THE YALE LAW JOURNAL

ANDREW KEANE WOODS

Litigating Data Sovereignty

ABSTRACT. Because the internet is so thoroughly global, nearly every aspect of internet governance has an extraterritorial effect. This is evident in a number of high-profile cases that cover a wide range of subjects, including law enforcement access to digital evidence; speech disputes, such as requests to remove offensive or hateful web content; intellectual property disputes; and much more. Although substantively distinct, these issues present courts with the same jurisdictional challenge: how to ensure one state's sovereign interest in regulating the internet's local effects without infringing on other states' interests.

The answer, for better or for worse, is comity, the foreign affairs principle that informs a number of sovereign-deference doctrines. Sovereignty arguments have pervaded a number of recent consequential cases, including Google's challenge to the "right to be forgotten" in Europe and Microsoft's challenge to a court order to produce foreign-held emails under the Electronic Communications Privacy Act. These arguments will continue to play a significant role in future cases. Yet the proper application of foreign affairs law to cross-border internet disputes is not what many litigants and courts have claimed. Crucially, no sovereign-deference doctrine prohibits global takedown requests, foreign production orders, or other forms of extraterritorial exercises of jurisdiction over the internet. To the contrary, one of the key lessons of the sovereign-deference jurisprudence is that in order to avoid tensions between sovereigns, courts often enable, rather than inhibit, extraterritorial exercises of authority.

This Article has three goals. First, it seeks to identify and characterize an emerging body of case law, which we might call data-sovereignty litigation: a diverse set of cases pitting national sovereigns against large internet firms. Second, the Article aims to show how the doctrinal rules of sovereign deference ought to apply to these disputes. Finally, it makes the case for a policy of sovereign deference beyond courts. The stakes are considerable. If we do not find ways to accommodate legitimate sovereign claims over global cloud activity, states will forcefully assert those interests—typically by taking physical control over local network infrastructure—imposing significant costs on entrepreneurship, privacy, and speech.

AUTHOR. Associate Professor, University of Arizona College of Law. The author thanks Bill Dodge, Graeme Dinwoodie, Jack Goldsmith, Carlos Vazquez, Kristen Eichensehr, Maggie Gardner, Ingrid Wuerth, Albertina Antognini, Ben Wittes, Jennifer Daskal, Shalev Roisman, Matthew Perault, Alan Rozenshtein, Orin Kerr, Rick Salgado, Chris Bradley, Greg Nojeim, Nathaniel Jones, Alex Abdo, as well as the policy and legal teams at Google, Facebook, Twitter, Microsoft, Yahoo!, the Global Network Initiative, the ACLU, the Center for Democracy and Technology, and the Electronic Frontier Foundation. Thanks also to the editors of the *Yale Law Journal*, most especially Ali Cooper-Ponte, whose insights improved the Article considerably. The Article benefited from conferences and workshops at Stanford Law School, Vanderbilt Law School, Yale Law School, Florida State University, the University of Arizona, the University of Texas, the Department of Justice, the Hoover Institution, as well as the Yale/Stanford/Harvard Junior Faculty Forum and the American Society of International Law Domestic Courts Workshop. Much of this Article was written while the author was a Senior Cybersecurity Fellow and Visiting Professor at the University of Texas School of Law, and he owes a special debt to his students in the Tech Policy seminar there.

ARTICLE CONTENTS

INTRODUCTION

The key questions of internet global governance—including which nations get to determine how internet services operate globally—are being resolved by courts. A number of high-stakes cases ask courts to identify foreign sovereign interests, weigh them against domestic interests, and defer to foreign sovereigns where appropriate.[1] Consider a few recent examples:

1. On February 27, 2018, the United States Supreme Court heard oral argument in Microsoft's long-running dispute with the Department of Justice (DOJ) over the territorial reach of the Electronic Communications Privacy Act (ECPA).[2] In its petition for certiorari, the DOJ asked the Court to overturn the Second Circuit's ruling that ECPA does not apply extraterritorially—a ruling that prevented American law enforcement from compelling technology companies to produce emails stored on foreign datacenters.[3] The petitioner urged the Court to allow ECPA's production orders to compel the production of foreign-held emails,[4] a view that Microsoft argued would be an incursion upon Irish sovereignty.[5] The case raised questions, Microsoft noted, about "the sovereignty of data."[6]
2. On July 27, 2017, Google asked the U.S. District Court for the Northern District of California for declaratory relief from a Canadian court order that required Google to remove certain websites from its search results. The order sought to change Google's search results not just in Canada but also globally.[7] The issue, Google said, is one of "international comity"[8] because the "Canadian Order purports to place the Canadian court

1. These disputes ask courts to answer Lawrence Lessig's old but still unresolved question: "[W]hat kinds of claims should one sovereign be able to make on others, and what kinds of claims can these sovereigns make on cyberspace?" LAWRENCE LESSIG, CODE 302 (2d ed. 2006).
2. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam).
3. Petition for a Writ of Certiorari at 2-3, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2).
4. *Id.* at 21-25.
5. Transcript of Oral Argument at 51, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2).
6. *Id.* at 60.
7. Complaint at 2, Google Inc. v. Equustek Sols. Inc., No. 5:17-cv-04207-NC (N.D. Cal. July 24, 2017).
8. *Id.* at 3.

in the position of supervising the law enforcement activities of a foreign sovereign nation (the United States)."[9]

3. On July 19, 2017, France's top administrative court, the Conseil d'État, referred a case to the European Court of Justice for the European Union regarding Google's refusal to comply with an order that the firm apply its right-to-be-forgotten regime not only within Europe, but worldwide.[10] Google stated that it is fighting the order because "one country should not have the right to impose its rules on the citizens of other countries."[11]

Despite their substantive differences, each of these cases presents a court with a similar set of jurisdictional line-drawing questions. What is the scope of sovereign authority over the cloud?[12] Are extraterritorial exercises of jurisdiction lawful? How much deference is owed to foreign sovereign interests in regulating internet activity? How should courts weigh competing claims of sovereign authority? In other words, each of these disputes implicates the subset of foreign affairs law known as comity.[13] Comity is the principle that courts should recognize and sometimes defer to foreign sovereign interests. This principle has been

---

9. *Id.* at 12. Google won a default judgment on the grounds that the Canadian order violates Section 230 of the Communications Decency Act. *Equustek*, 2017 U.S. Dist. LEXIS 206818, at *1, *3.

10. Mark Scott, *French Court Refers Google Privacy Case to ECJ*, POLITICO (Jan. 28, 2018, 10:12 PM CET), https://www.politico.eu/article/french-court-refers-google-privacy-case-to-ecj [https://perma.cc/TH2P-GFRN].

11. Kent Walker, *A Principle that Should Not Be Forgotten*, GOOGLE (May 19, 2016), https://www.blog.google/topics/google-europe/a-principle-that-should-not-be-forgotten [https://perma.cc/D3UY-665Q].

12. The Article will refer to the cloud and the internet as interchangeable, since so many of the dominant internet services and applications today use a cloud-based model of distributed data and software. *See* PETER MELL & TIMOTHY GRANCE, U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011) (providing the most widely cited definition of cloud computing); *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."). This Article refers to data as digital information capable of being uploaded and shared on the internet.

13. As the Supreme Court wrote more than a hundred years ago:

> "Comity," in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial

incorporated into American law in a number of different sovereign-deference doctrines.[14] How, then, do these doctrines apply to cross-border internet disputes?

This Article offers a roadmap for answering this question. Despite the novelty of the underlying technologies involved in these cases, the doctrinal challenges are not so new. Courts have long resolved cross-border legal controversies by applying sovereign-deference principles, and in that regard today's data sovereignty disputes are no different. A study of these principles reveals that courts have a suite of tools at their disposal to manage data sovereignty concerns and in so doing craft sensible global internet policy. The Article examines both how these sovereign-deference doctrines might apply to data sovereignty disputes[15] and how they might not apply.[16] Contrary to what some have claimed, these doctrines anticipate that sovereign interests extend beyond territorial borders.[17] In several high-profile internet disputes, large technology firms and some states

> acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws.

Hilton v. Guyot, 159 U.S. 113, 163-64 (1895). Comity is "a sort of intercourt diplomacy long assumed to be within courts' constitutional competence." Pamela K. Bookman, *Litigation Isolationism*, 67 STAN. L. REV. 1081, 1096 (2015).

14. Scholars use the phrase "comity doctrines" and "sovereign-deference doctrines" interchangeably, and often as a subset of "foreign relations doctrines" and "international relations doctrines." Eric Posner and Cass Sunstein, for example, speak interchangeably about "foreign relations law" and "international relations doctrines," which they divide into "comity doctrines" and "anti-comity doctrines." Eric A. Posner & Cass R. Sunstein, *Chevronizing Foreign Relations Law*, 116 YALE L.J. 1170, 1173-81 (2007). As William Dodge notes, comity is "deference to foreign government actors that is not required by international law but is incorporated in domestic law." William S. Dodge, *International Comity in American Law*, 115 COLUM. L. REV. 2071, 2078 (2015) (emphasis omitted). Comity, along with other foreign affairs doctrines, was incorporated into American law long ago. *See* CURTIS BRADLEY & JACK GOLDSMITH, FOREIGN RELATIONS LAW 4 (6th ed. 2017) ("An understanding of history is . . . particularly useful when studying foreign relations law. The Constitution was written against the background of, and was designed in part to redress, concrete foreign relations problems that arose in the preconstitutional period.").

15. I focus on American foreign affairs doctrines — not the international legal doctrines — because although some of these issues will first be litigated in foreign courts, they will ultimately end up before an American judge who must decide whether to enforce the foreign judgment against the world's leading internet companies, most of which are American. For a summary of the reach of American firms across the global internet, see Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 287-88 (2015); and see also Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 741 (2016), which cites evidence that the world's most popular internet services are American.

16. *See infra* Part IV.

17. *See id.*

have argued that sovereignty concerns prohibit extraterritorial exercises of jurisdiction.[18] However, no principle of sovereign deference per se prohibits global injunctions, global takedown requests, or other forms of extraterritorial exercises of jurisdiction over the cloud.[19] Instead, comity principles sometimes call for deference to and even enforcement of cross-border legal orders.[20] Ultimately, the Article offers a defense of two controversial positions: (1) that efforts by national sovereigns to regulate the internet in ways that have extraterritorial effects are inevitable; and (2) that courts are well equipped to manage disputes where conflicts arise.

In earlier work, which focused on law enforcement access to data in other jurisdictions, I argued that courts should rely on a relatively simple conflicts-of-laws principle: they should balance competing governments' interests against one another.[21] This Article builds on that idea by clarifying the meaning of "government interest" in the context of the frequently invoked sovereignty doctrines, and by looking beyond the law enforcement context to the cross-border regulation of the internet more generally.

In doing so, the Article connects two distinct scholarly literatures: scholarship about the regulation of data and scholarship about foreign affairs. Reading these literatures together makes good sense today for two reasons. First, scholars of data regulation are increasingly concerned with sovereignty, which has long been a central focus of foreign affairs scholarship. While sovereignty concerns

---

18. *See, e.g.*, Brief for Respondent at 57, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam) (No. 17-2) ("Such a projection of U.S. law-enforcement power into foreign countries would trammel their sovereignty and threaten to disrupt harmony among nations . . . ."); Brief in Support of Appellant Microsoft, Inc. by Apple Inc. as Amicus Curiae at 10-14, Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016) (No. 14-2985-cv) (arguing that the case raises novel comity concerns); Brief of Amicus Curiae Ireland, *Microsoft*, 829 F.3d 197 (No. 14-2985-cv) (relying on arguments of comity and respect for foreign sovereignty); Factum of the Intervener the Attorney General of Canada at 3-4, Google Inc. v. Equustek Sols. Inc., [2017] 1 S.C.R. 824 (Can.) (No. 36602) ("Applying Canadian law in another state without its consent amounts to the impermissible exercise of extraterritorial enforcement jurisdiction, which is precluded by the principles of sovereignty, non-intervention and comity."); Application Record of the Applicant, Google Inc. at 120, *Equustek*, [2017] 1 S.C.R. 824 (No. 36602) (arguing that comity counsels against using Canadian courts to "directly command a person outside of Canada who has committed no civil wrong in Canada to do something, or risk being punished for contempt of the Canadian court").

19. *See infra* Part IV.

20. *Id.*

21. Woods, *supra* note 15, at 776.

arose in even the earliest internet scholarship, they have new significance today.[22] Many of the early internet-jurisdiction cases dealt with relatively simple scenarios—such as when someone in State A posts something online that violates the law in State B[23]—that do not match the scale or complexity of, say, the European Union regulating speech rules for a two-billion-user platform like Facebook.[24] The power dynamics were different then as well. When Yahoo! battled with France over a decade ago, in one of the early data sovereignty cases, Yahoo! was a relatively small company.[25] By contrast, today's data sovereignty disputes pit the world's most valuable companies against nation-states. Indeed, in their extreme form, they pit alliances of powerful companies against alliances of nations.[26] This new power dynamic is precisely what has caused some scholars to worry—wrongly, in my view[27]—that states have ceded sovereignty to large technology firms.[28]

---

22. *See* JAMES GRIMMELMANN, INTERNET LAW 51-63 (7th ed. 2017) (describing the early internet-jurisdiction disputes and noting that all internet issues are at some level jurisdictional).

23. *See id.*

24. *See* Daniel Boffey, *EU Threatens to Crack Down on Facebook over Hate Speech*, GUARDIAN (Apr. 11, 2018, 5:18 PM), https://www.theguardian.com/technology/2018/apr/11/eu-heavy-sanctions-online-hate-speech-facebook-scandal [https://perma.cc/6SC9-NEYM].

25. Yahoo!'s legal battle with France ended in 2006. Yahoo! Inc. v. La Ligue Contre Le Racisme Et l'Antisemitisme, 433 F.3d 1199 (9th Cir. 2006). At the time, the firm was rapidly losing market share to Google. *See* Fred Vogelstein, *How Yahoo Blew It*, WIRED (Feb. 1, 2007, 12:00 PM), https://www.wired.com/2007/02/yahoo-3 [https://perma.cc/5Z7Q-TMDF]. Google is valued today at $600 billion, and there is talk that it will soon be worth $1 trillion. Anita Balakrishnan, *Amazon, Apple, and Alphabet Are in a Race to Become the First Trillion-Dollar Company - Munster*, CNBC (Apr. 21, 2017, 5:57 PM), https://www.cnbc.com/2017/04/21/gene-munster-the-1-trillion-market-cap-chances-for-amazon-apple-or-google.html [https://perma.cc/Q2NG-Y7VS].

26. For example, the European Union has taken on the social media industry as a whole on a number of issues. *See infra* Section I.A.1.

27. *See infra* Section II.A.

28. *See* Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 182 (2018) ("The multinational companies that manage our data have taken on a form of international governance in ways that traditional governments can't and won't."); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 365 (2015) (describing the longstanding view that the "unilateral exercise of law enforcement in another state's territory is a breach of that state's sovereignty" and noting that "data is beginning to challenge this established understanding"); Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 325 n.30 (2015) (describing the "weakness or absence [of national sovereignty] in the current cyberspace context"); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 187 (2018) ("[I]nternet companies challenge the state's monopoly over security, the very locus of traditional conceptions of sovereignty."); *Digital Security and Due Process: Modernizing Cross-Border Surveillance Law for the Cloud Era* (June 22, 2017), https://www.heritage.org/technology/event/digital-security-and-due-process-modernizing-cross-border-surveillance-law-the (describing the rise of cyberspace

Second, reading these literatures together reveals a shared concern over institutional competence. Scholars writing about the regulation of new technologies have engaged in a decades-long debate about the proper role of courts as creators of technology policy.[29] Some argue that courts should exercise special restraint in areas of fast-changing technology policy because they are less well suited to developing technology policy than the other branches of government.[30] Others disagree, arguing that technology policy is not so exceptional and that courts offer certain advantages over the other branches.[31] This exchange echoes similar debates about the role of courts in foreign affairs.[32] There is a growing body of scholarship that describes how courts engage in forms of isolationism,[33]

---

as "perhaps the most transformative issue since the fall of the Berlin Wall back in the 1980s in terms of how it is reordering society," because unlike nation states, "characterized by borders, by exercising jurisdiction and law in particular places," we now live in "a different kind of reality, a reality of information space, this network that has no inherent borders, bears no inherent jurisdiction"). These claims are modern incarnations of much older arguments. For the most well-known argument of this sort, see John Perry Barlow, *A Declaration of the Independence of Cyberspace* (1996), https://www.eff.org/cyberspace-independence [https://perma.cc/G2S3-5L99], which argues that cyberspace is ungovernable by nation-states. For a related view, see David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1400-01 (1996), which argues that cyberspace is its own domain, deserving of its own rules, different from those that apply on any particular sovereign soil; and see also Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1202-05 (1998), which responds to Johnson and Post.

29. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004) (arguing that courts are ill-equipped to make criminal law in areas where technology is fast evolving). For responses to Kerr's institutional-competence argument, see Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 498 (2013), which argues that courts and legislatures are not an either/or proposition, but rather can work together to achieve optimal policy; David Alan Sklansky, *Two More Ways Not to Think about Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 224-33 (2015), which disputes Kerr's view that privacy protections are best left to the political branches and questions whether the institutional comparison is fruitful; and Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 761-74 (2005), which argues that the legislative record in addressing new technologies is insufficient, filled with gaps, and suggests that legislatures are neither as nimble nor as informed as Kerr suggests.

30. *See generally* Kerr, *supra* note 29.

31. *See generally* Solove, *supra* note 29.

32. Much of this literature is focused on the procedural doctrines courts use to avoid cross-border litigation. *See, e.g.*, Bookman, *supra* note 13, at 1085 (summarizing the litigation isolationism literature).

33. *See* Donald Earl Childress III, *Escaping Federal Law in Transnational Cases: The Brave New World of Transnational Litigation*, 93 N.C. L. REV. 995 (2015) (exploring the doctrines federal courts use to avoid resolving transnational disputes); Maggie Gardner, *Parochial Procedure*, 69

while others argue that judicial management of foreign relations is more common and less exceptional than previously thought.[34] Whether these developments are cause for celebration or cause for concern depends on one's views about the appropriate role for courts in foreign affairs,[35] perhaps the central normative question among foreign affairs scholars.[36]

These two literatures converge in the data-sovereignty cases. One might view the cases as *especially* ill-suited for courts because they require courts to set technology policy for the global internet. And yet, these cases continue to test both our foreign affairs doctrines and the judiciary's ability to manage new areas of technology policy. We may need to look to other actors besides courts to manage these disputes, and we may also learn something new about the appropriate relationship between the judiciary and other branches in managing both foreign affairs and technology policy.[37]

The Article proceeds as follows. Part I examines several high-profile internet-governance cases and identifies some of their shared features. The resolution of each of these issues defines, often for the first time, the limits of state control over the internet. Because the phrase "sovereignty" is so notoriously broad, Part II offers a specific articulation of what that concept might mean in the context of the internet. This Part interrogates the idea that state sovereignty is diminished

---

STAN L. REV. 941, 954-56 (2017) (summarizing the literature critical of courts' increasingly narrow approach to transnational cases); David L. Noll, *The New Conflicts Law*, 2 STAN. J. COMPLEX LITIG. 41, 82-84 (2014) (arguing that courts are defining their jurisdictional authority narrowly to avoid hearing transnational cases); Cassandra Burke Robertson, *Transnational Litigation and Institutional Choice*, 51 B.C. L. REV. 1081, 1113 (2010) (describing courts' use of court-access doctrines to avoid hearing transnational disputes); Christopher A. Whytock, *The Evolving Forum Shopping System*, 96 CORNELL L. REV. 481, 483-84 (2011) (presenting empirical evidence that while transnational litigation has grown over the last two decades, federal courts have become more reluctant to hear transnational cases).

34. *See* Zachary D. Clopton, *Judging Foreign States*, 94 WASH. U. L. REV. 1 (2016) (debunking the myth that courts avoid judging foreign sovereigns' actions); Ganesh Sitaraman & Ingrid Wuerth, *The Normalization of Foreign Relations Law*, 128 HARV. L. REV. 1897 (2015) (showing that courts no longer treat foreign relations cases so differently from domestic cases).

35. *Compare* Posner & Sunstein, *supra* note 14, at 1198, *with* Dodge, *supra* note 14, at 2132.

36. *See* Curtis A. Bradley, Chevron *Deference and Foreign Affairs*, 86 VA. L. REV. 649, 694 (2000); Zachary D. Clopton, *Replacing the Presumption Against Extraterritoriality*, 94 B.U. L. REV. 1, 40 (2014) (arguing that *Chevron* deference is an appropriate way to manage ambiguity about extraterritorial jurisdiction); Dodge, *supra* note 14, at 2132 ("A second myth of international comity is the notion that the executive branch enjoys a comparative advantage in making comity determinations."); Posner & Sunstein, *supra* note 14, at 1207 ("[T]he expertise rationale for deference to the executive is stronger in the foreign relations setting than in the traditional *Chevron* setting.").

37. *See infra* Part V.

in the internet era, and suggests that policymakers face a stark choice—not between an open internet and the "splinternet," but between better and worse forms of a fragmented internet.[38] Do we prefer a world where courts apply comity principles, recognizing and deferring to foreign sovereign interests where appropriate, or a world where they decline to do so and tempt states to assert their sovereign power forcefully? The answer is clearly the former.

The final three Parts turn to the sovereign-deference doctrines themselves and their judicial application. Part III introduces these doctrines as a way for courts to manage competing and overlapping claims of sovereignty over the internet. Part IV clarifies what those doctrines *do not* require. Most importantly, the Part shows that comity neither requires nor even exhibits a consistent bias against extraterritoriality. To the contrary, when the litigated dispute is transnational, comity often calls for *accommodating* another sovereign's extraterritorial regulations. That is, comity promotes recognition at least as much as it does restraint. Part V turns to institutional questions and offers an assessment—and a limited defense—of courts as internet policy makers. The Part concludes by looking beyond courts to ask what a broad policy of sovereign deference might mean for other key actors in internet governance debates.

