a matter of law enforcement necessity.

Finally, requests should be required to meet minimum shared standards of due process and human rights. Under the current ECPA regime, foreign law enforcement officials must prove to a U.S. judge that they have probable cause (the Fourth Amendment standard) to obtain a warrant.[262] Solving the problem of American exceptionalism by requiring other countries to meet some other American standard seems to defeat the purpose of reform. Many countries have different due process standards in criminal investigations, and the rule should be flexible enough to allow for a wide range of state interests to be satisfied.[263] That is not to say that the U.S. legislature cannot have an interest in ensuring the quality of the standard used; of course they can.[264] But rather than articulate a standard in terms of American law, Congress could refer to a set of widely accepted due process norms, or otherwise allow countries to establish these norms on a mutually agreeable basis as part of a bilateral agreement. Of course, there is no settled set of clearly defined norms as to the precise requirements of criminal due process.[265] But Congress could refer to a set of principles derived from the larger "general principles of law recognized by

262. *See* 18 U.S.C. § 2703(a).

263. *See, e.g.*, Frederick F. Schauer, *English Natural Justice and American Due Process: An Analytical Comparison*, 18 WM. & MARY L. REV. 47 (1976) (describing the differences between British and American notions of due process, paying particular attention to the scope and reach of the protections); David E. Shipley, *Due Process Rights Before EU Agencies: The Rights of Defense*, 37 GA. J. INT'L & COMP. L. 1, 8-12 (2008) (describing the basic due process rights in the European Union and noting some of their differences from American law); Noriho Urabe, *Rule of Law and Due Process: A Comparative View of the United States and Japan*, 53 LAW & CONTEMP. PROBS. 61, 61-63 (1990) (describing the different meanings of rule of law and due process in Japan, the United States, the United Kingdom, and Germany).

264. Indeed, scholars and judges have been urging Congress to act on this matter. *See* Transcript of Oral Argument, *supra* note 12, at 99 (Judge Lynch noting that "it would be helpful if Congress would engage in that kind of nuanced regulation, and we'll all be holding our breaths for when they do"); Kerr, *supra* note 6, at 416.

265. *Cf.* Charles T. Kotuby Jr., *General Principles of Law, International Due Process, and the Modern Role of Private International Law*, 23 DUKE J. COMP. & INT'L L. 411, 412-13 (2013) (describing universal due process norms in broad terms).

civilized nations."[266] As the *Restatement* notes, there is some shared understanding of what constitutes "fair procedure."[267] Congress could refer to these broad and somewhat vague international principles, while articulating a floor on behavior based in human rights.[268]

This proposal has a number of benefits. First, it has the benefit of relying on international standards, rather than American ones, which should make it more palatable to foreign law enforcement. Second, it frees companies to comply directly with local law enforcement requests, reducing some of the pressure that law enforcement currently places on Internet companies, and reducing the likelihood that those agents will call for more surveillance or data localization. Third, it protects users from unwarranted intrusions into their privacy. Fourth, it does not put Internet companies in the position of making arbitrary determinations about when to comply with foreign government requests for data.

This proposal is distinct in important ways from other proposals for ECPA reform, all of which have serious drawbacks. For example, the LEADS Act, proposed by Senator Hatch, fixes some of the problems regarding U.S. government attempts to get data stored abroad—it would allow U.S. governments to access, via warrant, data about U.S. persons wherever it is stored—but the Act says nothing about foreign governments' ability to get access to that data, meaning that ECPA still acts as a blocking statute for foreign governments.[269] The ECPA Amendments Act, proposed by Senators Leahy and Lee, also does little to resolve the blocking statute problem.[270] Orin Kerr comes closer by suggesting that disclosure by Internet providers to foreign governments be voluntary—which would eliminate ECPA's blocking features—but without any guidelines about when companies ought to comply with foreign legal orders.[271] Without these guidelines, the bill would do nothing to promote the United States' interest in ensuring that American companies offer their non-U.S. users minimum privacy protections.

---

266. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102 reporters' note 1 (quoting Statute of the International Court of Justice art. 38(1)(c) (June 26, 1945)).

267. *Id.* § 102 cmt. b; *see also* BIN CHENG, GENERAL PRINCIPLES OF LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS 279 (1953) (describing the universal due process principle of *nemo debet esse judex in propria sua causa*, which prohibits someone from being the judge in her own case).

268. *See* WOODS, *supra* note 46, at 14.

269. *See* Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015).

270. The Act is focused narrowly on requiring a warrant for all digital content, where ECPA currently only requires a warrant for content stored for less than 180 days. *See* Electronic Communications Privacy Act Amendments Act of 2015, S. 356, 114th Cong. (2015).