I. THE DATA-SOVEREIGNTY DISPUTES

There are a number of flashpoint issues that implicate the state's sovereign authority over the cross-border internet. This Part surveys some of the high-profile disputes, and it identifies some of their shared characteristics. The particular substantive disputes in each case are not as important as the overall picture that emerges: across a number of different issues and jurisdictions, states and some of the world's most powerful companies are regularly clashing in litigation that asks courts to identify the limits of state sovereignty over the internet.

38. The "splinternet" is the idea that the internet may be carved up in the image of nation-states. SCOTT MALCOMSON, SPLINTERNET: HOW GEOPOLITICS AND COMMERCE ARE FRAGMENTING THE WORLD WIDE WEB 7 (2016).

A. The Issues

1. Takedown Orders for Extremist Content

States routinely demand that internet service providers remove content—such as a website or photos—because the content violates local law.[39] In particular, governments have placed internet firms under increased pressure to take responsibility for extremist content that users post on their platforms.[40] In June 2017, several of the biggest internet companies—Facebook, Microsoft, Twitter, and Google—formed an industry alliance to coordinate their efforts to identify and remove extremist content from their platforms.[41] This was the latest in a series of industry actions aimed at satisfying European regulators who have pushed for more censorship of extremist content by internet intermediaries.[42] This pressure intensified following the terrorist attacks in Paris and Brussels in 2015.[43] In response to those attacks, technology companies implemented a code of conduct under which they agreed to remove extremist and hateful content within twenty-four hours.[44] However, the firms' efforts did not satisfy European regulators.[45] In the United Kingdom, the Home Affairs Select Committee produced a report slamming the companies for failing to do more.[46] The rhetoric

39. *See* GRIMMELMANN, *supra* note 22, at 119-213 (collecting cases regarding censorship over internet content).

40. *See* Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1040-49 (2018).

41. Selena Larson, *Tech Giants Bolster Collaborative Fight Against Terrorism*, CNN MONEY (June 26, 2017, 2:47 PM EDT), https://money.cnn.com/2017/06/26/technology/business/global-Internet-forum-to-counter-terrorism/index.html [https://perma.cc/U3G4-J8DY].

42. For a summary of these developments, see Citron, *supra* note 40.

43. *See, e.g.*, Mark Scott, *Europe Presses American Tech Companies to Tackle Hate Speech*, N.Y. TIMES (Dec. 7, 2016), https://www.nytimes.com/2016/12/06/technology/europe-hate-speech-facebook-google-twitter.html [https://perma.cc/X8LU-HFPB]; Amar Toor, *UK Lawmakers Say Facebook, Google, and Twitter Are 'Consciously Failing' to Fight ISIS Online*, VERGE (Aug. 26, 2016 5:58 AM EDT), https://www.theverge.com/2016/8/26/12656328/facebook-google-twitter-isis-propaganda-uk-report [https://perma.cc/KK7T-RLDF].

44. *Code of Conduct on Countering Illegal Hate Speech Online*, EUR. COMMISSION (2016), https://edri.org/files/privatisedenf/euhatespeechcodeofconduct_20160531.pdf [https://perma.cc/9MFT-ZQW8].

45. *See* Amar Toor, *Germany Passes Controversial Law to Fine Facebook over Hate Speech*, VERGE (June 30, 2017, 4:18 AM EDT), https://www.theverge.com/2017/6/30/15898386/germany-facebook-hate-speech-law-passed [https://perma.cc/WT2D-YW7T].

46. *UK Lawmakers Criticize Social Media over Response to Extremist Content*, REUTERS (Apr. 30, 2017, 7:04 PM), https://www.reuters.com/article/us-britain-socialmedia-idUSKBN17W0U1 [https://perma.cc/6UE8-NZPH].

was far from measured, with the chairwoman of the Committee saying publicly: "Social media companies' failure to deal with illegal and dangerous material online is a disgrace."[47]

American efforts to regulate American social media firms have not been as successful as these European regulatory efforts.[48] In the United States, proposals to force internet companies to moderate offensive or dangerous content have stalled, hindered by the First Amendment and the Communications Decency Act.[49] The recent triumphs of European regulators also contrast with the first round of internet-jurisdiction disputes, many of which centered around hate speech regulations permissible in Europe but not in the United States.[50] In those disputes, technology firms resisted cross-border takedown requests and often won. Today, firms bow to pressures in one market to remove certain content, and the consequences are felt around the world. Facebook's "Community Standards"—which govern what content can stay up or must come down—apply globally, "without differentiation to cultural or national boundaries."[51] Because the takedowns apply worldwide, scholars and activists have expressed concern about one sovereign having the ability to set internet speech policy internationally.[52]

2. *Delisting and the Right to Be Forgotten*

Sometimes, rather than ordering a provider to remove content from its own website, states ask the provider to stop *linking* to or *directing* users to content hosted elsewhere, including by removing links to this content from search results. These delisting requests—typically lodged against search engines like Google—are mostly used to force companies to remove links in accordance with

47. *Id.*

48. *See* Citron, *supra* note 40, at 1037-38.

49. 47 U.S.C. § 230 (2018). For a discussion of both, see Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435, 1453 nn.110 & 111 (2011); and Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Defying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 406-07 (2017).

50. *See, e.g.*, Yahoo!, Inc. v. La Ligue Contre Le Racisme Et l'Antisemitisme, 169 F. Supp. 2d 1181, 1194 (N.D. Cal. 2001) (finding that enforcing a French judgment that would require Yahoo! to make geolocation changes to its technology in California violated the First Amendment and was therefore unenforceable).

51. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1642 (2018).

52. *See* Citron, *supra* note 40, at 1056.

the so-called right to be forgotten.[53] Since the European Court of Justice acknowledged this right, Google has taken down links to nearly a million websites,[54] while continuing to challenge similar delisting orders around the world.[55]

Foremost among these challenges to delisting orders is Google's litigation in Spain, where the data protection authority, Agencia Española de Protección de Datos (AEPD), ordered Google to remove material at a user's request.[56] Google's local and international offices sought clarification from Audiencia Nacional, Spain's highest court,[57] which then sought clarification from the European Union Court of Justice (CJEU) on the European Data Protection Directive.[58] The CJEU sidestepped the question of whether the European Union's Data Protection Directive guarantees a fundamental right to be forgotten,[59] but it found that Google is a data "controller" within Spanish territory for the purposes of determining the state's personal jurisdiction over Google.[60] This meant that the AEDP's order applied to Google. The court left open the question of how far the ruling reached on the internet—whether just to Spanish domains, to users with

53. Alan Travis & Charles Arthur, *EU Court Backs 'Right to be Forgotten': Google Must Amend Results on Request*, GUARDIAN (May 13, 2014), https://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results [https://perma.cc/M8G5-DDRB] (describing how EU data protection laws force search engines like Google to remove private information at the request of users).

54. *Search Removals Under European Privacy Law*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/eu-privacy/overview (showing that from May 29, 2014 to August 5, 2018, Google has received requests to delist 2,300,526 websites, and has agreed to delist 1,010,276 of those websites).

55. In addition to Google's disputes with Spanish and French authorities, the firm has also fought the right to be forgotten in Argentina, Japan, and other countries. *See* Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 989-90 (2018); *see also* Farhad Manjoo, '*Right to be Forgotten' Online Could Spread*, N.Y. TIMES (Aug. 5, 2015), https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html [https://perma.cc/6CHR-NSMD] (discussing how the European Court of Justice's decision could reverberate throughout the world).

56. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 [https://perma.cc/Q694-URG7].

57. *Id.* ¶ 1.

58. *Id.* ¶¶ 19-20.

59. *Id.* ¶¶ 89-99.

60. *Id.* ¶¶ 32-41, 43, 45, 50, 57, 60.

Spanish IP addresses, or perhaps to users globally.[61] Google convened an advisory committee to discuss how to implement the ruling.[62] The committee's report concluded that Google should remove offending content from the relevant country-level domain—in this case, www.google.es—but not from www.google.com, even for users located within Spain.[63] In response, European authorities signaled to Google that it would need to delist offending material worldwide.[64]

This set up the company's dispute with France's data-protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL).[65] In France, Google complied with delisting requests by removing offending material from the country-level domain, google.fr.[66] After Google concluded that it had the technology to identify user location, it also delisted search results for users that appeared to be in France.[67] The CNIL concluded that this was insufficient, determining that Google must delist offending material not just on all Google products within the EU, but also on all Google products wherever they are accessed worldwide.[68] Google rejected this argument and appealed to the Conseil d'État, France's highest court for administrative justice.[69] That court in turn referred the case to the European Court of Justice, where the case is pending.[70]

Delisting orders can also be used to ask firms to stop linking to content that violates intellectual property rules.[71] For example, on June 27, 2017, the Canadian

---

61. *Id.*

62. *See Advisory Council to Google on the Right to Be Forgotten*, GOOGLE (Feb. 6, 2015), https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf [https://perma.cc/WP8K-DEB2].

63. *Id.*

64. Natasha Lomas, *Google Faces Fight in Europe on Search Delisting*, TECHCRUNCH (Feb. 6, 2015), https://techcrunch.com/2015/02/06/google-rtbf-report [https://perma.cc/CCQ3-D5KW].

65. *CNIL Orders Google to Apply Delisting on All Domain Names of the Search Engine*, CNIL (June 12, 2015), https://www.cnil.fr/fr/node/15790 [https://perma.cc/Z92U-8SJE].

66. Walker, *supra* note 11.

67. *Id.*

68. *See* Julia Fioretti, *France Fines Google over 'Right to Be Forgotten,'* REUTERS (Mar. 24, 2016, 12:38 PM), https://www.reuters.com/article/us-google-france-privacy/france-fines-google-over-right-to-be-forgotten-idUSKCN0WQ1WX [https://perma.cc/YD76-KHUA].

69. Walker, *supra* note 11.

70. CE Sect., July 19, 2017, 399922 (Fr.), http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC [https://perma.cc/XT3J-R79G].

71. Joe Mullin, *Google Must Alter Worldwide Search Results, Per Orders from Canada's Top Court*, ARS TECHNICA (June 28, 2017, 3:30 PM), https://arstechnica.com/tech-policy/2017/06

Supreme Court held that Google must delist web pages relating to Datalink, a firm accused of violating Canadian intellectual property law.[72] The Supreme Court upheld the order of the Court of Appeal for British Columbia, which had demanded that Google remove references to pages selling Datalink's wares not only on Google's Canadian site, google.ca, but also on all Google websites.[73] The order applied to Google's products anywhere in the world.[74] Google appealed the lower court's order, arguing that the takedown request represented an invalid exercise of extraterritorial jurisdiction.[75] The Canadian Supreme Court disagreed by a seven-to-two vote, and held that the order was appropriate in scope.[76]

Google did not take issue with the intellectual property dispute between Equustek and Datalink.[77] Nor was Google averse to fashioning a remedy,[78] proposing to remove the offending links from its Canadian domain, google.ca.[79] Rather, Google expressed concern about the global reach of the injunction, which it argued set a dangerous precedent for other countries.[80] A number of civil-society groups also weighed in, filing amicus curiae briefs in support of Google's position and arguing that a worldwide injunction both violated U.S. sovereignty[81] and set a dangerous precedent for other countries.[82] Specifically, Google and the civil-society groups worried about the precedent the case might set for other cross-border delisting requests—especially those made pursuant to the right to be forgotten in Europe.[83]

/canadas-supreme-court-orders-google-to-alter-search-results-worldwide [https://perma.cc/JN2Z-HH7N] (describing Equustek's successful de-indexing case against Google).

72. Google Inc. v. Equustek Sols. Inc., [2017] 1 S.C.R. 824, 826 (Can.).

73. *Id.*

74. Complaint, *supra* note 7, at 2.

75. *Id.*

76. *Equustek*, [2017] 1 S.C.R. at 826.

77. The underlying dispute was between Equustek, a Canadian networking firm, and Datalink, a firm that allegedly stole and attempted to resell some of Equustek's products and designs. *See* Equustek Sols. Inc. v. Jack, 2014 BCSC 1063, 63 B.C.L.R. 5th 145 (Can. B.C. S.C.).

78. *Equustek*, [2017] 1 S.C.R. at 836-37.

79. Andrew Keane Woods, *No, the Canadian Supreme Court Did Not Ruin the Internet*, LAWFARE (July 6, 2017, 2:25 PM), https://lawfareblog.com/no-canadian-supreme-court-did-not-ruin-Internet [https://perma.cc/6VVP-TBDG].

80. *Equustek*, [2017] 1 S.C.R. at 846-47.

81. *See* Factum of Intervener Electronic Frontier Foundation, *Equustek*, [2017] 1 S.C.R. 824 (No. 36602).

82. *See* Factum of Intervener Human Rights Watch, *Equustek*, [2017] 1 S.C.R. 824 (Can.) (No. 36602).

83. *See* Woods, *supra* note 79.

Whatever the reason for the delisting request, the question in both *Equustek* and *Google v. CNIL* is not whether the state can regulate a search engine's means of serving search results, but whether the state can enforce its delisting orders across borders—and, indeed, what counts as a border.[84]

3. Law Enforcement Requests for Data

States also exert extraterritorial control over the internet in the context of law enforcement efforts to access foreign-held data. Governments seek access to this data for a number of reasons,[85] but their interest is fundamentally traceable to the fact that evidence of crimes is now often digital,[86] often stored in the cloud,[87] and often managed by a service provider located in another jurisdiction.[88] This evidence routinely crosses borders because much of it passes through the wires of the global internet.[89] As long as this is the case, law enforcement will continue to face jurisdictional barriers to accessing criminal evidence.[90]

Microsoft's recent dispute with the Department of Justice is a prime example of this phenomenon.[91] When the DOJ sought the contents of an email account that Microsoft stored in Ireland, Microsoft refused on the grounds that the Stored Communications Act (SCA) did not apply extraterritorially.[92] The technology firm initially challenged the order in court and lost.[93] On appeal before the Second Circuit, the firm won.[94] The Supreme Court then granted certiorari[95]

---

84. *See infra* Section III.C.

85. Woods, *supra* note 15, at 742.

86. *Id.* at 742-44.

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.* at 745-47.

91. *See supra* text accompanying note 6.

92. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 855 F.3d 53 (2d Cir. 2017) (denying rehearing en banc).

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

94. *Microsoft Corp.*, 855 F.3d 53.

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

and heard oral arguments,[96] but the Clarifying Lawful Overseas Use of Data (CLOUD) Act ultimately mooted the case.[97]

The question before the Court was whether ECPA applies extraterritorially.[98] The Second Circuit below held that it does not, but five other courts had reached a different conclusion. These courts held that the relevant location of the search is in the United States (where Microsoft receives search warrants) and therefore the case does not present a question about ECPA's extraterritorial reach after all.[99]

These are two different approaches to the same cross-border problem. The Second Circuit chose to address the jurisdictional questions head on.[100] It considered the weight of the authority and decided that limiting ECPA's territorial reach "serves the interests of comity that . . . ordinarily govern the conduct of cross-boundary criminal investigations."[101] In other words, the Second Circuit saw the issue as a matter of sovereign deference. The other courts to consider the issue skirted this question by finding that the disputed activity was domestic, regardless of where the data is stored.[102] They concluded that asking an internet firm to produce records was therefore not a novel application of ECPA across borders, but rather a domestic application of a search warrant, consistent with the courts' longstanding ability to compel firms to disclose evidence that the firm "can access and deliver within the United States."[103]

---

96. Transcript of Oral Argument, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam) (No. 17-2).

97. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam).

98. Petition for a Writ of Certiorari, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2).

99. *See, e.g.*, *In re* Search of Info. Associated with [Redacted]@Gmail.com that Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 2480752 (D.D.C. June 2, 2017); *In re* Search of Content that Is Stored at Premises Controlled by Google, No. 16-mc-80263, 2017 WL 1398279 (N.D. Cal. Apr. 19, 2017); *In re* Search of Premises Located at [Redacted]@Yahoo.com, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017); *In re* Info. Associated with One Yahoo Email Address that Is Stored at Premises Controlled by Yahoo, No. 17-M-1234, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017); *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708 (E.D. Pa. 2017).

100. *Microsoft Corp.*, 829 F.3d 197.

101. *Id.* at 221.

102. *In re Search of Info. Associated with [Redacted]@Gmail.com*, 2017 WL 2480752, at *6 ("Every court outside the Second Circuit that has considered the issue has rejected the holding of *Microsoft* . . . .").

103. *In re Info. Associated with One Yahoo Email*, 2017 WL 706307, at *3.

The enactment of the CLOUD Act resolves only some of these issues.[104] Under the Act, U.S. law enforcement can now obtain a search warrant under 18 U.S.C. § 2703 for data regardless of where that data resides.[105] However, the Act does not clarify how U.S. providers should respond to lawful requests for data from foreign governments that have not arrived at an executive agreement with the United States, as contemplated under the Act.[106] For example, suppose that a U.S. provider gets a request from a country not covered by the CLOUD Act; can the provider reply directly under local law or must the country apply for a U.S. warrant using the Mutual Legal Assistance Treaty (MLAT) process? The Act is simply unclear. The revisions to the SCA allow U.S. courts to grant warrants that reach foreign-held data, but they do not appear to resolve the question of whether the SCA prohibits U.S. providers from complying with foreign law enforcement requests for foreign-held data.

4. Surveillance

States have also sought to exercise extraterritorial control over the internet by enacting legislation that requires technology companies to store within their borders data about the country's citizens. These efforts do not align with the way internet companies organize their networks. Internet firms design their networks in ways that optimize for a number of different variables, including delivery speed, storage cost, national laws, and more.[107] As part of this optimization, some data will naturally leave one jurisdiction to be processed in another.[108] Requiring companies to store data in the country from which it originated would defeat the many benefits of a global network and would instead impose enormous startup costs on young companies.[109]

---

104. Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, §§ 103, 105 (2018) (to be codified at 18 U.S.C. §§ 2523, 2713).

105. *Id.* § 103(a)(1) (to be codified at 18 U.S.C. § 2713).

106. The question of whether and how ECPA applies abroad is still left somewhat unclear. The CLOUD Act's drafters clearly envisioned a world in which countries would be incentivized to strike agreements with the United States in order to make direct requests for data, but arguably if and where ECPA does not apply abroad—say, in an entirely foreign matter with regard to foreign-held data—why should that country feel the need to seek such an agreement?

107. *See* David Mytton, *Cloud Location Matters—Latency, Privacy, Redundancy*, SERVER DENSITY BLOG (Aug. 21, 2014), https://blog.serverdensity.com/cloud-location-matters-latency-privacy-redundancy [https://perma.cc/YLY4-AGD8].

108. *See id.*

109. Anupam Chander, *Why Democrats and Republicans Should Oppose Data Localization*, COUNCIL ON FOREIGN REL. (July 20, 2016), https://www.cfr.org/blog/why-democrats-and-republicans-should-oppose-data-localization [https://perma.cc/653V-YW7C].

Forced data localization is also harmful because it makes data more vulnerable to state surveillance. The storage location of data is enormously consequential for those concerned about interception by spying eyes,[110] notwithstanding arguments that location does not matter.[111] It follows that states seeking to protect the privacy of their citizens might strive either: (1) to keep their data within the country's borders, where it can be secured, or (2) to secure assurances from the states where the data are being sent.

These goals motivated the Safe Harbor Privacy Principles, developed by the U.S. Department of Commerce in conjunction with the European Commission, which allowed firms to self-certify that they would not make public certain kinds of personal data.[112] In the wake of the Snowden revelations about the scale of American surveillance on foreign targets, [113] Austrian citizen Maximilian Schrems challenged the Safe Harbor principles[114] and won. Here, the CJEU ruled that the Safe Harbor regime violated the Data Protection Directive because it provided insufficient protection from U.S. government surveillance.[115] Although this ruling created issues for both American and European firms doing cross-border business,[116] it was particularly challenging for the world's largest technology companies, which are primarily American firms.[117] In response, gov-

110. Woods, *supra* note 15, at 753.

111. *Cf. supra* note 28 and accompanying text.

112. The Safe Harbor regime was approved by the European Commission in a July 26, 2000 Decision, Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7, and pursuant to Directive 95/46/EC of the European Parliament and of the Council, 1995 O.J. (L 281) 31, *repealed by* Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

113. *See* Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded: What the Revelations Mean for You*, GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded [https://perma.cc/M9R4-6QTL].

114. Case C-362/14, Schrems v. Data Prot. Comm'r (Oct. 6, 2015), http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143358 [https://perma.cc/UP5Q-7FBS].

115. *Id.*

116. Timothy Edgar, *Surveillance Reform Is Only Hope for Reviving Safe Harbor*, LAWFARE (Oct. 7, 2015, 4:04 PM), https://www.lawfareblog.com/surveillance-reform-only-hope-reviving-safe-harbor [https://perma.cc/2XA2-RBDS] ("Just to be clear about the stakes—the US-EU safe harbor agreement is vital to transatlantic trade, and not just for big technology firms like Facebook and Google.").

117. *See id.*

ernments on both sides of the Atlantic worked to devise a remedy, and implemented a new regime called the EU-US Privacy Shield.[118] The Privacy Shield is a self-certification regime much like the Safe Harbor principles, but with more stringent privacy policy requirements and slightly stricter compliance obligations.[119] It quickly gained approval from relevant authorities in the United States and the European Union, and garnered significant support from technology companies.[120]

However, this regime is fragile. It depends on the assurances the U.S. government made in the Presidential Policy Directive 28 (PPD-28).[121] PPD-28 is a policy document developed by the Obama Administration that commits American signals intelligence efforts to meeting certain minimization, oversight, and transparency requirements, addressing in particular some concerns of allies about the collection of data on foreign persons.[122] In response, Digital Rights Ireland filed an "action for annulment" with Europe's second highest court, challenging the Privacy Shield on the grounds that the decision ratifies the American authorities' foreign-surveillance program without due respect for the privacy laws of all the sovereigns covered by the regime.[123] The adequacy of PPD-28 and the entire Privacy Shield regime is under review in a European court.[124]

---

118. European Commission Press Release IP 16/216, EU Commission and United States Agree on New Framework for Transatlantic Data Flows: EU-US Privacy Shield, (Feb. 2, 2016), http://europa.eu/rapid/press-release_IP-16-216_en.htm [https://perma.cc/7GPN-GWP5].

119. Cynthia J. Rich, *Privacy Shield v. Safe Harbor: A Different Name for an Improved Agreement?*, MORRISON & FOERSTER (Mar. 3, 2016), https://www.mofo.com/resources/publications/privacy-shield-vs-safe-harbor-a-different-name-for-an-improved-agreement.html [https://perma.cc/R8G6-36K5]; *see also A Side-by-Side Comparison of "Privacy Shield" and the "Safe Harbor": The Easiest Way to Understand What Privacy Shield Is and What You Need to Do to Use It*, BRYAN CAVE LLP (July 17, 2016), https://www.bryancave.com/images/content/8/5/v2/85609/Comparison-of-Privacy-Shield-and-the-Safe-Harbor.pdf [https://perma.cc/CQ6T-SYBG] (comparing the Privacy Shield's and Safe Harbor regime's provisions).

120. *See* Cameron Kerry & Alan Charles Raul, *The Economic Case for Preserving PPD-28 and Privacy Shield*, LAWFARE (Jan. 17, 2017, 3:19 PM), https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield [https://perma.cc/2B2Z-285R].

121. *See id.*

122. Office of the Press Sec'y, *Presidential Policy Directive—Signals Intelligence Activities*, WHITE HOUSE § 4 (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/829D-AR7K].

123. Case T-670/16, Dig. Rights Ir. v. Comm'n (Sept. 16, 2016), http://curia.europa.eu/juris/document/document.jsf?text=&docid=185146&pageIndex=0&doclang=en [https://perma.cc/VNB6-42BA].

124. *Id.*

5. Digital Trade Restrictions

States have also exercised extraterritorial control over trade in digital goods. What does it mean to "import" or "export" in a world where firms send products across borders digitally? Consider the case of ClearCorrect, a dental-products company that takes scans of customers' teeth in the United States and sends those scans to Pakistan, where a digital model is created and then sent back to the United States, where the model is used to drive a 3-D printer that produces the ultimate product.[125] When a competitor accused the firm of violating a patent, the U.S. International Trade Commission (ITC) had to determine whether it had jurisdiction over the dispute.[126] Relevant to the inquiry, the Tariff Act gives the ITC authority over the importation of articles.[127] The ITC thus had to determine whether emailing designs from Pakistan to have them printed in Texas constituted the importation of articles, and concluded that it did.[128] The Federal Circuit reversed, finding that "articles" means "material things," and that the ITC accordingly does not have jurisdiction over digitally transmitted designs.[129] The court noted that "it is difficult to see how one could physically stop electronic transmissions at the borders under the current statutory scheme."[130] Many parties filed amicus briefs in the case, including the Internet Association[131] — which represents Apple, Facebook, Google, and other internet companies — the Motion Picture Association of America, and the Recording Industry Association of America.[132] The matter ended when the ITC declined to petition for a writ of certiorari, but courts have not heard the last of sovereignty concerns in the context of digital imports.[133] The question of restraints on digital trade played a ma-

125. ClearCorrect Operating, LLC v. Int'l Trade Comm'n, 810 F.3d 1283, 1287 (Fed. Cir. 2015).

126. Certain Incremental Dental Positioning Adjustment Appliances and Methods of Producing Same; Notice of Institution of Formal Enforcement Proceeding, 77 Fed. Reg. 25747, 25747 (May 1, 2012).

127. Tariff Act of 1930 § 337, 19 U.S.C. § 1337(a) (2018).

128. *ClearCorrect Operating*, 810 F.3d at 1287-89.

129. *Id.* at 1286-87.

130. *Id.* at 1295.

131. Brief of the Internet Ass'n as Amicus Curiae in Support of Appellants & Urging Reversal, *ClearCorrect Operating*, 810 F.3d 1283 (No. 2014-1527).

132. Brief of the Motion Picture Ass'n of America & the Recording Industry Ass'n of America as Amici Curiae in Support of the U.S. International Trade Commission's Petition for Rehearing En Banc, *ClearCorrect Operating*, 810 F.3d 1283 (No. 2014-1527).

133. Ryan Davis, *ITC Won't Appeal ClearCorrect Patent Ruling to High Court*, LAW360 (Aug. 31, 2016, 6:50 PM EDT), https://www.law360.com/articles/834949/itc-won-t-appeal-clearcorrect-patent-ruling-to-high-court [https://perma.cc/4HZV-FG3Y].

jor role in the Trans-Pacific Partnership negotiations[134] and is now a key focus of the U.S. Trade Representative.[135]

B. Common Features

These seemingly disparate issues share a common set of features. In each case (1) an old problem wears new clothes, thanks to a once-physical process becoming digital; (2) there is a cross-border dimension to the problem that raises jurisdictional questions about the scope of territorial or extraterritorial authority; (3) the cross-border nature raises conflicts-of-laws questions; and (4) there are opportunities for arbitrage that flow from the fact that laws are not harmonized and internet business can easily be conducted across borders.

1. Digitization

In each of these issues, a relatively old and settled area of the law—like search-and-seizure law or free-speech law—appears unresolved because the activity in question is now digital. For example, while there are many cases articulating the standards for importation of articles,[136] before the *ClearCorrect* case there were none in the Federal Circuit about whether digital files constituted articles.[137] Regarding the production of evidence, the fact that evidence is now digital often makes it harder to access, either because it is held by a provider located in another jurisdiction or because it is held in another jurisdiction.[138] Digitization makes old problems new by taking formerly domestic issues—like what sorts of speech can be prohibited, or when governments can compel the production of criminal evidence—and introducing a cross-border dimension, which

134. *See* Greg Hicks, *Digital Trade and Cross Border Data Flows in the Trans-Pacific Partnership*, CTR. FOR STRATEGIC & INT'L STUD. (Mar. 12, 2014), https://www.csis.org/analysis/digital-trade-and-cross-border-data-flows-trans-pacific-partnership [https://perma.cc/AR4U-5Z36].

135. *Key Barriers to Digital Trade*, OFF. U.S. TRADE REPRESENTATIVE (Mar. 2017), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade [https://perma.cc/59Y4-GBNQ].

136. *See* ClearCorrect Operating, LLC v. Int'l Trade Comm'n, 819 F.3d 1334, 1342-44 (Fed. Cir. 2016) (Newman, J., dissenting from denial of rehearing en banc).

137. *See* Brian Busey et al., *Indecision at the ITC: Ramifications of the ITC's First Stay of a Remedy Order*, MORRISON & FOERSTER (Aug. 24, 2015), https://mofoatitc.mofo.com/itc-procedures/indecision-at-the-itc-ramifications-of-the-itcs-first-stay-of-a-remedy-order [https://perma.cc/FE33-7DRX].

138. Woods, *supra* note 15, at 739.

typically arises because the data are, or the provider is, now connected to a global network.

2. *The Cross-Border Cloud*

The cross-border nature of the internet is particularly salient outside of the United States. The vast majority of internet users hail from countries other than the United States.[139] Yet American firms continue to operate the most popular websites and internet services around the world.[140] This means that, for most state regulators, regulating the internet means regulating across borders. For example, criminal evidence was typically found in the same jurisdiction as the crime and the criminal.[141] This is no longer true. Now law enforcement agents routinely seek access to evidence controlled by foreign internet companies—typically American firms—who store or control that evidence in another jurisdiction.[142] Speech issues are similar. France once could control what speech was made within its territory and had in fact sought remedial action for impermissible domestic speech.[143] No more. When the French government asks Twitter to remove offending material, it depends on the cooperation of an American company, which will often need to take action in another country.[144] The company might raise a number of arguments, including that the relevant data is abroad; the company is headquartered abroad; the team that handles takedown requests is located outside of France; the terms of service are subject to California law; and more.[145] Each of these claims may frustrate the French regulatory effort.

---

139. *See* Kerr, *supra* note 15, at 287.

140. Woods, *supra* note 15, at 741.

141. *Id.* at 745.

142. *Id.*

143. 1 CENSORSHIP: A WORLD ENCYCLOPEDIA 39 (Derek Jones ed., 2001) (describing the censorship in France of *La Question*).

144. *See, e.g.*, *U.S. Judge Dismisses Lawsuit Against Twitter over ISIS Rhetoric*, NBC NEWS (Aug. 11, 2016, 3:26 AM EST), http://www.nbcnews.com/tech/social-media/u-s-judge-dismisses-lawsuit-against-twitter-over-islamic-state-n627661 [https://perma.cc/9JAP-YBH5].

145. *See, e.g.*, Warwick Ashford, *Google Claims It Is Not Subject to UK Privacy Laws*, COMPUTER WKLY. (Aug. 19, 2013, 8:12 AM), http://www.computerweekly.com/news/2240203739/Google-claims-it-is-not-subject-to-UK-privacy-laws [https://perma.cc/EBW3-2F7M] (noting Google's domicile theory of jurisdiction); Aurelien Breeden, *French Court Rules It Has Jurisdiction over Facebook in Nude Painting Case*, N.Y. TIMES: ARTSBEAT (Mar. 6, 2015, 10:17 AM), https://artsbeat.blogs.nytimes.com/2015/03/06/french-court-rules-it-has-jurisdiction-over-facebook-in-nude-painting-case [https://perma.cc/YQ45-C68D] (noting that Facebook argued its terms of service prevented a French court from exercising jurisdiction); Christopher Williams, *Google Argues UK Privacy Laws Do Not Apply to It*, TELEGRAPH (Aug. 18, 2013,

3. Conflicts of Laws

The extraterritorial nature of these issues often raises conflict-of-laws issues. If France asks Yahoo! to remove internet content from its site globally, that may give rise to a direct conflict of laws—for instance, if that content is protected speech in California.[146] The same is true for law enforcement requests. If a court in California orders an internet firm to produce data held in Germany, it may violate German privacy laws or the European General Data Protection Regulation.[147]

The first step in any conflicts analysis is to determine whether there is a conflict at all.[148] In many cases, there is more hand-wringing about conflicts than actual conflict of laws.[149] For example, in *Microsoft Ireland*, Microsoft argued that "[t]he power to embark on unilateral law enforcement incursions into a foreign sovereign country—directly or indirectly—has profound foreign policy consequences."[150] Ireland agreed, filing an amicus curiae brief arguing that its own sovereignty was at stake.[151] However, neither Microsoft nor Ireland pointed to a particular law in Ireland that would be violated as a consequence of compelling Microsoft to produce emails stored in Ireland.[152] Something similar occurred in

5:26 PM BST), http://www.telegraph.co.uk/technology/google/10250801/Google-argues-UK-privacy-laws-do-not-apply-to-it.html [https://perma.cc/MEM8-96J6] ("Google has argued that as an American company it is not 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.").

146. *See* Yahoo!, Inc. v. La Ligue Contre Le Racisme Et l'Antisemitisme, 169 F. Supp. 2d 1181, 1194 (N.D. Cal. 2001).

147. *See Microsoft to Use German Data Centers for Privacy*, LEGAL SOLUTIONS BLOG (Nov. 16, 2015), http://blog.legalsolutions.thomsonreuters.com/law-and-techology/microsoft-to-use-german-data-centers-for-privacy [https://perma.cc/5JS8-FWBE].

148. Larry Kramer, *Rethinking Choice of Law*, 90 COLUM. L. REV. 277, 291-92 (1990).

149. *Id.*; *see also* Woods, *supra* note 15, at 775 ("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.").

150. Brief for Appellant at 3, Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 855 F.3d 53 (2d Cir. 2017) (No. 14-2985).

151. *See* Brief of Amicus Curiae Ireland, *supra* note 18, at 3.

152. Woods, *supra* note 15, at 775 n.226 ("Ireland has not explicitly argued that a conflict of laws exists."). The European Union's amicus brief raises the *possibility* that Microsoft's compliance with the order might be inconsistent with the EU's General Data Privacy Regulation, but the brief does not say outright that it would be. Brief of the European Commission on Behalf of

Equustek, in which Google argued that the court's worldwide takedown order constituted a breach of international comity.[153] Google made this argument even though, as the court noted, it had offered no evidence that compliance with the court order would produce a conflict of laws anywhere.[154]

4. Arbitrage Opportunities

Firms that operate across borders are able to take advantage of arbitrage opportunities.[155] The best-known examples of arbitrage come from tax law. Apple—one of the wealthiest companies in the world—famously pays little corporate tax through clever accounting that takes advantage of jurisdictional differences.[156] But Apple is hardly alone,[157] and tax is not the only area that presents opportunities for arbitrage. Companies deploy similar strategies for data storage: they carefully choose where to store data based on the location of users, fiber optic cable placements, storage cost, and national laws.[158]

Firms will also operate strategically to exploit differences between one state's laws and another's. For example, Yahoo! and Google move data around the world between company servers located on several different continents.[159] As a consequence, they regularly tell governments that the data is stored in another

the European Union as Amicus Curiae in Support of Neither Party, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam) (No. 17-2).

153. Factum of the Intervener the Attorney General of Canada, *supra* note 18, at 7.

154. Google Inc. v. Equustek Sols. Inc., [2017] 1 S.C.R. 824, 828 (Can.) ("If Google has evidence that complying with such an injunction would require it to violate the laws of another jurisdiction, including interfering with freedom of expression, it is always free to apply to the British Columbia courts to vary the interlocutory order accordingly. To date, Google has made no such application.").

155. *See* Victor Fleischer, *Regulatory Arbitrage*, 89 TEX. L. REV. 227 (2010) (describing how arbitrage opportunities are created when two jurisdictions regulate the same conduct differently).

156. Charles Duhigg & David Kocieniewski, *How Apple Sidesteps Billions in Taxes*, N.Y. TIMES (Apr. 28, 2012), https://www.nytimes.com/2012/04/29/business/apples-tax-strategy-aims-at-low-tax-states-and-nations.html [https://perma.cc/2WPK-E3RE].

157. David Leonhardt, *The Big Companies that Avoid Taxes*, N.Y. TIMES (Oct. 18, 2016), https://www.nytimes.com/2016/10/18/opinion/the-big-companies-that-avoid-taxes.html [https://perma.cc/T7L3-QWXW].

158. Mytton, *supra* note 107.

159. Petition for Rehearing and Rehearing En Banc at 3, Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 855 F.3d 53 (2d Cir. 2017) (No. 14-2985) ("Major U.S.-based providers like Google and Yahoo! store a customer's email content across an ever-changing mix of facilities around the world.").

jurisdiction, and is therefore not accessible to local law enforcement.[160] In the wake of the *Microsoft Ireland* decision, firms made the same arguments to U.S. law enforcement, suggesting that data could be moved to a jurisdiction where it is inaccessible to law enforcement at the firm's command.[161]

The CLOUD Act resolves some of these jurisdictional challenges with regard to law enforcement access to data,[162] but the broader issue remains: the internet makes regulatory arbitrage especially simple. Firms can choose, among other things, where to be headquartered, where to keep money and employees (both of which risk being seized),[163] and which country's laws will govern the terms of service.[164] Each of these decisions allows the firm to determine how much leverage states have over it.

5. Sovereignty Concerns

Finally, and most importantly, the data-sovereignty disputes all raise concerns about state sovereignty—about the state's ability to regulate the global internet in ways that do not conflict with the prerogatives of other sovereigns. While the data-sovereignty cases come to courts framed as conflicts between a firm and a state, they implicitly involve a conflict between two states, each one seeking to regulate the same internet conduct. The *Microsoft Ireland* case was a good example. At one level, the case presented a domestic question of statutory interpretation: did Congress intend for the SCA to apply abroad, and are the facts of the case extraterritorial or domestic?[165] But in another sense, the case was

---

160. *See, e.g.*, *id.* at 19 ("[T]he *only* employees who can access the entirety of a customer's account, including those portions momentarily stored overseas, are located in the United States.").

161. Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, WASH. POST: VOLOKH CONSPIRACY (Nov. 29, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case [https://perma.cc/59F5-2Y5F].

162. Andrew Keane Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018, 5:49 PM), https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems [https://perma.cc/7VZS-MBSL].

163. For example, Facebook's Vice President for Latin American operations was arrested in Brazil for not complying with a law enforcement request there. Will Connors, *Facebook Executive Arrested in Brazil*, WALL ST. J. (Mar. 1, 2016), https://www.wsj.com/articles/facebook-executive-arrested-in-brazil-1456851506 [https://perma.cc/SAJ2-D93F].

164. Klonick notes that the major social media firms' terms of service are heavily influenced by U.S. law, including the First Amendment. Klonick, *supra* note 51, at 1621.

165. Petition for Writ of Certiorari, *supra* note 3, at 13-14 (framing the question as one of statutory interpretation in line with the *Morrison v. National Australian Bank*, 561 U.S. 247 (2010), two-

about whether data stored in Ireland ought to be accessible to Irish or American authorities or both. As a number of amicus briefs from foreign sovereigns suggested,[166] the case implicated intersovereign relations, despite being framed before the Court as a dispute between an American firm and American law enforcement. And, as this Article has shown, the phenomenon of sovereigns asserting their interests over internet conduct before a foreign court is hardly unique to the issue of law enforcement access to data abroad.[167]

What are we to make of the fact that sovereign-to-sovereign disputes are being resolved in cases that involve corporate intermediaries? One common reaction is to make two distinct but related arguments: (1) intermediaries threaten state sovereignty; and (2) as a result of the world moving online, state power is in decline. That is, because private intermediaries—often corporations—are able to exploit arbitrage opportunities, they raise concerns about the "quasi-sovereign"[168] power of intermediaries. In particular, some worry that the power of private firms threatens national sovereignty.[169] This is understandable, given how much power some internet companies wield. Because these corporations have considerable latitude in how they handle customer data, how they structure their operations, and which legal rules they comply with, they have become powerful organizations that play key roles in determining major aspects of internet policy. Consider takedown requests.[170] Regardless of whether France demands that Facebook take down certain content—hate speech, say, or private information—Facebook's own content rules and terms of service shape online free-

step analysis: (1) whether the SCA applies extraterritorially and (2) whether the focus of the statute is implicated by the facts of the case that are domestic or extraterritorial).

166. *See, e.g.*, Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, *supra* note 152; Brief for Ireland as Amicus Curiae in Support of Neither Party, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam) (No. 17-2); Brief for the New Zealand Privacy Commissioner as Amicus Curiae in Support of Neither Party, *Microsoft*, 138 S. Ct. 1186 (No. 17-2); Brief of the Government of the United Kingdom of Great Britain & Northern Ireland as Amicus Curiae in Support of Neither Party, *Microsoft*, 138 S. Ct. 1186 (No. 17-2).

167. *See supra* Section I.A.

168. Rozenshtein, *supra* note 28, at 188.

169. *See supra* note 28.

170. *See, e.g.*, *Government Requests for User Data*, FACEBOOK TRANSPARENCY REP., https://transparency.facebook.com/government-data-requests [https://perma.cc/3FAD-H36N]; *Government Requests to Remove Content*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/government-removals/overview [https://perma.cc/TJU9-DXYT]; Microsoft Corp. Soc. Responsibility, *Content Removal Requests Report: July-December, 2017*, MICROSOFT, https://www.microsoft.com/en-us/about/corporate-responsibility/crrr [https://perma.cc/9A23-EFW9].

speech policy.[171] In fact, those rules may be more influential in shaping speech on the platform than any one state's law.[172] For this reason, Kate Klonick calls these firms "the New Governors,"[173] and she develops a "conceptualization of online platforms as governance."[174]

In addition to setting substantive policy, intermediaries also play a role in determining which states can enforce their laws and to what extent they can do so.[175] In the cross-border law enforcement context, intermediaries may have little say in the substantive criminal laws of a given country, but they have enormous latitude in determining when and how to comply with law enforcement demands for evidence.[176] Firms hoping to bolster their public image as defenders of user privacy may choose to drag their feet, claim they cannot find responsive data, and even move the data into another jurisdiction, scuttling lawful investigations.[177] In the surveillance context, Alan Rozenshtein has argued that intermediaries are powerful entities, without whom the government cannot do its job.[178] He notes that "internet companies challenge the state's monopoly over security, the very locus of traditional conceptions of sovereignty."[179] Government surveillance efforts are shaped not only by whether the firm complies with requests to coordinate, but also by the nature of the firm itself. For example, if a firm chooses to encrypt all customer communications, it can engineer itself into

171. Klonick, *supra* note 51, at 1620.

172. *Id.* at 1630-62.

173. *Id.* at 1662-64.

174. *Id.* at 1602. Although Klonick notes that governance does not mean government, *id.* at 1617, the thrust of her argument is that private firms now deploy self-regulatory mechanisms and play a role that was once left for the state, *id.* at 1602 ("[P]latforms have developed a system that has marked similarities to legal or governance systems."); *see also* Anupam Chander, *Facebookistan*, 90 N.C. L. Rev. 1807, 1817-19 (2012) (describing how Facebook does not fit the definition of a nation-state in every sense, but nonetheless plays a considerable governance role and can enter into agreements with states).

175. *See* Klonick, *supra* note 51, at 1622-23 (describing firm efforts to stymie government requests).

176. *Id.* at 1650.