271. Kerr, *supra* note 6, at 417-18.

One possibility is to create a club-like system, modeled on the Visa Waiver Program, where ECPA is reformed to suggest that only certain countries can have access to data stored in the United States by U.S. service providers.[272] However, such a proposal effectively creates a club of preselected countries who get access to data controlled by U.S. firms. A club model is less effective than a standards-based model like the one proposed here because it will unnecessarily anger the countries that are not included. Indeed, countries that do not have significant demands for access to data stored in the cloud may nonetheless take offense at being excluded from the club. Just as importantly, clubs inspire anti-clubs, as the International Telecommunication Union Internet governance debates demonstrated.[273] If Congress hopes to avoid those sorts of political clashes, it should avoid explicitly articulating winners and losers. The stakes are somewhat higher than those in the Visa Waiver Program. States that are excluded from that program can impose reciprocal visa burdens on Americans visiting them. But in the digital realm, the response by a state excluded from the club would be to demand data localization—imposing an enormous infrastructure cost on Internet businesses and likely reducing privacy protections.[274]

B. Interpreting ECPA

Before ECPA is revised, however, courts will have to resolve disputes regarding ECPA's reach. The foregoing conflicts analysis should suggest to a court that it has wide latitude to craft a resolution to such disputes. First, the court could decide that ECPA has no extraterritorial reach. The text of the statute says nothing about extraterritorial application, so the court could simply apply the presumption against extraterritorial application and decline to extend ECPA abroad.[275] Second, even if the court decides that ECPA has territorial limits, the court might create a test for locating the data that puts the data within ECPA's reach—by defining the test as the location of the server that was last accessed; the location of the user who last accessed the data; the

272. *See* Swire & Hemmings, *supra* note 100, at 33-37. For information on the Visa Waiver Program, see Bureau of Consular Affairs, *Visa Waiver Program*, U.S. DEP'T STATE, https://travel.state.gov/content/visas/en/visit/visa-waiver-program.html (last visited Apr. 4, 2016).

273. *See* Danielle Kehl et al., *Visualizing Swing States in the Global Internet Governance Debate*, NEW AM. WKLY.: OPEN TECH. INST. (Oct. 20, 2014), https://www.newamerica.org/oti/visualizing-swing-states-in-the-global-internet-governance-debate.

274. *See supra* text accompanying notes 111-14.

275. The presumption dates to *American Banana Co. v. United Fruit Co.*, 213 U.S. 347, 357 (1909), which describes the rule that if there is any doubt, courts construe "any statute as intended to be confined in its operation and effect to the territorial limits over which the lawmaker has general and legitimate power."

location of the user who first created the data; or any number of other tests. Third, and finally, regardless of what the court thinks about the territoriality of ECPA or the location of the data, the court should still balance competing state interests in regulating the data.

Under a conflicts approach to adjudicating competing state claims over access to data in the cloud, the state's legitimate interest in the data may matter more than the location of the data or the company. Kerr has argued that the court would only need to engage in a balancing of state interests if the court decides that the SCA does not apply to the data—presumably because the data is found to be extraterritorial—and the government could seek the data using a subpoena.[276] But it is unclear why a court would not also need to engage in the same balancing test even if it decided that the SCA applied. The court in *Microsoft Corp.*, for example, might find that the relevant test for territoriality under the SCA is where the company is headquartered—meaning that the SCA applies to Microsoft regardless of where it stores its data—but that would not stop the court from asking whether compelling a U.S. data controller to provide data that it stores abroad implicates the interests of foreign governments.

This insight relieves some of the pressure on the seemingly arbitrary choice of articulating a single test for where data is located for the purposes of the SCA. Given the morass of competing claims over how to define where data is located for jurisdictional purposes, and the potential incompatibility of different state laws, it may provide some relief to users to know that the jurisdiction over their data is the same across service providers, many of which have different terms of service regarding the location of their data, different corporate structures, and different data distribution models. The second effect is that courts will engage in a reciprocity analysis, just as they do in enforcement of foreign judgments. This could have the salutary effect of encouraging similar court behavior by fellow judges in other countries.

C. Improving Mutual Legal Assistance

Another implication of this analysis is that greater international cooperation is needed. Indeed, the U.S. government's position in the *Microsoft Corp.* case turns on the claim that requesting data from another jurisdiction via MLAT takes too long.[277] However the *Microsoft Corp.* case is decided, and regardless of how ECPA is reformed, foreign governments will have occasion to seek data that they are unable to compel and must ask for mutual legal assistance (MLA). If receiving states did a better job processing MLAT requests, it would relieve some of the pressure in the current system—pressure on

276. *See* Kerr, *supra* note 206.

277. *See* Brief for the United States of America, *supra* note 213, at 52-53.

companies to comply with local law enforcement requests and pressure on law enforcement to take drastic measures to get the data via other means.