177. *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (2017) [hereinafter *Data Stored Abroad*] (statement of Richard Downing, Acting Deputy Assistant Att'y Gen., Dep't of Justice), https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era [https://perma.cc/99QQ-LW8S]; Kerr, *supra* note 161.

178. Rozenshtein, *supra* note 28.

179. *Id.* at 187.

a position of being unhelpful to surveillance efforts.[180] Because it controls the data, the intermediary can shape much of the key policy landscape.

The rise of intermediary power therefore corresponds with a sense that state sovereignty is diminishing. In the surveillance realm, U.S. law enforcement agents regularly complain of the "going dark" problem to describe the spread of encrypted communications tools—a term that reflects a sense of loss.[181] Where the state could previously intercept domestic communications—usually with a wiretap—today it finds that many lines of communication have been encrypted.[182] Activity in the digital sphere also has the potential to make it harder for the state to manage internal affairs.[183] In 2015, Russia and China signed an agreement to jointly combat the use of information technology "to interfere in the internal affairs of states; undermine sovereignty, political, economic and social stability; [and] disturb public order."[184] The concern, according to Russian officials, is that the internet exposes the state to foreign espionage, cybersecurity attacks, and civil unrest.[185]

States' own statements about their loss of power might seem like definitive proof that state power is on the wane in the digital era. Indeed, there are a number of areas where state efforts are frustrated by private intermediaries. But the rise of corporate intermediaries and state fears about their influence over online conduct do not tell the whole story.

---

180. *See* Nathaniel Mott, *Take That, FBI: Apple Goes All in on Encryption*, GUARDIAN (June 15, 2016), https://www.theguardian.com/technology/2016/jun/15/apple-fbi-file-encryption-wwdc [https://perma.cc/SC26-F6VA].

181. *Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy*: *Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 1 (2015) (joint statement of James B. Comey, Dir., Fed. Bureau of Investigation, and Sally Quillian Yates, Deputy Att'y Gen., Dept. of Justice) (describing how encryption and other developments "have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant. We in law enforcement often refer to this problem as 'Going Dark.'").

182. *Id.*

183. *See* Gary King et al., *How Censorship in China Allows Government Criticism but Silences Collective Expression*, 107 AM. POL. SCI. REV. 1 (2013) (showing how the primary concern for China's censors is not criticism, as commonly believed, but rather attempts at social unrest through collective action); *see also* Jessi Hempel, *Social Media Made the Arab Spring, But Couldn't Save It*, WIRED (Jan. 26, 2016, 3:06 PM), https://www.wired.com/2016/01/social-media-made-the-arab-spring-but-couldnt-save-it [https://perma.cc/FFH2-DXT4] (noting that while there was once great hope about the Arab Spring, "governments take an aggressive hand in shutting down digital channels people use to organize against them").

184. Jack Margolin, *Russia, China, and the Push for "Digital Sovereignty,"* GLOBAL OBSERVATORY (Dec. 2, 2016), https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization [https://perma.cc/2QB6-P855].

185. *Id.*

II. THE CASE FOR SOVEREIGN DEFERENCE

Competing claims of sovereign authority over the internet will be an enduring feature of internet lawsuits. Ultimately, this means that courts will have to adapt sovereign-deference doctrines to the internet. But before turning to *how* courts might manage competing sovereign claims in this area,[186] we must consider whether sovereigns are owed deference at all. As a normative matter, what is the case for sovereign deference? This Part provides one. It begins by showing that the sovereignty concerns raised in cross-border internet disputes are ultimately surmountable: while states may find it harder than usual to accomplish their aims in the face of foreign internet services, they have powerful tools at their disposal to do so. The key governance challenge for the global internet is not whether the state can accomplish its goals, but rather finding ways for states to do so that are compatible with a global internet.

This means two things: accommodating sensible sovereign control over the internet and, relatedly, embracing a global internet governance ideal that reflects sovereign differences. We should not give states reason to assert control by brute force—taking physical control over the network architecture in ways that produce negative externalities. Instead, we should allow sovereigns to enforce their laws on their soil wherever doing so does not interfere unreasonably with other sovereigns' regulation of the internet. Accordingly, we must reject the fantasy that the internet can or should be governed by the same rules everywhere. Early visions of internet governance were insensitive to state interests, but as they evolved to accommodate the idea of state regulation over the internet, the anarchist dream of an internet free from government rules morphed into a cosmopolitan dream of an internet with one set of rules for all.[187] For the global governance of the internet, cosmopolitanism is nearly as impractical as anarchy.

---

186. *See infra* Part III.

187. *Cf.* Scott J. Shackelford & Amanda N. Craig, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 128 (2014) (describing the emergence of the "multi-stakeholder model of Internet governance" and noting the criticism that model has faced from a "growing array of states").

A. What Is Data "Sovereignty"?

Sovereignty is a notoriously amorphous concept.[188] Yet, as we have seen, it is increasingly invoked in cross-border internet disputes.[189] What might sovereignty mean in this context? Despite the contested nature of the term, nearly all definitions of sovereignty contain the following elements:[190] (1) supreme control;[191] (2) over a territory;[192] (3) independent from other sovereigns.[193] These features can be mapped onto the concept of a global internet in a number of different ways. What will become clear, however, is that without committing too deeply to a particular conception of data sovereignty, there is little doubt that states have the *capacity* for sovereign control over the internet. The question—indeed, a crucial question for internet governance—is how they exert that control.

1. Sovereign Capacity

Do states have supreme control over the data in their territory to the exclusion of other sovereigns? In at least one very real sense, they have the capacity to exercise that control. Despite the concerns about state sovereignty mentioned above—and despite early internet thinkers' desires to the contrary[194]—states can command considerable control over the internet if only because they control the

---

188. *See, e.g.*, MARTTI KOSKENNIEMI, FROM APOLOGY TO UTOPIA: THE STRUCTURE OF INTERNATIONAL LEGAL ARGUMENT 240-41 & n.49 (2005) [hereinafter KOSKENNIEMI, APOLOGY TO UTOPIA] (noting that scholars have found the concept hard to pin down—Kelsen identified eight distinct definitions of the term—and that some are outright dismissive of efforts to do so); *see also* Martti Koskenniemi, *Conclusion: Vocabularies of Sovereignty—Powers of a Paradox*, *in* SOVEREIGNTY IN FRAGMENTS: THE PAST, PRESENT AND FUTURE OF A CONTESTED CONCEPT 222, 222-42 (Hent Kalmo & Quentin Skinner eds., 2010) (reviewing the multiplicity of discourses in which sovereignty is invoked and acknowledging its appeal as a rhetorical device).

189. *See supra* Section I.B.5.

190. Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 476 n.5 (1998).

191. JEAN BODIN, THE SIX BOOKES OF A COMMONWEALE 84 (Richard Knolles trans., London, Impensis G. Bishop 1606) ("Soueraigntie is the most high, absolute, and perpetuall power ouer the citisens and subiects in a Commonweale.").

192. KOSKENNIEMI, APOLOGY TO UTOPIA, *supra* note 188, at 241-42.

193. Koskenniemi suggests that independence might even be a synonym for sovereignty, albeit a less-than-helpful one. This is often referred to as the internal/external dimension of sovereignty. *Id.* at 240-42.

194. *See, e.g.*, Barlow, *supra* note 28; Johnson & Post, *supra* note 28.

physical components of the network within their borders.[195] Today, nearly all observers acknowledge that the internet is not a lawless zone. To the contrary, states have an impressive arsenal of tools they use to assert control over the internet, and they are increasingly willing to deploy these tools.[196]

The most basic means of state control over the internet is physical control over the network architecture—the fiber, servers, and computers—that comprises the internet and that is located within the state's borders.[197] This gives the state power to censor content,[198] to monitor online activity,[199] and to cut a country's access to the network entirely.[200] But physical control over the nodes of the network is only the crudest form of state power over the internet, which is also facilitated by the market for internet services. This is especially true today as large technology companies dominate the internet. Across a range of issues—from surveillance[201] to speech[202]—states are able to harness the market and the considerable power of corporate intermediaries to accomplish their aims. States with lucrative markets can demand that firms comply with local law as the price of admission to those markets. The compliance measures might include giving the state physical access to corporate servers—as in China[203]—or access to its

195. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 50-58 (2006).

196. *See*, *e.g.*, Justin Hendrix, *The Age of Unregulated Social Media Is Over*, JUST SECURITY (Feb. 15, 2018), https://www.justsecurity.org/52346/age-unregulated-social-media [https://perma.cc/K9EW-VTLK] (cataloguing increased political pressure around the globe to regulate internet firms, especially in the wake of allegations of undue influence on the U.S. 2016 presidential election).

197. *See, e.g.*, Craig Timberg, *NSA Slide Shows Surveillance of Undersea Cables*, WASH. POST (July 10, 2013), https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html [https://perma.cc/HKQ2-M2SC] (explaining how the U.S. government's physical access to fiber-optic cables allowed the National Security Agency to surveil internet traffic as part of its Upstream program).

198. *See* Nikhil Sonnad & Keith Collins, *How Countries like China and Russia Are Able to Control the Internet*, QUARTZ (Oct. 5, 2016), https://qz.com/780675/how-do-internet-censorship-and-surveillance-actually-work [https://perma.cc/A6SB-M2UA] (surveying research about different countries' efforts to censor, monitor, and otherwise control the internet).

199. *See id.*

200. *See id.*

201. *See* Rozenshtein, *supra* note 28.

202. *See* Klonick, *supra* note 51.

203. *See* Sherisse Pham, *Use iCloud in China? Prepare to Share Your Data with a State-Run Firm*, CNN (Jan. 11, 2018, 11:09 AM), http://money.cnn.com/2018/01/10/technology/apple-china-icloud/index.html [https://perma.cc/E32W-MP8G] (describing how the government will have access to corporate servers in mainland China).

domestic bank accounts or employees. And even if states do not have physical control over the data itself, they can assert control over the people and property that administer access to the data.

States also respond to threats to their sovereignty by directly or indirectly competing in the marketplace with their own homegrown intermediaries, which offer alternatives to foreign internet firms and which might be more cooperative with the government. For example, in Russia, Kaspersky Lab is a prominent firm that does significant business in the global marketplace for cybersecurity and antivirus services. The Russian government likely has greater leverage over Kaspersky than over a foreign firm, as Kaspersky can be more easily made to follow Russian rules and might also be persuaded to do the state's bidding.[204] The same thing has been said of Chinese technology companies, where homegrown entities like Huawei provide the state with greater access to internal compliance mechanisms and may also act as a vehicle for accomplishing foreign policy aims.[205]

Indeed, if there is any question about whether states can bend the internet to local rules, one need only look to China.[206] In order to do business there, firms face a stark choice: store the physical components of firm architecture—data centers, encryption keys—in the country or leave it entirely. Apple, for example, announced that it would build a Chinese datacenter in accordance with China's data localization law, making that data vulnerable to government authorities.[207] Apple promised that there would be "no backdoors" and that Apple would retain control over the encryption keys which would be stored in the United States.[208]

---

204. For example, Russian state hackers used Kaspersky Lab products to infect 400 million computers around the world with Russian government software. Nicole Perlroth & Scott Shane, *How Israel Caught Russian Hackers Scouring the World for U.S. Secrets*, N.Y. TIMES (Oct. 10, 2017), https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html [https://perma.cc/3JY7-L6QR].

205. *See* Steve Lohr, *F.C.C. Joins Push to Limit China's Telecom Reach*, N.Y. TIMES (Mar. 26, 2018), https://www.nytimes.com/2018/03/26/technology/fcc-huawei-security-rule.html [https://perma.cc/UM8T-E9W7].

206. *See* Simon Denyer, *China's Scary Lesson to the World: Censoring the Internet Works*, WASH. POST. (May 23, 2016), https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html [https://perma.cc/3TK6-UHD4].

207. Alyssa Abkowitz & Eva Dou, *Apple to Build China Data Center to Meet New Cybersecurity Law*, WALL ST. J. (July 12, 2017, 6:52 PM), https://www.wsj.com/articles/apple-to-build-china-data-center-to-meet-new-cybersecurity-law-1499861507 [https://perma.cc/5ZWW-V37F].

208. *Id.*

However, less than a year later, it announced plans to move the keys to its Chinese iCloud accounts to Chinese territory.[209] Apple made the move to comply with Chinese government demands. Google and Facebook have also begun efforts to comply with Chinese law in order to access the Chinese market,[210] in Google's case even going so far as to develop a censored version of its flagship search product.[211]

This is not to say that states will never be frustrated by foreign or even domestic internet companies, or that states do not incur costs when they assert control over the internet. Governments can experience enormous political pressure to refrain from exercising their powers online. A judge in Brazil sparked an uproar when he ordered local telecommunications carriers to block the popular chat service WhatsApp,[212] and another judge ultimately reversed the order on the grounds that it would be unfair to users.[213] Likewise, when the U.S. government asked Apple to provide it with keys to access an encrypted iPhone, protests were planned, and public officials urged the FBI to rescind its request.[214] Nevertheless, in the end, states have the tools necessary to assert control over the internet—the final, absolute control indicative of sovereign power. The question for litigants, judges, and policymakers, then, is not *whether* states can assert their power over data, but rather *how* they might do so.

---

209. *Apple Moves to Store iCloud Keys in China, Raising Human Rights Fears*, CNBC (Feb. 24, 2018, 5:48 AM), https://www.cnbc.com/2018/02/24/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears.html [https://perma.cc/TTH5-V23E].

210. *See* Mike Isaac, *Facebook Said to Create Censorship Tool to Get Back into China*, N.Y. TIMES (Nov. 22, 2016), https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html [https://perma.cc/F5KR-VX6X]; Jon Russell, *Google Moves into Shenzhen in Latest China Expansion*, TECHCRUNCH (Jan. 16, 2018), https://techcrunch.com/2018/01/16/googles-moves-into-shenzhen [https://perma.cc/BHU4-UWX3].

211. Ryan Gallagher, *Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal*, INTERCEPT (Aug. 1, 2018, 4:58 AM), https://theintercept.com/2018/08/01/google-china-search-engine-censorship [https://perma.cc/C6HV-65S6].

212. *See* Vinod Sreeharsha, *WhatsApp Blocked in Brazil as Judge Seeks Data*, N.Y. TIMES (May 2, 2016), https://www.nytimes.com/2016/05/03/technology/judge-seeking-data-shuts-down-whatsapp-in-brazil.html [https://perma.cc/7L4G-W2W3].

213. Jonathan Watts, *Judge Lifts WhatsApp Ban in Brazil After Ruling Block Punished Users Unfairly*, GUARDIAN (Dec. 17, 2015, 12:36 PM), https://www.theguardian.com/world/2015/dec/17/brazil-whatsapp-ban-lifted-facebook [https://perma.cc/R2PR-SG9B].

214. Matt Hamilton et al. , *Apple vs. FBI: Congressman Urges Comey to Drop Demands, 'Take a Deep Breath,'* L.A. TIMES (Feb. 23, 2016, 10:03 AM), http://www.latimes.com/business/technology/la-me-ln-apple-vs-fbi-protests-planned-across-the-nation-over-phone-privacy-20160222-story.html [https://perma.cc/TR7V-YAM8].

2. *Embracing Data Sovereignty*

We can separate states' sovereign powers over the internet into two broad categories: powers to *compel compliance* and powers to *control the means of compliance*. Compelled compliance leaves companies and their users free to design and use the internet as they see fit, as long as they comply when the government comes knocking. Controlled compliance, on the other hand, means that the state tells internet firms how to operate. This distinction may seem slight—in both scenarios, the police get the evidence or the website comes down—but in practice, there is a considerable difference between the two.

Regulation by compulsion says the following to users and firms: give us the evidence, or else. It articulates the consequences of refusing to comply, but it does not dictate the means. Regulation by control, however, says something else: weaken your security protocols in the following ways to allow government access to your platform. The difference is in the process that is due. Under compelled compliance, law enforcement offers the firm a choice: comply, or challenge the order in court or in the press. State powers of control, by contrast, offer no such opportunity. This exercise of power is considerably more insidious, because it allows the state to dictate the everyday operation of internet services.

Suppose that we have a choice between two worlds. In the first, Microsoft is free to store its data wherever it chooses, and it is also free to comply with lawful requests for data when presented with those requests by state governments. In the second world, Microsoft is not free to choose where it stores customer data. Instead, it must keep data on local drives and allow government agents direct access to the data. The second world is considerably worse than the first. Microsoft is much less capable of resisting unlawful exercises of state power; surveillance of customer data is considerably easier—both for local and foreign intelligence agencies. This world also requires the firm to spend considerably more money developing bespoke network architecture in each market. These costs—to autonomy, privacy, and entrepreneurship—are the result of a state asserting physical control over a particular piece of internet infrastructure.

States naturally resort to controlled enforcement powers when compulsion does not work. This is why states demand data localization.[215] Not only is locally stored data more helpful for state efforts at surveillance, but it also makes it easier for states to assert other sorts of control over intermediaries, for example, by

215. *See* Reema Shah, Comment, *Law Enforcement and Data Privacy: A Forward-Looking Approach*, 125 YALE L.J. 543, 548 (2015).

compelling the production of digital evidence[216] and blocking unwanted internet content.[217] This exercise of physical control over the network is problematic for a number of reasons, including increased costs and privacy concerns.[218] It should be a last resort. When the state acts in accordance with local law over a matter properly within its jurisdiction, it ought to be able to accomplish its aims without controlling the physical components of the network. In order to achieve this end, states should seek to accommodate each other and also to encourage firms to do the same.

Indeed, some of the worst clashes between governments and intermediaries have occurred where states sought to achieve their regulatory aims by compelling an intermediary to comply, and the intermediary refused. As mentioned earlier, when a Brazilian judge was frustrated with WhatsApp's inability to respond to a demand for evidence in a criminal case, the judge issued an injunction blocking the app in Brazil.[219] This meant that nearly 100 million users were unable to access the service.[220] The injunction was eventually overturned,[221] but the episode threatened to revive a bill that Brazilian legislators considered only a few years earlier that required internet firms to store data in Brazil, giving the state certain powers to control compliance.[222] Similarly, when Indian police sought the account information of a Facebook user who allegedly posted material that was critical of a Hindu god and Facebook resisted, the police raided Facebook's offices in Mumbai.[223] That same year, India's chief telecommunications authority publicly floated the idea of requiring foreign firms to store data locally, giving

---

216. *See* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 717 (2015).

217. *Id.* at 735-38.

218. *See id.* at 721-28.

219. Sreeharsha, *supra* note 212.

220. *Id.*

221. Russell Brandom, *Brazilian Courts Order WhatsApp Blackout, Change Course Hours Later*, VERGE (July 19, 2016, 1:11 PM), https://www.theverge.com/2016/7/19/12226884/brazil-whatsapp-blackout-order-encryption [https://perma.cc/FW26-8XBX].

222. Elias Groll, *Why Did Brazil Block WhatsApp?*, FOREIGN POL'Y (Dec. 17, 2015, 5:22 PM), https://foreignpolicy.com/2015/12/17/why-did-brazil-block-whatsapp [https://perma.cc/6QXM-S26N].

223. *Police Raid Facebook's Mumbai Office Looking the Details a Man Accused of Posting Derogatory Content*, TIMES INDIA (Dec. 12, 2016), https://www.indiatimes.com/news/india/police-raid-facebook-s-mumbai-office-looking-the-details-a-man-accused-of-posting-derogatory-content-267286.html [https://perma.cc/X29A-E7W5].

the state greater control over how foreign firms comply with Indian government orders.[224]

In each of these cases, a state government sought to enforce its laws on its soil and encountered resistance from an American firm. After the state's coercive power to compel the foreign intermediary to comply with local law failed, the state sought to assert its power by obtaining physical control over the data in question. This proved an unfortunate development—and an entirely unnecessary one. Had Facebook (which is also the owner of WhatsApp) complied with local requests, it might have accommodated the state's compulsion orders and avoided further pressure by the state to seek physical control over its data. Instead, conflict ensued—all because the firm would not comply with a domestic production order.[225]

In a world, then, where states retain the capacity to control the internet, and where a state's efforts to exercise that control often have spillover effects in another state, judges and policymakers have a choice. They can regulate the internet ex ante in ways that accommodate other sovereign interests by mutual recognition and deference—thereby allowing each state to regulate the internet with laws; or they can leave the foreign state to assert its interests by force. We should strongly prefer the former. The better regime of internet governance is one where users and providers are free to comply with state rules however they choose. This requires that states recognize other states' legitimate interests and provide mutual accommodation. This idea is rooted in longstanding notions of international relations, but it is also an idea deeply at odds with the dominant cosmopolitan ideal of internet governance.

B. Embracing Sovereign Differences

If the early debates about internet governance were about *whether* states had the power to regulate internet conduct, today's debates (as we have seen) are

224. Anuj Srivas, *Cross-Border Data Flows Debate Hits India as TRAI Issues Paper on Cloud Services*, WIRE (June 11, 2016), https://thewire.in/42300/cross-border-data-flows-debate-hits-india-as-trai-issues-paper-on-cloud-services [https://perma.cc/WSE9-J33T].

225. Why do the firms resist law enforcement orders? One answer is that firms find that they simply are prohibited from doing so under American law. *See, e.g.*, *Data Stored Abroad*, *supra* note 177 (statement of Richard Salgado, Director, Law Enforcement and Information Security, Google Inc.). Another possible explanation is that the firm has concerns about the human-rights record of the country where the order is being produced. This is not terribly satisfying, however, since the largest technology companies routinely push back on state law enforcement efforts in ways that appear at first blush to be principled but upon closer inspection appear to be driven by business interests. The best explanation of this dynamic is Rozenshtein, *supra* note 28, at 122-140.

about *which* states' rules should apply and where. There are, generally speaking, two competing visions of internet governance today: (1) a *cosmopolitan* ideal that aspires to one set of rules everywhere, which is diametrically opposed to (2) a *sovereign-difference* ideal that sees the internet operating differently in different places according to local norms, customs, and rules. The cosmopolitan ideal is grounded in the idea that the internet should be "free"[226]—an adjective that signals the wish that internet providers and users be at liberty to ignore local rules and operate instead by their own set of global internet rules.[227] The chief proponent of the cosmopolitan view is the United States, which has pursued an "open internet" policy for the past decade.[228] The animating conception is of the internet as a cosmopolis—a space that, if regulated by governments, should operate the same everywhere as "one internet."[229] This can be achieved through the universal imposition of a single set of rules.

But whose rules? Without saying as much, the answer is often implicitly "American rules."[230] For example, American providers—and the vast majority of the most popular web services in most countries are American[231]—embrace American free speech norms.[232] This reflects both the internal values of the members of the firm and the power of the U.S. government over the biggest internet firms.[233] As a result, these firms regularly resist foreign government ef-

---

226. Bureau of Democracy, Human Rights & Labor, *Global Internet Freedom Task Force (GIFT) Strategy: A Blueprint for Action,* U.S. DEP'T STATE (Dec. 28, 2006), https://2001-2009.state.gov/g/drl/rls/78340.htm [https://perma.cc/4JJ3-ZB72].

227. *See* Jack Goldsmith, *The Failure of Internet Freedom*, KNIGHT INST. (2018), https://knightcolumbia.org/sites/default/files/content/Emerging_Threats_Goldsmith.pdf [https://perma.cc/Z4BP-5SFE]. There is some confusion on this point, however. While the State Department uses the phrase "open Internet" to mean an internet free from censorship or other government controls, the Federal Communications Commission has used the phrase to refer to an internet free from paid prioritization in violation of net neutrality rules. *See Consumer Guide: Open Internet*, FED. COMM. COMMISSION (June 14, 2016), https://transition.fcc.gov/cgb/consumerfacts/openinternet.pdf [https://perma.cc/Q3AB-WFRB].

228. Fergus Hanson, *Internet Freedom: The Role of the U.S. State Department*, BROOKINGS (Oct. 25, 2012), https://www.brookings.edu/research/internet-freedom-the-role-of-the-u-s-state-department [https://perma.cc/H8G9-8P98].

229. Glob. Comm'n on Internet Governance, *One Internet*, CTR. FOR INT'L GOVERNANCE INNOVATION (2016), https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf [https://perma.cc/N8K7-YFM2].

230. Goldsmith, *supra* note 227, at 4-5 (describing the American conception of internet freedom).

231. *See* Woods, *supra* note 15, at 741.

232. *See* Klonick, *supra* note 51, at 1618-25.

233. *Id.*

forts to impose their own domestic speech rules.[234] These efforts, and the subsequent resistance, suggest one reason why other governments seek to establish strong domestic internet industries with firms that would be both more pliable at home and exert more soft influence abroad.[235]

The sovereign-difference ideal, by contrast, is concerned principally with state control over the internet's local effects. It places a premium on the standard components of sovereignty: state control over a territory. If the internet threatens the state's ability to achieve its domestic aims, or if it invites foreign meddlers, the sovereigntists see a global internet framework that respects difference, and respects state efforts to protect that difference.

These two conceptions of internet governance do not exist independent of each other. They are reactions to one another and reflect larger geopolitical struggles. The strong sovereignty approach to internet policy is a reaction to the sense non-Western states have that the internet rules are being written by Western states. Sovereigntists see the cosmopolitan ideal as a farce: under their view, it is American imperialism masquerading as globalism.[236] Cosmopolitans, for their part, accuse sovereigntists of trying to break apart the internet.[237] They often frame the debate as over whether the internet should be "open" or "balkanized."[238] But this framing is wrong for two reasons. First, the internet can be both. It can be uniform in many respects but also different where it needs to be (language, legal compliance, and so on). One does not lose openness—or interoperability—by embracing sovereign differences. The second reason this dichotomy is unhelpful is that fragmentation is already here. It is happening because states want it, because users want it, and because firms want it. The question is

---

234. *Id.* at 1650-52.

235. *See, e.g.*, *Vladimir Putin, Presidential Address to the Federal Assembly*, PRESIDENT RUSS. (Mar. 1, 2018), http://en.kremlin.ru/events/president/news/56957 [https://perma.cc/K82X-PYGF] ("Technological lag and dependence translate into reduced security and economic opportunities of the country and, ultimately, the loss of its sovereignty.").

236. Evgeny Morozov, *Who's the True Enemy of Internet Freedom—China, Russia, or the US?*, GUARDIAN (Jan. 3, 2015), https://www.theguardian.com/commentisfree/2015/jan/04/internet-freedom-china-russia-us-google-microsoft-digital-sovereignty [https://perma.cc/V2C4-9CPZ].

237. Fergus Ryan, *China Wants to Make the World Less Wide and Run Its Own Splinternet*, HUFFINGTON POST (Feb. 11, 2017, 10:12 AM EDT), https://www.huffingtonpost.com.au/fergus-ryan/china-wants-to-make-the-world-web-less-wide-and-run-its-own-splinternet_a_23262679 [https://perma.cc/F3JL-6QF3].

238. For example, Milton Mueller in a recent treatment suggests that there is "an inherent clash between alignment"—state efforts to hew the internet to local laws—"and the economic efficiencies and capabilities of digital technology." MILTON MUELLER, WILL THE INTERNET FRAGMENT? SOVEREIGNTY, GLOBALIZATION, AND CYBERSPACE 104 (2017).

not "should the internet fragment," but rather what kind of fragmentation should we encourage? The answer has to be the kind of fragmentation that allows maximal sovereign difference with minimal harm to other sovereigns. The answer, in other words, is the kind of fragmentation that is possible by state-to-state negotiation and mutual accommodation.

There are three principal objections to a sovereign-difference approach to internet governance. First, proponents of the cosmopolitan ideal of internet governance claim that their vision for the internet enhances privacy, speech, and entrepreneurship. But if generalizations are to be made about the two ideals, then it is precisely the other way around: deference to state differences is a necessary first step toward an internet-governance regime grounded in the rule of law rather than of technologies. Insisting that states follow American rules—or telling states that their rules are not applicable to the internet—is the surest way to encourage state control of technology rather than of law. Despite considerable efforts at supranational political organizations, states remain the single greatest source of legitimate rules for different peoples with varied community values and experiences on a diverse planet.[239] As a space for human communication and connection, the internet will and should reflect those differences. Cosmopolitans may pay lip service to this idea, but the reality is that cosmopolitan companies regularly resist state efforts to enforce their laws.[240]

Another natural objection to any argument for sovereign deference on the internet is that it is tantamount to splintering the internet into as many distinct networks as there are countries. But this argument tends to ignore political reality. Even if one is not persuaded by normative arguments about the legitimacy of a state's rules over conduct on its soil, the fact of the matter is that states will always insist—with brute force if necessary—that their rules apply. If the above estimation of state power over the physical components of the internet is correct, then some regional variation is inevitable. In such a world, the question is not whether there will be differences in how the internet behaves in different states, but rather how those differences will occur: by compulsion or by control? If we are to hope that states will achieve their aims without asserting physical control over servers and fiber cables, then states must be left free—and must leave each other free—to control how the internet operates on their territory. Indeed, we already operate in a world of sovereign deference for the regulation of nearly everything else—money, debt, securities, people, and goods—that flows across

239. *See* Stephen D. Krasner, *Think Again: Sovereignty*, FOREIGN POL'Y (Nov. 20, 2009, 3:28 PM), https://foreignpolicy.com/2009/11/20/think-again-sovereignty [https://perma.cc/N4GW-EHA3].

240. Rozenshtein, *supra* note 28, at 122-149 (describing and cataloguing internet firms' techniques of resisting state compliance efforts).

borders. Unless a state has explicitly granted a waiver of its own rules by agreement, sovereign deference is the rule rather than the exception. Why would we think that data, and the firms that handle that data, should be treated any differently?

The problem with the goal of a single set of rules for the internet is that it always redounds to the same question: whose rules will they be? In a world where the vast majority of the most popular internet services in most countries are American,[241] and the body responsible for governing the internet's architecture is widely perceived to be American,[242] the answer has long been that mostly American rules apply.[243] To a certain extent, then, rejecting internet globalism is rejecting American internet imperialism.

A final objection one might have to sovereignty arguments is that they serve as an apology for bad state behavior. Even if the strong sovereignty approach more accurately reflects political reality, cosmopolitans may also appeal to empirical evidence. Because the states that have pursued sovereign visions of the internet have so far largely been able to achieve their aims by exerting control over the technology, one might hesitate to embrace regional differences if doing so is a mere cover for state crackdowns on users.[244] But this is a mistake. The two issues—the global internet governance model and the state's use of power—are distinct. Embracing regional or state differences does not mean sacrificing human rights. One can accept sovereign differences—such as France's hate speech rules applied to Twitter in France, even where they contravene the First Amendment—without acquiescing to a future where every country behaves as China does, insisting on local storage of cloud architecture and direct, unmediated physical access and control over internet data. Indeed, one can defend China's sovereign interest in regulating the internet's domestic effects while deploring its civil and political rights record. In a world of inevitable sovereign control, a world of inevitable sovereign differences, sovereign deference is the best way forward. But deference does not mean endorsement or celebration. We

241. *See* Woods, *supra* note 15, at 741.

242. Maria Farrell, *Quietly, Symbolically, U.S. Control of the Internet Was Just Ended*, GUARDIAN (Mar. 14, 2016), https://www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana [https://perma.cc/7JTY-W9W6] (explaining how ICANN, the Internet Corporation for Assigned Names and Numbers, which is responsible for running the internet's naming and numbering systems, such as domain names, had long been perceived as American controlled).

243. *See* Kerr, *supra* note 15, at 287.

244. MUELLER, *supra* note 238, at 106 ("[Alignment] empowers repressive governments and protectionist interests by insulating people from access to information environments outside their own country.").

can, and we should, embrace the idea of state differences without embracing the idea of a state-run internet or a state-controlled internet.

C. The Case for Sovereign Deference

The most compelling defense of sovereign deference in cross-border data disputes is that it offers the best chance at creating the kinds of norms needed for a lasting and global internet. Sovereign states retain the capacity to regulate and control the internet, and they are going to exercise that control differently. The key question, then, is the shape these disparate exercises of sovereign power are going to take. Do states accomplish this fragmentation by force, or through negotiation—explicit or implicit—among international partners? Sovereign-deference doctrines offer a sensible guidepost for the latter path. We might imagine that deferring to other states' interests is in every state's best interest when it might lead to reciprocal treatment. Rather than ask what is right or wrong in another state, deference doctrines allow courts to treat coequal sovereigns as such. They allow courts to defer to the better judgment of the sovereign without actually judging whether it *is* better. This in turn may encourage reciprocity from the courts of foreign sovereigns.[245] We might also add here an antiexceptionalism argument: data is just another globally distributed good, and as such its treatment by sovereigns and among sovereigns should abide by the usual rules of foreign affairs and international law.[246] In the final analysis, if we choose indifference to deference, and allow ideals of internet cosmopolitanism to cloud our thinking, then states will eventually assert their sovereign differences anyway, and through worse means. Very simply, the case for sovereign deference is that it represents the best possible hope for global governance of the internet.

III. THE SOVEREIGN-DEFERENCE DOCTRINES

Global internet activity creates a cross-jurisdictional problem: devising a set of rules that accommodates the overlapping and sometimes competing interests of different states in regulating internet conduct. At some level, this challenge is not a new one.[247] Since the founding of the Republic, American courts have been

245. Kramer, *supra* note 148, at 340-41.

246. Woods, *supra* note 15, at 756-63.

247. *Id.* at 764.

sensitive to the foreign affairs implications of their actions.[248] Indeed, the Framers were acutely aware of this problem and took several steps to address it.[249] Perhaps nothing in American legal jurisprudence captures this idea better than the comity doctrines—also sometimes called foreign relations doctrines[250] or international affairs doctrines.[251]

Comity is an ill-defined[252] but fundamental concept in American foreign relations law.[253] It can be broadly understood as a jurisprudential principle holding that courts should acknowledge and in some cases defer to the legitimate sovereignty interests of other states.[254] While comity is often referred to as "international comity"—to distinguish it from comity among U.S. states—it is a creature of domestic law.[255] Comity is "a sort of intercourt diplomacy long assumed to be within courts' constitutional competence."[256] As William Dodge notes, it can be defined simply as: "deference to foreign government actors that is not required by international law but is incorporated in domestic law."[257] Importantly, deference has both positive and negative elements; it requires both recognition and restraint.[258]

Comity is a judicial principle for encouraging cooperation among sovereigns.[259] There may be reasons for states not to defer to one another on certain

---

248. *See, e.g.*, Ariel N. Lavinbuk, *Rethinking Early Judicial Involvement in Foreign Affairs: An Empirical Study of the Supreme Court's Docket*, 114 YALE L.J. 855 (2005) (showing that a considerable portion of the early Court's docket was taken up with foreign affairs concerns).

249. BRADLEY & GOLDSMITH, *supra* note 14, at 4.

250. Posner and Sunstein, for example, discuss "international relations doctrines," which they divide into "comity doctrines" and "anti-comity doctrines." Posner & Sunstein, *supra* note 14, at 1173-82.

251. *Id.*

252. Michael D. Ramsey, *Escaping "International Comity,"* 83 IOWA L. REV. 893, 893 (1998) ("'International comity' is frequently invoked by courts but rarely defined with precision."); *see also* William Dodge, *supra* note 14, at 2073-75 (summarizing the widely held view that the term lacks precise definition).

253. BRADLEY & GOLDSMITH, *supra* note 14, at 4.

254. *See* Dodge, *supra* note 14, at 2078.

255. *Id.*

256. Bookman, *supra* note 13, at 1096.

257. Dodge, *supra* note 14, at 2078 (emphasis omitted).

258. *Id.* at 2078-79; *see also* Maggie Gardner, *Retiring Forum Non Conveniens*, 92 N.Y.U. L. REV. 390, 392-93 (2017) (modifying Dodge's categories slightly and emphasizing positive and negative kinds of comity).

259. *Cf.* Kramer, *supra* note 148, at 340 (proposing canons "designed to capture . . . potential gains from cooperation" in the context of conflicts of laws between U.S. states).

issues or at particular moments in time, but over the long run, with repeat interactions, states are better off if they agree as a general matter not to meddle in each others' affairs.[260] For this reason, comity doctrines have a rich history in the United States and abroad. They have developed in light of interactions between different countries' legal systems. For example, in one of Canada's leading comity cases, the Canadian Supreme Court relied on an early American comity case, *Hilton v. Guyot*,[261] to define the doctrine: "'Comity' in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation."[262]

Of course, to defer to foreign state interests, courts must take notice of them. This requires a brief examination of what counts as a legitimate state interest and how courts take notice of that interest. The *Restatement (Third) of the Foreign Relations Law of the United States* gives five classic bases for prescriptive jurisdiction.[263] Each of these is a ground for a state legitimately to pass a law or regulation, and together they provide insight into what courts have deemed to be legitimate state interests. States may legitimately prescribe law with respect to: (1) conduct that occurs within the state's territorial borders; (2) persons or things on the state's territory; (3) extraterritorial conduct that is intended to have or has substantial effects within the state's territory; (4) conduct of the state's nationals, at home and abroad; and (5) extraterritorial conduct that threatens the state's security or national interests.[264] Elsewhere, I have suggested how these five bases of jurisdiction apply to cloud services.[265]

Two of these bases are most relevant to the present discussion, as they are the primary bases for the conflicts described in Part I. Those conflicts arise where a court is hoping to protect one of its citizens and fashions an extraterritorial remedy in order to do so, as in *Equustek*.[266] They also arise where there is some extraterritorial conduct that falls within whatever territory the court happens to

260. *Id.*

261. 159 U.S. 113 (1895).

262. Spencer v. The Queen, [1985] 2 S.C.R. 278, 283 (Can.) (quoting *Hilton*, 159 U.S. at 163-64).

263. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (AM. LAW INST. 1987).

264. *Id.*

265. Woods, *supra* note 15, at 764-69.

266. Google Inc. v. Equustek Sols. Inc., [2017] 1 S.C.R. 824 (Can.).

sit in, as in *Microsoft Ireland*.[267] Notice that these categories reflect the state's interest—and this is echoed in longstanding American legal jurisprudence[268]—in conduct that has *effects* on the state, wherever that conduct occurs. The state will seek to provide remedies that maximally satisfy that interest, including extraterritorially. In the cloud context, this means that judges have a set of tools for managing and crafting cross-border data policy. Comity can be used for restraint—to refrain from stepping on another state's toes—but also for recognition—to recognize another nation's interest in a matter and extend that state's authority beyond its borders.

A. Restraint

One consequential form that comity takes is a set of doctrines of restraint.[269] With regard to production orders,[270] compulsion to testify,[271] and other potential cross-border conflict, international comity often calls for a weighing of state interests. As the Second Circuit noted, "a court of one country should make an effort to minimize possible conflict between its orders and the law of a foreign state affected by its decision."[272] Once a foreign sovereign interest is identified, courts have some discretion about how to refrain from interfering in that interest.[273] This might manifest itself in a number of different domains.

1. Remedies

One way that courts refrain from interfering with another state's sovereignty is by limiting the reach of the remedies they provide. For example, suppose that a court seeks to fashion a remedy—say an injunction—in a case where someone

267. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 855 F.3d 53 (2d Cir. 2017).

268. *See* Calder v. Jones, 465 U.S. 783, 789 (1984) (articulating an "effects" test for personal jurisdiction cases).

269. Dodge, *supra* note 14, at 2076.

270. *See, e.g.*, Linde v. Arab Bank, PLC, 706 F.3d 92, 112 (2d Cir. 2013) (holding that extraterritorial discovery orders were not inconsistent with comity where the balance of state interests weighed in favor of evidence production).

271. *See, e.g.*, United States v. Field (*In re* Grand Jury Proceedings), 532 F.2d 404, 407 (5th Cir. 1976) (embracing the "Restatement position" to balance the interests of the United States with those of the Cayman Islands, where a noncitizen was compelled to testify before a U.S. grand jury and such production would violate Caymanian bank secrecy laws).

272. United States v. First Nat'l City Bank, 396 F.2d 897, 902 (2d Cir. 1968).

273. *Id.*

claims a harm that can only be fully extinguished by a global injunction. The court must decide not only the appropriate remedy, but also its reach. In *Google Spain*, the court concluded that it had the authority to order Google to delist private information from Google's search results, not only in Google's Spanish country domain (google.es), but also in its home domain (google.com).[274] A similar issue is now pending before the CJEU.[275] *Equustek* is the same story.[276] Google disputed neither Canada's authority to hear the case, nor its authority to issue appropriate remedies, including an injunction to remove internet content. Rather, Google challenged the territorial reach of the court's remedy.[277] Recall that in this case, Google produced search results that included links to a page selling Datalink's illegal product, harming a Canadian corporation.[278] The appropriate remedy was simple enough: the court ordered Google to delist any links to the offending pages.[279] But where?

What matters, in terms of comity, is that courts restrain themselves from interfering with the legitimate interests of other states. That typically requires some limiting principle to guide the remedies that courts deploy. In the internet governance context, we can imagine three types of remedy. Comity will require a limiting principle to each one, regardless of the remedy's scope.

1. *Domain-Limited Remedy*: The court issues an injunction ordering the service provider to remove the offending material from its Canadian domain (google.ca), but not its other domains. This would allow someone sitting in Canada to find the material by visiting google.com. The limiting principle is country domain.
2. *Location-Limited Remedy*: The court issues an injunction ordering the service provider to filter out users located in Canada, and remove any offending material for those users, regardless of which Google domain they visit (google.ca or google.com). The limiting principle is user location.
3. *Comity-Limited Remedy*: The court issues a global injunction, requiring Google to remove the offending material across all of its domains and for all users, wherever they are located, except where doing so would

274. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 [https://perma.cc/Q694-URG7].

275. Scott, *supra* note 10.

276. Google Inc. v. Equustek Solutions, Inc., [2017] 1 S.C.R. 824 (Can.).

277. *Id.*

278. *Id.* at 825.

279. *Id.* at 826.

> conflict with the laws or interests of other states. The limiting principle is conflict with other nations' interests.

The first remedy is the least satisfactory because it does not accomplish what the court seeks: to protect the rights of Equustek by not allowing Datalink to sell its infringing products, especially in Canada. Suppose that a user in Canada hoped to buy one of the Datalink products. All she would need to do is visit www.google.com from her computer in Canada.[280] This is not an effective solution from the standpoint of remedying the harm posed to Equustek, the Canadian firm.

A location-based remedy is preferable to a domain-specific remedy because the state's core interest is ensuring that whatever rules it adopts are enforced within its territory.[281] Under this approach, the service provider takes steps to identify the location of its users and to deliver a product that complies with the law where the user is located.[282] One standard critique of such a system is that the firm might struggle to identify its users' locations.[283] However, it is fairly easy for internet firms accurately to locate the vast majority of their users.[284] Indeed, much internet advertising is location-based, suggesting that it can be done successfully. After all, location-based advertising would not have much value if the locations were all wrong.[285] Another possible critique of a location-based remedy is that it, too, can be evaded. To be sure, determined internet users can deploy virtual private networks and other anonymization tools that circumvent the firm's system for identifying user location.[286] And while a relatively small

---

280. Woods, *supra* note 79.

281. As the *Restatement* suggests, the link between territory and jurisdiction is fundamental. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 reporters' notes (AM. LAW INST. 1987).

282. This is increasingly feasible. *See, e.g.*, Nihar Bihani, *Geo-Blocking Content with Amazon CloudFront*, AWS NEWS BLOG (Jan. 19, 2012), https://aws.amazon.com/blogs/aws/guest-post-geo-blocking-content-with-amazon-cloudfront [https://perma.cc/R9KB-5KMG].