There are a number of straightforward reforms that could be implemented without legislative action to greatly speed up the MLA process.[278] First, the MLA process should be standardized and made electronic. This means that requesting countries should use a single, standardized form that clarifies the legal standard that must be met, and this form should be transmitted electronically for faster processing.[279] Ideally, such a system would be developed by the DOJ and would include a tracking system so that the requesting officer and the Internet service provider could track the progress of the request as it travels through the MLA process. Second, the DOJ should institute additional training of foreign law enforcement officers so that when MLAT requests arrive at the DOJ, they are complete and meet the U.S. probable cause standard. Third, the DOJ critically needs more staff to handle incoming MLA requests—not only legal staff but also translators to assist when requests come in another language.[280] Fourth and finally, the OIA should take steps to increase the transparency of the MLA process. This should include issuing an annual report notifying the public of the number and nature of the requests that the office processed each year.[281] It would also include ensuring that Internet companies are aware that the warrants they receive are being served on behalf of a foreign government. This is critical because many major Internet companies now produce transparency reports and they necessarily record some requests from foreign governments as U.S. government requests because that is how they appear.[282]

D. The Case Against a Global Treaty

As more and more personal data is stored in the global cloud, and state jurisdiction over that data overlaps to a greater degree, how can states harmonize their laws so as to mitigate these conflicts? One approach would be to push for a broadly supported multilateral agreement.[283] Such an agreement is appealing for a number of reasons. First, a treaty could explicitly demarcate

278. *See* WOODS, *supra* note 46, at 14.

279. Unbelievably, many requests for mutual legal assistance are still made by paper and transmitted via diplomatic pouch. *See id.* at 8.

280. *See id.* at 10.

281. This is a welcome feature of the proposed Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015).

282. WOODS, *supra* note 46, at 11.

283. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 26, at 1210 (suggesting that Internet jurisdictional conflicts can theoretically, if not practically, be resolved by international agreements).

the jurisdictional limits of government access to cloud-based data. Second, the treaty could articulate the basis for dispute resolution in the event of jurisdictional conflict. Such uniformity in state policy would provide users, Internet companies, and law enforcement agents much-needed predictability about when governments can get access to Internet data.[284] Finally, an agreement could articulate a mechanism for government-to-government data sharing—where state *A* seeks access to data that the treaty deems to be properly under the authority of state *B*, the treaty could articulate a basis for the two states to share the data.[285]

But an international agreement of this sort is both practically unnecessary and normatively undesirable. It is unnecessary because conflicts-of-laws rules already provide a ready-made mechanism for navigating and settling jurisdictional disputes. As private international law scholars have shown, state-based conflicts-of-laws rules provide more flexibility and adaptability over time than a comparatively rigid and inflexible treaty regime.[286]

Perhaps more importantly, such an agreement would either be ineffective or dangerous. It is a dangerous proposition because in order to get a broad number of states to agree to an international treaty, that agreement will necessarily be based on a lowest common denominator, which would represent a significant threat to due process.[287] Alternatively, if the agreement begins with a small club of like-minded states with robust due process protections—as some have proposed[288]—it will be small and therefore do little to solve the hardest conflicts cases. A better approach would be to rely on a few simple conflicts principles.

Conclusion

In the end, data exceptionalists—those who argue that data challenges territorial conceptions of sovereignty and therefore cries out for a global treaty—have it wrong. Despite the cloud's seemingly magical qualities—

284. *See* WOODS, *supra* note 46, at 4-5 (describing the interests of various stakeholders implicated in MLAT reform).

285. *See id.* at 15-16.

286. *See* Riles, *supra* note 191, at 105-06 (characterizing the development of legal rules through conflicts of laws cases as a flexible and decentralized alternative to the comparatively rigid and centralized treaty process).

287. *See* Stephen J. Schulhofer, *An International Right to Privacy?: Be Careful What You Wish for* 15 (N.Y.U. Pub. Law & Legal Theory Working Papers, No. 508, 2015), http://lsr.nellco.org/cgi/viewcontent.cgi?article=1511&context=nyu_plltwp ("One obvious obstacle to a broad international agreement is the wide—probably unbridgeable—gulf between privacy commitments in the West and in many undemocratic governments.").

288. *See* Brown et al., *supra* note 20, at 34-35; *Time for an International Convention on Government Access to Data*, *supra* note 20.

location independence, lightning speed, interchangeability of data—these features are neither novel nor unique enough to support the data exceptionalist view. Courts have dealt with similar features in determining jurisdiction over a wide range of globally distributed and mobile assets, such as money, debts, and more. Moreover, regardless of the novelty of data's essential properties, age-old jurisdictional principles provide a solid foundation for countries to regulate people and property that affect national soil, and that often means compelling parties to produce evidence regardless of its location. Data will be no different. This fact will of course cause conflicts of laws. But transnational conflicts are not new; indeed, courts have a set of tools precisely designed to address and mitigate such conflicts.

A more grounded and realistic analysis of the jurisdictional questions raised by the global cloud is a sensible starting place for considering reforms. Rather than declaring that data is entirely novel and therefore calls for sweeping and novel solutions, reformers should attempt to regulate the global cloud mindful of the jurisdictional principles that undergird each state's authority. Rather than attempt to wipe away all potential conflicts of laws with a wishful global treaty, for example, a more realistic and productive reform strategy would be to seek to remove existing obstacles to the smooth functioning of conflicts rules so that countries can regulate their interests, and courts can adjudicate disputes as they arise. The most pressing of these reforms is not to prevent states from asserting extraterritorial jurisdiction over data, as many have suggested; rather, it is to remove blocking statutes where they prevent global Internet companies from complying with local law. For the United States, where most of the world's biggest Internet companies are based, this means revising ECPA, and doing so in a way that balances foreign state interests in American-controlled data with the U.S. interest in ensuring that American companies do not violate American values.

*