283. Woods, *supra* note 79.

284. *Id.*

285. *See* Lauren Johnson, *Are Marketers Finally Getting the Hang of Location-Based Ads?*, ADWEEK (Sept. 28, 2015), http://www.adweek.com/digital/are-marketers-finally-getting-hang-location-based-mobile-ads-167212 [https://perma.cc/A7DK-ZACU].

286. *See, e.g.*, *What Is Geo Blocking and Are There Ways to Get Around It?*, QUORA, https://www.quora.com/What-is-geo-blocking-and-are-there-ways-to-get-around-it [https://perma.cc/RV6R-5AWJ].

portion of internet users actually use such tools,[287] these are precisely the users that a firm might legitimately be worried about. But this is not an insurmountable problem: internet firms have tools to combat location masking, and they regularly use these tools in order to comply with licensing arrangements for music, books, and movies.[288]

When France and Spain asked Google to take down search results in accordance with the Right to be Forgotten, Google initially resisted.[289] After losing the jurisdictional argument in court, the firm offered the first remedy: it agreed to take down the material at issue only on the country-specific domains (Google.es and Google.fr).[290] This did not satisfy the data authorities,[291] and after some back-and-forth, Google relented.[292] Today, in order to comply more fully with the French and Spanish regulations regarding the Right to be Forgotten, Google deploys a user-location based product in Europe. That is, Google geo-blocks the material that users have requested be delisted, but only for users located in Europe. This, however, did not satisfy the French data authorities, who referred the matter to Europe's top court to decide whether Google must instead implement the third remedy, a global takedown.[293]

The state, naturally, may prefer the third remedy if it maximally protects its interests. If Canada attempts to secure the interests of a Canadian citizen by prescribing certain conduct, then it has a recognized interest in prescribing that conduct everywhere.[294] As the *Equustek* court explained:

---

287. VPNs are used by around a quarter of internet users, typically to access out-of-market content. Olivia Valentine, *VPN Usage Around the World in 2018*, GLOBAL WEB INDEX (July 2, 2018), https://blog.globalwebindex.com/chart-of-the-day/vpn-usage-2018 [https://perma.cc/3KEY-5VBA].

288. Zach Epstein, *Netflix Is Winning a War It Doesn't Even Want to Fight*, BOY GENIUS REP. (Oct. 17, 2016, 5:16 PM), http://bgr.com/2016/10/17/netflix-vpn-ban-fix-sites-giving-up [https://perma.cc/HWH9-28S8].

289. Jens-Henrik Jeppesen & Emma Llansó, *EU's "Right to Be Forgotten" Policy Sets Bad Precedent for Free Expression Worldwide*, CTR. FOR DEMOCRACY & TECH.: BLOG (Feb. 11, 2016), https://cdt.org/blog/eus-right-to-be-forgotten-policy-sets-bad-precedent-for-free-expression-worldwide [https://perma.cc/6VRL-V6KD].

290. *Id.*

291. *Id.*

292. Peter Fleischer, *Adapting Our Approach to the European Right to Be Forgotten*, GOOGLE BLOG (Mar. 4, 2016), https://www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig [https://perma.cc/DYZ9-QZPG].

293. Request for a Preliminary Ruling from the Conseil d'État (France), Case C-507/17, Google Inc. v. Commission Nationale de l'Informatique et des Libertés (CNIL), 2017 O.J. (C 347) 30.

294. Recall that one of the standard bases for asserting prescriptive jurisdiction is to prescribe law with respect to "the activities, interests, status, or relations of its nationals outside as well as

> Where it is necessary to ensure the injunction's effectiveness, a court can grant an injunction enjoining conduct anywhere in the world. The problem in this case is occurring online and globally. The Internet has no borders – its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates – globally.[295]

But can Canadian courts ensure the enforcement of their injunctions elsewhere? Certainly not. That depends on how comity principles are deployed in the forum state where the injunction is challenged. As we will see, global injunctions are not necessarily inconsistent with comity.[296] The point is that even with the cross-border cloud, courts can fashion cross-border remedies that contain built-in restraints. They have wide latitude in fashioning these remedies, and they often will do so with an eye toward other sovereigns, or they will not but the remedy will nonetheless be limited unilaterally by that sovereign.

2. Production Orders

Microsoft Ireland[297] – like several cases since[298] – is fundamentally about the reach of production orders across borders. Here, law enforcement agents seek access to data stored overseas and obtain a production order, like a subpoena, 2703(d) order, search warrant, or some other kind of legal process.[299] The question is then whether the order compels the production of foreign-held data.

---

within its territory." RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (AM. LAW INST. 1987).

295. Google Inc. v. Equustek Sols. Inc., [2017] 1 S.C.R. 824, 827 (Can.).

296. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 482(2)(d) (AM. LAW INST. 1987).

297. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 855 F.3d 53 (2d Cir. 2017).

298. *In re* the Search of Info. Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757(GMH), 2017 WL 2480752 (D.D.C. June 2, 2017); *In re* the Search of Content that Is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, 2017 WL 1398279 (N.D. Cal. Apr. 19, 2017); *In re* the Search of Premises Located at [Redacted]@yahoo.com, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017); *In re* Information Associated with One Yahoo Email Address that Is Stored at Premises Controlled by Yahoo, No. 17-M-1234, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017); *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708 (E.D. Pa. 2017).

299. Woods, *supra* note 15, at 745.

Comity could limit the way that such orders operate by asking a court to consider the possibility that a production order implicates another state's interest in the data not being produced.[300] So far, comity has played a relatively small role in the court battles over digital production. Only one brief in the *Microsoft Ireland* case called attention to the issue.[301] Because the court decision turned on statutory interpretation and the court's use of the presumption against extraterritoriality, it did not need to address the comity argument explicitly.

But it could have. Indeed, it would not be surprising to see a court use comity to resolve a dispute about the reach of a cross-border production order. If a magistrate judge issued an ECPA order[302] that compelled a provider to deliver information that plainly violated the laws of another country, a federal judge might be open to modifying the order so as to avoid the conflict of laws. In *Linde v. Arab Bank*,[303] the Second Circuit acknowledged that production orders can be curtailed out of a concern for international sovereign interests[304]:

> We observe that when weighing the conflicting legal obligations of U.S. discovery orders and foreign laws, "[m]echanical or overbroad rules of thumb are of little value; what is required is a careful balancing of the interests involved and a precise understanding of the facts and circumstances of the particular case."[305]

This balancing of interests is not simply an inquiry into whether the judicial action in question creates a conflict of laws or puts a party at risk of foreign criminal sanctions.[306] Rather, the inquiry requires weighing "(on the one hand) the interests of foreign governments in enforcing their laws and the potential hardship [on the burdened party],"[307] against "(on the other hand) the interests of the

---

300. This is essentially the argument Apple made in its amicus brief, although it did not identify a compelling government interest in favor of limiting the reach of the production order. Brief for Apple, Inc. as Amicus Curiae Supporting Appellant at 10-14, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

301. *Id.*

302. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2222, 2701-2712, 3121-3127 (2018)).

303. 706 F.3d 92 (2d Cir. 2013).

304. *Id.* at 108.

305. *Id.* (quoting United States v. First Nat'l City Bank, 396 F.2d 897, 901 (2d Cir. 1968)).

306. *Id.* ("We would be reluctant to hold . . . that the mere absence of criminal sanctions abroad necessarily mandates obedience to a subpoena. Such a rule would show scant respect for international comity.").

307. *Id.* at 98.

United States in enforcing its laws and plaintiffs' need for the material in pursuing their claims."[308]

Courts conduct this balancing test with reference to five factors:[309]

> [T]he importance to the . . . litigation of the documents or other information requested; the degree of specificity of the request; whether the information originated in the United States; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.[310]

The court in *Linde* ultimately concluded that the order did not offend international comity because comity requires not absolute deference, but rather respect and a balancing of national interests.[311] There is often room in comity analysis for permission seeking.[312] The *Restatement (Third) of the Foreign Relations Law of the United States* notes that "a court or agency in the United States may require the person to whom the order is directed to make a good faith effort to secure permission from the foreign authorities to make the information available."[313] We could imagine, then, in the cloud context, that courts would be skeptical of claims by companies that cross-border production orders were likely to harm foreign government interests, where those service providers did not make a good-faith effort to ask permission from the relevant state first.

3. Statutory Interpretation

Another way courts refrain from interfering with another sovereign's authority is by interpreting vague laws in ways that do not offend comity.[314] For example, the *Charming Betsy* canon of construction—by which courts interpret

---

308. *Id.*

309. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 (AM. LAW INST. 1987).

310. *Id.* § 442(1)(c).

311. 706 F.3d at 111.

312. *Id.* at 99.

313. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 442(2)(a) (AM. LAW INST. 1987).

314. *See* Edward T. Swaine, *Cooperation, Comity, and Competition Policy: United States*, *in* COOPERATION, COMITY, AND COMPETITION POLICY 3, 13 (Andrew T. Guzman ed., 2011) ("[T]he Supreme Court is receptive to comity when presented as a tool for statutory construction.").

ambiguous statutes in ways that do not violate international law[315]—is one example of an interpretive rule that operates as a form of prescriptive comity.[316] So an internet service provider served with an order to produce emails stored abroad, issued under a statute like the SCA, might argue that doing so would contravene the territorial sovereignty of another state, and *that* is a violation of traditional notions of territorial sovereignty under international law.[317] Indeed, Microsoft made precisely this argument before the Second Circuit, noting: "The imperative to preserve the territorial integrity of foreign nations is so strong that it provides an independent basis on which to invalidate the Warrant."[318] This argument may or may not be convincing as a matter of international law—the customary international law regarding cross-border internet activity is unsettled—but the point of the canon is clear. Rather than argue for a particular interpretation of the statutory presumption in favor of or against extraterritorial application, the *Charming Betsy* canon asks courts to find ways of interpreting vague statutes in ways that do not violate international law.

B. Recognition

Comity can also mean more than restraint and may instead involve active recognition and outright enforcement of the interests of another state. This can take a number of different forms.

---

315. Murray v. Schooner Charming Betsy, 6 U.S. (2 Cranch) 64, 118 (1804) ("[A]n act of Congress ought never to be construed to violate the law of nations if any other possible construction remains . . . .").

316. Hartford Fire Ins. Co. v. California, 509 U.S. 764, 817 (1993) (Scalia, J., dissenting in part) (identifying the *Charming Betsy* rule of construction as deriving from a principle of "prescriptive comity"). *But see* Dodge, *supra* note 14, at 2076 n.37 (noting that "the *Charming Betsy* canon . . . is not really a comity doctrine").

317. *See* Brief for Appellant, *supra* note 150, at 33-35.

318. *Id.* at 34.

1. *Enforcement of Judgments*

American courts regularly recognize the court judgments of a foreign sovereign,[319] but not always. There is no federal statute that requires courts to recognize foreign judgments,[320] so the determination typically depends on the state law relevant to the case.[321] Enforcing foreign judgments is something courts do out of a sense of comity,[322] and as we have seen, comity hardly imposes a firm obligation on courts.[323]

Consider two examples. When a French court held that Yahoo! had to remove Nazi memorabilia from its French pages, Yahoo! brought suit in a U.S. court, asking the court whether it would enforce the French judgment.[324] The court, in order to determine whether to enforce the order, looked "to general principles of comity followed by the California courts."[325] Google took a similar step in its dispute with Equustek over the global injunction issued.[326] It asked a court to determine preemptively that Equustek would not be able to enforce the injunction granted a month earlier by the Canadian Supreme Court, on the grounds that the injunction would violate international comity.[327] Much like the Yahoo! litigation, this case has an odd posture: Google is relying on comity—a doctrine of deference to foreign sovereigns—in order to justify *not* deferring to the judgment of a foreign sovereign.[328] It would be more consistent with the

319. *See, e.g.*, Ungaro-Benages v. Dresdner Bank AG, 379 F.3d 1227 (11th Cir. 2004); Ingersoll Milling Mach. Co. v. Granger, 833 F.2d 680 (7th Cir. 1987). *But see* Matusevitch v. Telnikoff, 877 F. Supp. 1 (D.D.C. 1995) (choosing not to enforce a libel judgment from the United Kingdom on the grounds that doing so would contravene free speech policy in the United States); Bachchan v. India Abroad Publ'ns Inc., 585 N.Y.S.2d 661 (Sup. Ct. 1992) (same).

320. *See* FOREIGN JUDGMENTS RECOGNITION & ENF'T ACT (AM. LAW INST., Proposed Final Draft 2005).

321. Yahoo! Inc. v. La Ligue Contre Le Racisme Et l'Antisemitisme, 433 F.3d 1199, 1213 (9th Cir. 2006) (en banc) (per curiam) ("In a typical enforcement case, the party in whose favor the foreign judgment was granted comes to an American court affirmatively seeking enforcement. The standard rule in such a case is that the federal court sitting in diversity applies the law of the state in which it sits.").

322. Dodge, *supra* note 14, at 2072.

323. *See id.* at 2125-27.

324. *Yahoo! Inc.*, 433 F.3d at 1212-13.

325. *Id.* at 1213.

326. *See* Complaint, *supra* note 7, at 5-6, 12.

327. *Id.*

328. *See* Andrew Keane Woods, *Google Takes the Global Delisting Debate to a U.S. Court*, LAWFARE (July 27, 2017, 2:28 PM), https://lawfareblog.com/google-takes-global-delisting-debate-us-court [https://perma.cc/Z4US-765H].

logic of comity for Equustek to ask a U.S. court to find that comity calls for recognizing and enforcing the Canadian injunction.[329]

We might imagine the same thing occurring in other contexts, too. For example, suppose that a Brazilian court demands that an American intermediary produce customer data as part of a civil lawsuit, and the firm refuses to comply.[330] Brazil might make an application to a U.S. court to enforce the judgment, and comity would counsel the court to take a serious look at the order and consider whether to recognize and enforce it.[331]

2. Sovereign Compulsion

The sovereign-compulsion doctrine—perhaps best known in antitrust law[332]—is another doctrinal tool for courts to recognize sovereign interests, albeit indirectly. Under the doctrine, courts "have discretion to excuse violations of U.S. law, or moderate the sanctions imposed for such violations, on the ground that the violations are compelled by another state's law," where the party in question would suffer severe consequences if they did not comply with the foreign law and where they acted in good faith to avoid the conflict.[333] In *Interamerican Refining Corp. v. Texaco Maracaibo, Inc.*, a federal district court accepted the defendants' argument that foreign law—in this case Venezuelan law—prohibited them from delivering oil to the plaintiff, thereby releasing the defendants of liability.[334] The logic of the foreign-state compulsion doctrine extends to any number of internet disputes. Suppose, for example, that Brazil forces Google to

---

329. *Id.*

330. Brazil detained a Microsoft executive for exactly that. Brad Smith, *In the Cloud We Trust*, MICROSOFT, https://news.microsoft.com/stories/inthecloudwetrust [https://perma.cc/RY8Z-2MY7].

331. This hypothetical is a civil lawsuit, but we might imagine comity principles similarly informing a country's implementation of an MLAT in order to render assistance in a criminal investigation. Further, there is some evidence that the so-called public law taboo is eroding in foreign affairs law. *See* William S. Dodge, *Jurisdiction in the Fourth Restatement of Foreign Relations Law*, 18 Y.B. PRIV. INT'L L. 143, 167-68 (2017).

332. *See* Steven A. Kadish, *Comity and the International Application of the Sherman Act: Encouraging the Courts to Enter the Political Arena*, 4 NW. J. INT'L L. & BUS. 130, 138 (1982) (noting that the sovereign compulsion doctrine "insulates parties from liability under the antitrust laws when the challenged activity was compelled or required by a foreign government").

333. RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW: JURISDICTION § 222 (AM. LAW INST., Tentative Draft No. 2, 2016).

334. 307 F. Supp. 1291, 1296 (D. Del. 1970).

produce data in violation of ECPA. The sovereign-compulsion doctrine could relieve Google of liability.[335]

C. Encouraging Comity

Deference to foreign sovereigns largely stems from a recognition that states are part of an international system that depends in part on noninterference and mutual respect.[336] Comity is not only a consequence of that fact but also a cause. Accordingly, courts take a number of steps to actively encourage comity.

1. Resisting Blocking Statutes

Blocking statutes, which prohibit compliance with another country's laws, might be considered anticomity statutes.[337] For this reason, they are often not given the same deference as other statutes, and courts have developed antiblocking-statute norms. For example, courts that typically defer to state interests may decline to do so where that state has passed blocking laws deliberately in order to frustrate extraterritorial orders.[338] As the Supreme Court found in *Société Nationale Industrielle Aérospatiale v. United States District Court*,[339] blocking statutes are not due the same deference as other substantive rules.[340] The Court noted:

> The lesson of comity is that neither the discovery order nor the blocking statute can have the same omnipresent effect that it would have in a world of only one sovereign. The blocking statute thus is relevant to the court's particularized comity analysis only to the extent that its terms and

---

335. The flipside of this, as we will see, is that states sometimes refuse to grant another state the benefit of comity where that state has adopted a blocking statute. ECPA is one such statute.

336. Dodge, *supra* note 14, at 2085-86 (describing comity's intellectual roots and noting that sovereign deference is essential for the Westphalian system, which is made up of states whose sovereignty depends in part on noninterference in each other's affairs).

337. Posner and Sunstein catalog a series of anticomity doctrines—doctrines that privilege parochial interests at the expense of foreign-state interests. Posner & Sunstein, *supra* note 14, at 1182 ("[A]nti-comity doctrines assert American interests in the context of international relations, potentially or actually at the expense of the interests of other countries.").

338. *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)).

339. 482 U.S. 522 (1987).

340. *Id.* at 539-40, 544 n.29.

> its enforcement identify the nature of the sovereign interests in nondisclosure of specific kinds of material.[341]

The logic of *not deferring* to foreign blocking statutes in a regime that otherwise recognizes and defers to foreign interests is consistent with encouraging comity. Courts seek to make room for legitimate foreign interests and hope foreign courts will do the same, but not where legislatures have attempted to take advantage of comity rules.[342] It could have considerable effects on cross-border internet disputes for courts to ignore blocking statutes—especially given the significance of ECPA's blocking features around the world.[343]

2. Reciprocity

The idea of comity is rooted, at some level, in reciprocity and mutual accommodation.[344] Justice Blackmun, in his concurrence in *Aérospatiale*, noted that "[c]omity is not just a vague political concern favoring international cooperation when it is in our interest to do so. Rather it is a principle under which judicial decisions reflect the systemic value of reciprocal tolerance and goodwill."[345] That is, courts are mindful of the fact that their orders do not occur in a vacuum and that they are taken seriously by the courts of other countries. "The lesson of comity," the Court said in *Aérospatiale*, "is that neither the discovery order nor the blocking statute can have the same omnipresent effect that it would have in a world of only one sovereign."[346]

Courts can elect to recognize and defer to foreign interests *to the extent that* another state is willing to do the same.[347] This does not always work,[348] though,

---

341. *Id.* at 545.

342. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 reporters' note 5 (AM. LAW INST. 1987) ("[Blocking statutes] need not be given the same deference by courts of the United States as differences in substantive rules of law.").

343. *See* Woods, *supra* note 15, at 779.

344. *See* Gardner, *supra* note 258, at 392–93.

345. *Aérospatiale*, 482 U.S. at 555 (Blackmun, J., concurring in part and dissenting in part).

346. *Id.* at 545 n.29 (majority opinion).

347. *See* Dodge, *supra* note 14, at 2081 n.49.

348. John F. Coyle, *Rethinking Judgments Reciprocity*, 92 N.C. L. REV. 1109, 1169 (2014) ("If a policy of judgments reciprocity is unlikely to persuade the nations that currently refuse to enforce U.S. judgments to change their practice—as seems to be the case—then the answer to the question of whether to adopt such a policy is easy.").

and reciprocity is uncommon with respect to the enforcement of foreign judgments.[349] But the practice has a long pedigree.[350] It may especially make sense in the cloud context, where each state is attempting to design novel and sometimes comprehensive internet regulations. This is precisely the idea behind the proposed U.S.-U.K. agreement, the first of many such agreements provided for by the CLOUD Act. It grants law enforcement access to those countries that strike a deal with the United States, on the theory that such a deal will grant reciprocal law enforcement access to data held abroad.[351] Reciprocity may or may not be seen as comity-enhancing depending on the circumstances. In the case of ECPA, which acts as a blocking statute preventing most states from being able to compel American providers to produce evidence, a reciprocity requirement shows less deference to other sovereigns than merely removing the blocking statute altogether. In other contexts, though, we could imagine reciprocal increases in sovereign deference playing a crucial role. Indeed, this is part of the motivation for PPD-28, which guarantees similar baseline privacy protections for citizens and noncitizens alike.[352] Privacy Shield is built on a foundation of reciprocal privacy protections, and without that reciprocity, it would likely fail.[353]

IV. WHAT SOVEREIGN DEFERENCE DOES NOT PRECLUDE

Comity does sometimes counsel against extraterritoriality. It can be used by states to refrain from extending a ruling that interferes with another state's interests. But sometimes it cuts exactly the other way and calls for courts to give a foreign court's orders extraterritorial reach.[354] When a court issues a ruling with

349. *See* RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES: JURISDICTION § 404 reporters' note 11 (AM. LAW INST., Tentative Draft No. 1, 2014).

350. *See* Dodge, *supra* note 14, at 2081 n.49 (noting a century-old reciprocity rule for the enforcement of foreign judgments).

351. Jennifer Daskal & Andrew Keane Woods, *Congress Should Embrace the DOJ's Cross-Border Data Fix*, LAWFARE (Aug. 1, 2016, 8:52 AM), http://www.lawfareblog.com/congress-should-embrace-dojs-cross-border-data-fix-0 [https://perma.cc/7Z3S-32DG].

352. Press Release, White House, Presidential Policy Directive – Signals Intelligence Activities § 4 (Jan. 17, 2014), http://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/S93P-GHCE].

353. *See* Cobun Keegan, *Calm Down: Trump Hasn't Tanked Privacy Shield Just Yet*, IAPP: PRIVACY TRACKER (Jan. 27, 2017), http://iapp.org/news/a/calm-down-trump-hasnt-tanked-privacy-shield-just-yet [https://perma.cc/LJT4-J7HQ].

354. *See* Cameron Kerry & Alan Charles Raul, *The Economic Case for Preserving PPD-28 and Privacy Shield*, LAWFARE (Jan. 17, 2017, 3:19PM), http://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield [https://perma.cc/2VC6-5LCE].

effects in another state, the aggrieved party will often ask the other state to enforce the ruling. Courts recognize and enforce foreign judgments—giving them extraterritorial bite—in the name of comity. In other words, courts recognize that state interests extend beyond borders.

A. Extraterritorial Production Orders

Not all exercises of extraterritorial jurisdiction are incompatible with foreign sovereign interests. Even where they are in tension, courts need not defer completely to the foreign sovereign interest if it is outweighed by the domestic interest.[355] This is not reflected in the briefing of some of the highest-profile internet disputes today. For example, *Microsoft Ireland* was wrongheaded for many reasons—as has been discussed elsewhere[356]—but perhaps most strikingly, it was wrong from a comity perspective. As noted above, Apple's amicus brief argued that comity concerns cautioned against the court applying ECPA extraterritorially.[357] This is almost certainly wrong, at least in this case, but probably also beyond it. Comity requires a concern for other states' interests, which can be asserted directly or considered by the court sua sponte.[358] But that interest is not necessarily inconsistent with the extraterritorial application of another state's laws. To be sure, a presumption against extraterritorial jurisdiction can sometimes be consistent with comity. The Supreme Court has observed that the goal behind the presumption against extraterritoriality is "to protect against unintended clashes between our laws and those of other nations which could result in international discord."[359] To the extent the presumption achieves this goal, it

---

355. *See* Eric Roberson, *Comity Be Damned: The Use of Antisuit Injunctions Against the Courts of a Foreign Nation*, 147 U. PA. L. REV. 409, 421-22 (1998).

356. *See, e.g.*, Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, WASH. POST: VOLOKH CONSPIRACY (Nov. 29, 2016), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case [https://perma.cc/3LQ2-6ZSR]; Jennifer Granick, *The Microsoft Ireland Case and the Future of Digital Privacy*, JUST SECURITY (July 18, 2016), http://www.justsecurity.org/32076/microsoft-ireland-case-future-digital-privacy [https://perma.cc/6MQ9-UZH9].

357. Brief in Support of Appellant Microsoft, Inc. by Apple Inc. as Amicus Curiae, *supra* note 18, at 10-14.

358. Brewer v. Marshall, 119 F.3d 993, 999 (1st Cir. 1997) (noting that the district court raised comity sua sponte)*; see also* Katherine A. MacFarlane, *Adversarial No More: How Sua Sponte Assertion of Affirmative Defenses to Habeas Wreaks Havoc on the Rules of Civil Procedure*, 91 OR. L. REV. 177, 198 (2012) (noting how courts raise arguments sua sponte out of a concern for comity).

359. EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991) (citing McCulloch v. Sociedad Nacional de Marineros de Honduras, 372 U.S. 10, 20-22 (1963)).

is consistent with comity. Nevertheless, extraterritorial assertions of authority over the cloud are not, by the same token, inconsistent with comity.

That is, the presumption against extraterritoriality—often treated as a comity doctrine—is not in fact necessary for comity.[360] As we have seen, one state's internet regulations may raise many cross-border issues.[361] Fortunately, the solutions to these problems are often cross-border as well and often in ways that are harmless from the perspective of another state's interests. As the Supreme Court said in *F. Hoffman-La Roche Ltd v. Empagran S.A.*[362]:

> No one denies that America's antitrust laws, when applied to foreign conduct, can interfere with a foreign nation's ability independently to regulate its own commercial affairs. But our courts have long held that application of our antitrust laws to foreign anticompetitive conduct is nonetheless reasonable, and hence consistent with principles of prescriptive comity, insofar as they reflect a legislative effort to redress *domestic* antitrust injury that foreign anticompetitive conduct has caused.[363]

Comity requires the courts to weigh competing government interests, but it does not per se prohibit regulation of extraterritorial conduct.

Indeed, it is increasingly difficult to regulate domestic conduct in ways that do not have extraterritorial effects. The presumption against extraterritoriality is falling out of favor with scholars largely for the same reasons: in a globally connected world where many businesses are transnational, we can no longer assume that laws should not apply across borders.[364] In this vein, Zachary Clopton noted that "[t]he presumption against extraterritoriality rose in an era in which territoriality was more central to international law and conflict of laws than it is today, not to mention a time in which the nature, scope, and quantity of extraterritorial regulation was significantly different."[365]

---

360. *See* Clopton, *supra* note 36, at 11-12.

361. *See supra* Part I.

362. 542 U.S. 155 (2004).

363. *Id.* at 165.

364. *See* Larry Kramer, *Vestiges of Beale: Extraterritorial Application of American Law*, 1991 SUP. CT. REV. 179, 184 ("[T]he world in which a presumption against extraterritoriality made sense is gone.").

365. Clopton, *supra* note 36, at 10.

In fact, in some cases, applying one country's laws extraterritorially may be precisely the best way to accommodate another sovereign's interests.[366] Imagine, for example, that two countries worked together to solve a cross-border problem like a botnet—a network of computers infected with a program that allows them to be remotely controlled.[367] Suppose that each country has a choice between: (a) applying its laws territorially and ordering that providers take down websites that contain infected material, but *only* those websites with servers that operate on the country's soil; or (b) applying its laws extraterritorially and aiming to take down the websites and their servers wherever they are located. Option (b) may be preferable for any state that is affected by the bot. Indeed, one could imagine another country weighing in to alert the court that there is no need to hesitate for the sake of comity and that, to the contrary, the best way to satisfy that country's security interests would be to pursue the farthest-reaching remedy possible.[368]

B. Global Injunctions

Another relevant issue is the issuance of "global" injunctions, like the one in *Equustek*. The primary argument against these injunctions is that they are inconsistent with comity.[369] As Google noted in its complaint: "Foreign courts . . . ordinarily refrain from issuing worldwide injunctions because they only have jurisdiction to prescribe conduct that, wholly or in substantial part, takes place within or affects their own territories."[370]

---

366. *See* Hilton v. Guyot, 159 U.S. 113, 163 (1895) (calling comity "[t]he extent to which the law of one nation, as put in force within its territory, whether by executive order, by legislative act, or by judicial decree, shall be allowed to operate within the dominion of another nation").

367. *What Is a Botnet?*, CLOUDFLARE, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet [https://perma.cc/A9NN-844E]. This sort of cross-border cooperation is increasingly common. Microsoft recently worked with law enforcement agents around the world to remove a botnet that had infected millions of computers. Cory Bennett, *Officials Break Up Global Ring of 1m Infected Computers*, HILL (Dec. 4, 2015, 9:15 AM EST), https://thehill.com/policy/cybersecurity/262087-officials-break-up-global-ring-of-infected-computers [https://perma.cc/B48X-PRDX].

368. *See* Ralf Michaels, Empagran*'s Empire: International Law and Statutory Interpretation in the U.S. Supreme Court of the Twenty-First Century*, *in* INTERNATIONAL LAW IN THE U.S. SUPREME COURT: CONTINUITY AND CHANGE 533, 544 (David L. Sloss et al. eds., 2011) ("Cases from *The Antelope* through *Empagran* suggest that the *refusal* to apply law extraterritorially—especially regarding conduct that is almost universally condemned (slavery, price-fixing)—can also be a problem . . . .").

369. Complaint, *supra* note 7, at 11.

370. *Id.*

This is wrong. Comity requires weighing another country's interests and little more.[371] Indeed, courts have historically issued antisuit injunctions—which are effectively global injunctions—preventing litigants from pursuing their rights in other jurisdictions.[372] The idea behind these global injunctions is simple: courts hope to prevent duplicative lawsuits.[373] The issuance of these injunctions requires consideration of other nations' interests. "When a preliminary injunction takes the form of a foreign antisuit injunction, we are required to balance domestic judicial interests against concerns of international comity."[374]

Recall the *Equustek* court's global injunction, which, despite a great deal of consternation about its reach, did in fact explicitly embrace a limiting principle consistent with comity.[375] The court noted:

> Google's argument that a global injunction violates international comity because it is possible that the order could not have been obtained in a foreign jurisdiction, or that to comply with it would result in Google violating the laws of that jurisdiction, is theoretical. If Google has evidence that complying with such an injunction would require it to violate the laws of another jurisdiction, including interfering with freedom of expression, it is always free to apply to the British Columbia courts to vary the interlocutory order accordingly. To date, Google has made no such application.[376]

---

371. This is especially true of injunctions. Exactly how much discretion courts have depends on which international comity doctrine is being invoked. Enforcement of foreign judgments in civil cases, for example, leaves courts with less flexibility than other comity doctrines. *See* Dodge, *supra* note 14, at 2083 (referring to the rules of enforcement of foreign judgments as "nondiscretionary").

372. *See* BRADLEY & GOLDSMITH, *supra* note 14, at 114 ("Occasionally, U.S. courts will do essentially the opposite of international abstention: they will issue a so-called anti-suit injunction to prevent persons or entities subject to their personal jurisdiction from pursuing litigation in foreign tribunals.").

373. *Id.*

374. Karaha Bodas Co. v. Perusahaan Pertambangan Minyak Dan Gas Bumi Negara, 335 F.3d 357, 366 (5th Cir. 2003); *see also* Quaak v. Klynveld Peat Marwick Goerdeler Bedrijfsrevisoren, 361 F.3d 11, 17 (1st Cir. 2004) (noting that courts "must take account of considerations of international comity" when evaluating whether to grant an antisuit injunction); Laker Airways Ltd. v. Sabena, Belgian World Airlines, 731 F.2d 909, 926-27 (D.C. Cir. 1984) (noting that the decision to grant or deny an antisuit injunction requires examination of the "equitable circumstances" in each case).

375. Woods, *supra* note 79.

376. Google Inc. v. Equustek Sols. Inc., [2017] 1 S.C.R. 824, 827-28 (Can.).

The court invited a comity analysis, but there was no need for one, because there was no conflict of laws and indeed no conflict with another nation's sovereign interests.[377] Comity only requires *asking* whether there is a sovereign interest at stake and *asking* whether it is worth deferring to that interest.[378] Where states assert an interest in the case, comity does not dictate that courts defer automatically or in full to that interest; it merely requires that they seriously consider the state's asserted interest.[379]

In the internet context, observers fear that countries might unilaterally impose worldwide their vision for the internet. China, for example, could issue an order requiring that apps scrub any mention of Tibet wherever they operate, both in and out of China.[380] However, such an action is unlikely to survive in a comity-based regime. First, China would need to have personal jurisdiction over the app provider, and a court might decline (for comity reasons) to find that it has that jurisdiction.[381] Second, a foreign court might have to decide whether it has the authority to enforce a global injunction. This can cut in both directions. We have seen that enforcement of foreign judgments is a comity doctrine,[382] and the logic of comity runs *in favor* of recognizing foreign actors and judgments,

---

377. A conflict with another nation's laws is not the only relevant question in a comity analysis, but it can be dispositive. *See* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 798-99 (1993) (finding that "international comity" did not call for exercising jurisdiction where no conflict of laws existed).

378. *See* ULRICH HUBER, DE CONFLICTU LEGUM DIVERSARUM IN DIVERSIS IMPERIIS [OF THE CONFLICT OF DIVERSE LAWS IN DIVERSE GOVERNMENTS] (1689), *translated in* Ernest G. Lorenzen, *Huber's* De Conflictu Legum, 13 ILL. L. REV. 375, 403 (1919) ("Sovereigns will so act by way of comity that rights acquired within the limits of a government retain their force everywhere so far as they do not cause prejudice to the power or rights of such government or of its subjects.").

379. Animal Sci. Prods., Inc. v. Hebei Welcome Pharm. Co., 138 S. Ct. 1865, 1873 (2018) (holding that comity counsels courts to "carefully consider a foreign state's views about the meaning of its own laws" but that "a federal court is neither bound to adopt the foreign government's characterization nor required to ignore other relevant materials").

380. *See, e.g.*, *China: World Leader of Internet Censorship: Oral Statement at the 17th Session of the Human Rights Council*, HUM. RTS. WATCH (June 3, 2011, 9:30 AM EDT), https://www.hrw.org/news/2011/06/03/china-world-leader-Internet-censorship [https://perma.cc/93PA-CBJ6].

381. See, *e.g.*, Royal & Sun All. Ins. Co. of Can. v. Century Int'l Arms, Inc., 466 F.3d 88, 92-97 (2d Cir. 2006) (applying international comity abstention). *But see* RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES: JURISDICTION § 304 reporters' note 3 (AM. LAW INST., Tentative Draft No. 2, 2016) (suggesting that the Supreme Court has never explicitly endorsed these doctrines).

382. *See supra* Section III.B.

not against them.[383] It would be an odd result for a court to decide *not* to recognize another state's judgment out of a concern for comity. For example, in its cross-border litigation over a delisting order, Google argued that comity runs both ways. In Canada, Google argued that comity required the country not to extend its ruling abroad.[384] This argument, whatever its merits, was consistent with the logic of comity. States occasionally restrict the jurisdictional reach of their judgments in order not to offend another state's sovereignty.[385] Elsewhere, they recognize another state's judgments, giving those judgments extraterritorial effect, out of a concern for ensuring that foreign state's sovereign interests.[386] But the logic of comity does *not* compel a court to decline to enforce a foreign judgment out of respect for that foreign nation's sovereignty. Indeed, declining to enforce the order would have the opposite effect.

Yet while comity calls for enforcing a foreign judgment, states can also, *despite comity*, decline to enforce a foreign judgment because to do so would contravene some legitimate state interest. As the *Restatement* notes, American courts will not enforce a foreign judgment where "the cause of action on which the judgment was based, or the judgment itself, is repugnant to the public policy of the United States or of the State where recognition is sought."[387] Even if China passed the law forbidding apps from mentioning Tibet and attempted to enforce it globally, it could not succeed in enforcing that law in any country that has a similar public-policy exception to general comity principles. Courts in those countries would entertain challenges that China's order simply interferes too much with laws or interests in those states. As the Ninth Circuit pointed out in Yahoo!'s challenge to a French regulation regarding the sale of Nazi memorabilia, courts will not enforce foreign judgments where doing so would be fundamentally repugnant to the state's public policies.[388] The court noted that "[i]nconsistency with American law is not necessarily enough to prevent recognition and enforcement of a foreign judgment in the United States. The foreign judgment must be, in addition, repugnant to public policy."[389]

---

383. *See* Dodge, *supra* note 14, at 2074; *see also* The Sapphire, 78 U.S. (11 Wall.) 164, 167 (1870) (recognizing a foreign sovereign's privilege, based in comity, to bring lawsuits in U.S. courts).

384. *See supra* notes 71-84 and accompanying text.

385. *See* RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090, 2106 (2016) ("[P]roviding a private civil remedy for foreign conduct creates a potential for international friction beyond that presented by merely applying U.S. substantive law to that foreign conduct.").

386. *See* Dodge, *supra* note 14, at 2078.

387. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 482(2)(d) (AM. LAW INST. 1987).

388. Yahoo! Inc. v. La Ligue Contre Le Racisme Et l'Antisemitisme, 433 F.3d 1199, 1215 (9th Cir. 2006) (en banc) (opinion of Fletcher, J.).

389. *Id.*

Comity therefore provides two built-in protections for states worried about global injunctions that violate fundamental values. One state's courts might deploy comity on the front end—by limiting the reach or strength of an injunction—and another state's courts might *decline* to deploy comity on the back end, by refusing to enforce that extraterritorial injunction if it contravenes public policy. Comity is thus not inconsistent with global injunctions. Rather, it gives courts tools to modulate the reach and strength of those injunctions.

C. International Agreements

Comity calls for mutual accommodation. Agreements between states regarding their control over the internet—including agreements to cede some of this control—are not inconsistent with that principle.[390] To the contrary, international agreements are often struck in the spirit of mutual accommodation and may pave the way for greater clarity about, and more deference to, sovereign interests.[391] This is the idea behind, for example, mutual legal assistance treaties by which states agree to assist each other in criminal investigations.[392]

Efforts are underway to update the regime for cross-border law enforcement access to data.[393] The United States and the United Kingdom are working to reach an agreement on a joint framework for law enforcement access to data stored abroad[394] consistent with the framework established by the CLOUD Act.[395] That agreement reflects a recognition of both states' needs and is an attempt to accommodate those needs.[396] The agreement will ideally serve as a model for other states that will seek to strike similar agreements with the United States.[397] Similarly, the Privacy Shield regime, which represents an agreement

---

390. *See, e.g.*, Maher M. Dabbah, *Future Directions in Bilateral Cooperation: A Policy Perspective*, *in* COOPERATION, COMITY, AND COMPETITION POLICY 287, 288 (Andrew T. Guzman ed., 2011) (noting that comity is a dominant form of bilateral competition agreements).

391. *Id.* at 288 & n.2.

392. *See* Andrew Keane Woods, *Mutual Legal Assistance in the Digital Age*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 659 (David Gray & Stephen E. Henderson eds., 2017).

393. *See* David Kris, *U.S. Government Presents Draft Legislation for Cross-Border Data Requests*, LAWFARE (July 16, 2016, 8:07 AM), https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests [https://perma.cc/9BBF-SVNE].

394. *Id.*

395. 18 U.S.C. § 2523 (2018).

396. Draft Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism (on file with author).

397. *See Data Stored Abroad*, *supra* note 177, at 13-14 (statement of Richard W. Downing, Acting Deputy Assistant Att'y Gen., Department of Justice).

between the U.S. Department of Commerce, the Swiss Administration, and the European Commission, might also serve as a model.[398]

We might imagine reaching a similar set of agreements on other issues as well, from intellectual property rights to speech and privacy protections. When the European Court hears arguments challenging the Privacy Shield regime,[399] it should not take seriously arguments that the regime does not sufficiently respect sovereign interests (including sovereign privacy protections). The agreement was struck between sovereigns, and nothing in the sovereign-deference doctrines suggests that states cannot bind themselves in agreement to accommodate intersovereign concerns.

V. COURTS AND BEYOND

Where does this leave us? If, as this Article has argued,[400] we should have a general preference for sovereign deference, then the sovereign-deference doctrines are welcome tools. These doctrines are a useful guide for courts in the data sovereignty cases, and they may even offer more generalizable principles for determining how far each state's sovereign authority ought to extend over the internet and how much room other states ought to allow for that authority. They may even offer guidelines for other actors, beyond courts. This Part briefly addresses the question of courts' competence to manage data sovereignty disputes before asking what a policy of sovereign deference might mean for other actors. Whether one agrees with the criticisms of court-managed foreign affairs or not,[401] courts will be the ones to resolve these disputes unless steps are taken by the executive, by Congress, and by American internet firms themselves, preemptively, to defer to sovereign interests.

---

398. *Welcome to the Privacy Shield*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/welcome [https://perma.cc/2YA7-VTLQ].

399. *See, e.g.*, Case T-670/16, Dig. Rights Ir. Ltd. v. Comm'n (Nov. 22, 2017), http://curia.europa.eu/juris/document/document.jsf?text=&docid=197141&pageIndex=0&doclang=en [https://perma.cc/BZ2G-R7VD].

400. *See supra* Part II.

401. Dodge responds to both arguments. For the counterargument to the view that comity is an expansive doctrine with no limiting principles, see Dodge, *supra* note 14, at 2125-32. For the counterargument to the view that the executive branch ought to have dominion in making comity determinations, see *id.* at 2132-40.

A. The Question of Competence

As the last Part shows, the foreign affairs doctrines will not keep courts out of the business of resolving cross-border disputes. If globalization makes it difficult for courts to resolve disputes without producing *some* foreign relations effect,[402] then the data-sovereignty cases suggest that the internet accelerates that trend. This could serve to normalize foreign relations law even further.[403] It also suggests that courts will play a key role in deciding major questions of technology policy. Is this cause for concern? One of the dominant themes in the foreign affairs literature is the question of courts' institutional capacity to manage foreign relations.[404] The Constitution allocates foreign affairs responsibilities to the President; accordingly, some think, courts ought to attempt to stay out of foreign affairs.[405] Yet it is worth considering whether the data-sovereignty cases could change settled preferences for political-branch management of foreign affairs.

On the one hand, we might imagine that courts are *less* well suited to manage sovereign deference in the context of fast-changing technological disputes. If a court makes certain assumptions about the technological feasibility of one remedy or another, and those assumptions turn out to be wrong, then the court may apply foreign affairs norms in unfortunate ways. For example, a court could conclude that geo-blocking technology—the kind of technology that allows a firm to know where its users are located—is insufficiently accurate to capture territorial interests and therefore decide against a location-based remedy. What if this assumption later turns out to be wrong as geo-blocking technology advances? (Indeed, in its dispute with the CNIL at the European Court of Justice, Google was quick to point out that its geo-blocking technology is now good enough to identify the geographic location of 99.94% of users.[406]) The same concern might arise as technology develops with respect to locating users, identifying illegal content for takedowns, and so on. Another argument against courts' competency in this area is that they manage individual cases or controversies and, therefore, cannot link issues. Productive compromises may be possible by linking issues if parties compromise on one issue to achieve their goals on another. The literature

---

402. *See* Clopton, *supra* note 36, at 11-13.

403. *See* Sitaraman & Wuerth, *supra* note 34, at 1919-35.

404. *See* sources cited *supra* notes 35-36.

405. *See, e.g.*, BRADLEY & GOLDSMITH, *supra* note 14, at 119-32; Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361 (2009).

406. Mark Scott (@markscott82), TWITTER (Sept. 11, 2018, 1:53 AM), https://twitter.com/markscott82/status/1039436684562231296 [https://perma.cc/XG3N-P88F].

on issue linkage suggests that this is precisely one benefit of bundling issues,[407] which courts cannot do as well as legislatures, because they hear one dispute at a time.

We might also wonder if arguments about courts' competence in crafting technology policy might apply here. Orin Kerr, for example, suggests that the "legislative branch rather than the judiciary should create the primary investigative rules when technology is changing."[408] The problems, as Kerr sees them, are that "it is difficult for judges to fashion lasting guidance when technologies are new and rapidly changing," that "[c]ourts lack the institutional capacity to easily grasp the privacy implications of new technologies they encounter," and that judicially created rules "cannot change quickly" and therefore "tend to become quickly outdated or uncertain as technology changes."[409] Legislatures, by contrast, "usually act at a surprisingly early stage, and certainly long before the courts."[410] As the Fourth Circuit has recognized, courts are simply "institutionally ill-equipped" to handle fast-changing technologies, and therefore, courts ought to defer to legislatures that can act quickly and adapt rules to new facts.[411]

This view has been endorsed by several Supreme Court Justices.[412] But is it right—either in general or in the context of cross-border data disputes? Arguably not.[413] If the goal is flexibility, then one might simply prefer standards over bright-line rules. But courts can fashion flexible standards without the aid of legislative intervention, and they do so all the time, especially when the facts on the ground are fast-changing.[414] Kerr suggests that his argument carries special

---

407. *See, e.g.*, John S. Odell & Dustin Tingley, *Negotiating Agreements in International Relations*, *in* NEGOTIATING AGREEMENT IN POLITICS: REPORT OF THE TASK FORCE ON NEGOTIATING AGREEMENT IN POLITICS 144, 161-62 (Jane Mansbridge & Cathie Jo Martin eds., 2013).

408. Kerr, *supra* note 29, at 806.

409. *Id.* at 858-59.

410. *Id.* at 870.

411. United States v. McNulty (*In re* Askin), 47 F.3d 100, 105-06 (4th Cir. 1995).

412. *See* Sklansky, *supra* note 29, at 226 ("The idea that new technological threats to privacy are best addressed by legislatures rather than by courts recently picked up four new endorsements, from Justices Samuel Alito, Stephen Breyer, Ruth Bader Ginsburg, and Elena Kagan.").

413. For two responses to Kerr's institutional-competence argument, see Sklansky, *supra* note 29, at 224-33; and Solove, *supra* note 29, at 761-77.

414. Standards have long been celebrated for their ability to adapt to an uncertain future:

> What the author of a legal document is trying to control is the future itself . . . . You are trying to stabilize a part of the future, set it on a course, make it more foreseeable and more reliable . . . . But what happens in the future is necessarily uncertain, inchoate, contingent, only partly foreseeable, and you must therefore find some similar and corresponding quality in the words you are using. Briefly, your words

weight in the context of the Fourth Amendment.[415] But if the argument for judicial deference to other branches has special weight anywhere, then surely it is the data-sovereignty litigation where concerns about court competence to engage in foreign affairs accrue alongside concerns about the fast pace of technological change.

Kerr also suggests that his argument only applies where the technology is fast-changing.[416] But when is technology not in flux? Indeed, technology today is both fast-changing and far-reaching. If we think that courts should step back when technology is changing quickly, should we also think that courts can no longer fairly resolve disputes involving the financial sector, healthcare, or any other industry that is being transformed by technological change?

Courts have much to recommend them as policymakers. The fact that courts only hear cases based on the facts before them may make them precisely the *right* actors for regulating in such a fast-changing area.[417] Rather than implementing sweeping changes across a number of issues—changes that might be hard to roll back later—courts regulate case by case, allowing for incremental policy development, which might be preferable given the current pace of technological change. This may be especially true in the foreign affairs context, where courts can manage intersovereign disputes through what Baxter called comparative-impairment analysis.[418]

Courts can also invite further action by resolving individual cases while leaving the door open to the political branches to revise the law more broadly as it develops. As Erin Murphy writes, courts act when the legislature does not, and this fear of judicial uncertainty can be a powerful motivator for legislative action.[419] Better policy may emerge where courts and the other branches engage in a back-and-forth over how technology might apply in different contexts and in ways that are consistent with constitutional norms.[420] Murphy wrote specifically about applying privacy rules in criminal law to fast-changing technologies. But compelling evidence also supports her argument in the data-sovereignty cases.

---

should be as flexible, as elastic, indeed as vague, as the future is uncertain and unpredictable.

Charles P. Curtis, *A Better Theory of Legal Interpretation*, 3 VAND. L. REV. 407, 423-24 (1950), *as quoted in* Pierre Schlag, *Rules and Standards*, 33 UCLA L. REV. 379, 399 n.59 (1985).

415. Kerr, *supra* note 29, at 882 (distinguishing the "uniqueness of criminal procedure").

416. *Id.* at 859.

417. Kerr acknowledges this point explicitly but suggests that criminal law is particularly ill-suited to case-by-case rulemaking when technology is in flux. *Id.* at 883.

418. William Baxter, *Choice of Law and the Federal System*, 16 STAN. L. REV. 1, 18-19 (1963).

419. *See* Murphy, *supra* note 29, at 498.

420. *Id.*

The problem of jurisdictional hurdles to cross-border law enforcement data requests has been around for as long as there have been cross-border law enforcement data requests.[421] Despite repeated calls to change the law—calls by industry,[422] civil society,[423] and academics[424]—Congress sat still. Indeed, the Office of International Affairs in the Department of Justice, which manages cross-border requests for data, went to Congress repeatedly to ask for more funding, and Congress did little. Congress showed very little interest in addressing this issue until the *Microsoft Ireland* litigation. After the case began, congressional staffers began to entertain the idea of holding hearings, and in 2016, when it was clear that the case was bound for the Supreme Court, the House Judiciary Committee held a hearing on the matter.[425] In 2017, after the Supreme Court granted certiorari, the House and Senate Judiciary Committees both held hearings.[426] Only after the case had been argued at the Court—and after considerable lobbying on the Hill by both parties to the lawsuit—did Congress pass the CLOUD Act to resolve the issues raised by the case.[427]

As a result, it appears, in at least in one significant case, that Congress was unwilling to address the jurisdictional barriers to cross-border law enforcement until the judiciary acted. This is Murphy's "interbranch dialogue"[428] in action. Is

421. Woods, *supra* note 15, at 750 (showing requests going back to 2000); *see also* Transcript of Oral Argument, *supra* note 5, at 17 ("This is not a new problem.").

422. Brad Smith, *Time for an International Convention on Government Access to Data*, HUFFINGTON POST (Jan. 22, 2014, 9:38 AM ET), https://www.huffingtonpost.com/brad-smith/time-for-an-international-convention-on-government-access-to-data_b_4644130.html [https://perma.cc/KK2W-DWHK].

423. *Letter to US Congress Urging Increase to MLAT Funding*, CTR. FOR DEMOCRACY & TECH. (Nov. 18, 2014), https://cdt.org/insight/letter-to-us-congress-urging-increase-to-mlat-funding [https://perma.cc/3M5Z-PZ2G].

424. Andrew K. Woods, *Why Does Microsoft Want a Global Convention on Government Access to Data?*, JUST SECURITY (Feb. 19, 2014), https://www.justsecurity.org/7246/microsoft-global-convention-government-access-data [https://perma.cc/KS8U-X8ZU].

425. *International Conflicts of Law and Their Implications for Cross Border Data Requests by Law Enforcement: Hearing before the H. Comm. on the Judiciary*, 114th Cong. (2016).

426. *Data Stored Abroad*, *supra* note 177; *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 115th Cong. (2017).

427. Indeed, the interbranch dialogue was so intense that one of the sponsors of the CLOUD Act, Senator Orrin Hatch, attended oral argument, and the Court seemed genuinely confused about whether it would need to rule at all. *See* Andrew Keane Woods, *Analysis of Microsoft-Ireland Supreme Court Oral Argument*, LAWFARE (Feb. 27, 2018, 6:39 PM), https://www.lawfareblog.com/analysis-microsoft-ireland-supreme-court-oral-argument [https://perma.cc/9AB9-5FUH].

428. Murphy, *supra* note 29, at 538.

it optimal? That much is unclear. The Court might have interpreted the search as not occurring in Ireland, as many lower courts did in related cases, thereby sidestepping the issue.[429] This would have been a clean resolution to the problem, and it would have avoided some of the problems that the CLOUD Act creates.[430] But who knows how the Court would have ruled, and that uncertainty is one reason we might prefer legislative rulemaking—whether prompted by imminent judicial action or not—over court-made policy.

Should we prefer courts to avoid hearing data-sovereignty cases? It may not matter. A cadre of scholars has argued that judicial isolationism is indefensible today.[431] The message these globalist scholars have for courts is that they simply cannot escape foreign affairs in a globalized world. Adapting this argument to the data-sovereignty litigation and building on Murphy and Kerr, we can conclude that courts cannot escape technology policy in a digitized world. Ultimately, it may not matter whether courts are the *optimal* actors to address these conflicts if they end up being, by default, the primary ones to do so.

B. Sovereign Deference by the Legislature

The biggest barrier to law enforcement access to evidence in the world today is an American law: ECPA.[432] Rather than completely repeal ECPA's onerous blocking features, which create tensions around the world, Congress passed the CLOUD Act, which grants the executive branch the authority to allow certain countries into the "club"—meaning that those countries' governments are able to request data directly from American providers without the need for resort to the MLAT regime.[433]

The CLOUD Act has some limited but important features of sovereign deference built in. The Act explicitly states that providers may, upon receipt of a request to disclose the contents of a customer's account,

> file a motion to modify or quash the legal process where the provider reasonably believes:

---

429. *See supra* note 99.

430. *See Data Stored Abroad*, *supra* note 177, at 6 (statement of Andrew Keane Woods, Assistant Professor, University of Kentucky College of Law).

431. *See supra* note 34.

432. *See Data Stored Abroad*, *supra* note 177, at 6-7 (statement of Andrew Keane Woods, Assistant Professor, University of Kentucky College of Law).

433. *See id.* at 7.

> (i) that the customer or subscriber is not a United States person and does not reside in the United States; and
> (ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.[434]

Moreover, in weighing these motions to quash, courts are explicitly instructed to engage in a comity analysis.[435] Courts are told to take into account, where appropriate, "the interests of the United States" in having the data produced, the interests of "the qualifying foreign government" in keeping the data from being produced, the likelihood and extent of penalties the provider might suffer from disclosure, the location and nationality of the subscriber and their connection to the United States, and more.[436]

While this legislative framework has the trappings of sovereign deference—comity, balancing national interests, and so on—it actually appears to *narrow* considerably the influence that comity and related doctrines will have over these cases. Before the CLOUD Act, courts were free to conduct a comity analysis sua sponte and decline to enforce an order if it would infringe on another state's sovereignty.[437] Indeed, some had hoped that the Supreme Court might do just that in *Microsoft Ireland*.[438] Instead, a court might now reasonably conclude that its authority to weigh sovereign interests is *only permitted* under the specific circumstances spelled out by the Act. If Congress wanted comity to play a role in cross-border data cases, it might just as well have left these comity-limiting parameters out of the bill.

In other, more significant respects, the bill is a step backwards from the kind of sovereign deference that will be necessary for a lasting and interoperable internet. U.S. law now gives countries a choice: (1) behave well, comply with the due process standards set by the Americans, and ask nicely, and the United States might allow you to enforce your laws on your soil, or (2) take whatever steps are needed to enforce your laws on your soil. The creation of a club of insider coun-

---

434. 18 U.S.C. § 2703(h)(2)(A) (2018).

435. *Id.* § 2703(h)(3).

436. *Id.*

437. Andrew Keane Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018, 5:49 PM), https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems [https://perma.cc/4MJ4-EC8C] (noting that comity was available to courts before the CLOUD Act passed).

438. Brief in Support of Appellant Microsoft, Inc. by Apple Inc. as Amicus Curiae, *supra* note 18, at 10-14.

tries could ideally create a race to the top where countries seek to strengthen protections for human rights and privacy in order to be eligible for an agreement with the United States under the CLOUD Act. This is possible. But clubs lead to anticlubs[439]—and China is actively pursuing just such a club.[440]

Countries with attractive markets like India face a choice. They can comply with the United States' prerequisites and ask for admittance to the club—a necessary step if India is going to be able to enforce its laws on its soil without taking physical control over the Indian internet architecture—or they can take legislative steps to force compliance with Indian laws and hope that the country's market is lucrative enough to leave foreign firms little choice but to comply. A few months after the CLOUD Act passed, India's Justice BN Srikrishna Committee—a committee tasked by the government with creating a national privacy regime—released a comprehensive report and a draft data protection law, the "Personal Data Protection Bill, 2018."[441] The bill requires that data collected on Indians in India be stored on servers located in India. In short, the bill mandates data localization. In response, policy advocates have suggested that the government pursue a bilateral agreement of the sort envisioned by the CLOUD Act as an alternative to data localization.[442] It remains to be seen which view wins out, but it is clear that the CLOUD Act frames the choice in stark relief.

All of this could have been avoided with a simple reform to ECPA that clarified that ECPA did not apply to law enforcement requests made outside the United States and that U.S. companies are therefore free as a matter of U.S. law to comply with those requests.[443] Whether U.S. firms decide to comply with those orders is another matter, but they should at least have the choice that firms have in nearly every other industry: comply with local rules or exit the market. American law should not stand as a barrier to Indian or Brazilian law enforcement efforts (or American firms' efforts at compliance with those laws).

---

439. *See Data Stored Abroad*, *supra* note 177, at 7-8 (statement of Andrew Keane Woods, Assistant Professor, University of Kentucky College of Law).

440. *See* Eichensehr, *supra* note 28, at 319-20.

441. *The Personal Data Protection Bill 2018*, MINISTRY ELECTRONICS & INFO. TECH., https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf [https://perma.cc/AV3B-ZKVS].

442. Bedavyasa Mohanty & Madhulika Srikumar, *Data Localization Is No Solution*, OBSERVER RES. FOUND. (Aug. 3, 2018), https://www.orfonline.org/research/42990-data-localisation-is-no-solution [https://perma.cc/LH49-9PER].

443. *See Data Stored Abroad, supra* note 177, at 7 (statement of Andrew Keane Woods, Assistant Professor, University of Kentucky College of Law).

Cross-border law enforcement requests are unlikely to be the last chance Congress has to reveal itself as mindful of other sovereign interests over the internet. But there are reasons to worry that Congress will not recognize those interests. In the past decade alone, Congress has held nine hearings on so-called Internet Freedom bills, which are designed explicitly to frustrate China's efforts at controlling the internet within its territory.[444]

C. Sovereign Deference by the Executive

There are a number of steps that the executive could take to recognize foreign nations' legitimate sovereign interests over the internet. This is true even setting aside the fraught efforts to develop international norms regarding cyberwarfare.[445] The Presidential Policy Directive that grants some foreigners the same rights as American citizens is a prime example, as was the U.S.-U.K. agreement regarding law enforcement access to data. Yet both of these executive measures could go considerably further to defer to sovereign interests.

Trust in American internet companies and in the American intelligence community plummeted in the wake of the Snowden revelations.[446] This precipitated a much more aggressive stance by many American firms towards the U.S. government.[447] There were many other consequences of this loss of trust, including the *Schrems* decision that invalidated the safe harbor arrangement.[448] In re-

444. THOMAS LUM ET AL., CONG. RESEARCH SERV., R42601, CHINA, INTERNET FREEDOM, AND U.S. POLICY 14-15 (2012), https://fas.org/sgp/crs/row/R42601.pdf [https://perma.cc/VRD3-T4T6].

445. *See, e.g.*, Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SECURITY (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms [https://perma.cc/44PC-YABT] (describing how "after years of slow yet meaningful progress in developing State consensus regarding the application of international law norms to cyberspace, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (otherwise known as the Group of Governmental Experts, or GGE) collapsed").

446. *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 369 (E.D.N.Y. 2016).

447. *See* Rozenshtein, *supra* note 28, at 116 ("This, so far, has been Edward Snowden's main victory: to increase the incentives for surveillance intermediaries to resist the government.").

448. *See* Timothy Edgar, *Final Thoughts on Reforming Surveillance and European Privacy Rules*, LAWFARE (Nov. 8, 2015, 2:19 PM), https://www.lawfareblog.com/final-thoughts-reforming-surveillance-and-european-privacy-rules [https://perma.cc/EFC7-Q2F7] ("[T]he decision of the Court of Justice of the European Union (CJEU) in *Schrems v. Data Protection Commissioner* may turn out to be the most important consequence of the Snowden revelations.").

sponse, the United States immediately set about to repair its bond with the European Union.[449] President Obama gave a remarkable speech announcing PPD-28, where he declared: "[P]eople around the world—regardless of their nationality—should know that the United States is not spying on ordinary people who don't threaten our national security, and that we take their privacy concerns into account."[450] Yet PPD-28 is a slippery document, "one that conveys and writes into policy a great deal of values without constraining a great deal of practice."[451]

PPD-28 is an excellent example of executive branch sovereign deference, and it could be applied to other areas beyond surveillance. The President could develop an entire policy framework, in the vein of PPD-28, which assures foreign partners that the United States recognizes foreign sovereign interests across a range of internet-governance issues and that it will not stand in their way. This might take the form of the executive branch working with Congress to take legislative action, like it did when it worked with Congress to craft and pass the CLOUD Act.[452] It could include a foreign-sovereign litigation policy by which the United States will not oppose and might even work with foreign sovereigns litigating one of the issues described here. Finally, it likely would mean reversing course on the Internet Freedom program at the State Department,[453] which has

449. *See* Laura Smith-Spark, *Germany's Angela Merkel: Relationship with U.S. 'Severely Shaken' over Spying Claims*, CNN (Oct. 24, 2013, 1:10 PM ET), https://www.cnn.com/2013/10/24/world/europe/europe-summit-nsa-surveillance/index.html [https://perma.cc/2Y9K-99QM].

450. Ritika Singh, *Text of the President's Remarks on NSA and Surveillance*, LAWFARE (Jan. 17, 2014, 11:23 AM), https://www.lawfareblog.com/text-presidents-remarks-nsa-and-surveillance [https://perma.cc/7PBA-AQ4E].

451. Benjamin Wittes, *The President's Speech and PPD-28: A Guide for the Perplexed*, LAWFARE (Jan. 20, 2014, 11:02 AM), https://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed [https://perma.cc/GL8A-UX4R].

452. The executive branch has advocated for reforms along the lines of the CLOUD Act for years. *See, e.g.*, *Data Stored Abroad*, *supra* note 177, at 10 (statement of Richard W. Downing, Acting Deputy Assistant Att'y Gen., Department of Justice) (urging Congress to amend ECPA to allow U.S. law enforcement to be able to access data stored abroad); *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, PRESIDENT'S REV. GROUP ON INTELLIGENCE & COMM. TECHNOLOGIES 227 (Dec. 12, 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [https://perma.cc/37PD-2XTR] (suggesting that ECPA be amended to resolve the MLAT problem).

453. The Internet Freedom program is housed within the Bureau of Democracy, Human Rights, and Labor. *See Internet Freedom*, U.S. DEP'T ST., https://www.state.gov/j/drl/o/index.htm [https://perma.cc/P3XN-GJLM].

received considerable funding—$145 million since 2008[454]—and which many states see as a threat to their sovereign authority.[455]

International agreements are another avenue for recognizing sovereign interests.[456] For example, rather than allowing the European Court of Justice to decide, by its own jurisdictional analysis, whether Google must comply globally with the right to be forgotten, U.S. and European leaders could attempt to negotiate a solution. Lest this sound naive, it is worth noting that in the law enforcement context, we already have a model for such an agreement. The draft agreement struck between the United States and the United Kingdom regarding access to cross-border data for terrorism and serious crime is a good start because it openly acknowledges that each state has a legitimate interest in accessing data held in the other's territory.[457] But the agreement, which is planned as a model for future agreements, is to be implemented by legislation that requires potential parties to later agreements to be certified by the Attorney General as meeting certain human-rights standards, which are set at a high level.[458] This risks creating a dangerous incentive for states to pursue their own internet policies within their own territory.[459]

D. Sovereign Deference by Internet Firms

Finally, companies could elect to be more deferential to state interests than they currently are. This is not an argument for company capitulation to every state demand. But, as this Article has suggested, it is a dangerous game to frustrate state interests at every turn. Indeed, it is precisely the sort of antisovereign actions taken by major technology firms that have sparked the harshest criticism

---

454. *Id.*

455. *See* Marc Lynch, *The Internet Freedom Agenda*, FOREIGN POL'Y (Jan. 22, 2010, 4:01 PM), https://foreignpolicy.com/2010/01/22/the-internet-freedom-agenda [https://perma.cc/7B7M-GC92] (describing how most of the world codes internet freedom as "regime change"); *see also* Emily Parker, *Russia Is Trying to Copy China's Approach to Internet Censorship*, SLATE (Apr. 4, 2017, 1:25 PM), http://www.slate.com/articles/technology/future_tense/2017/04/russia_is_trying_to_copy_china_s_internet_censorship.html [https://perma.cc/3T5P-SQFM].

456. The CLOUD Act explicitly relies on international agreements to identify which countries are not subject to ECPA's blocking features. *See* 18 U.S.C. § 2523 (2018).

457. Letter from Peter J. Kadzik, Assistant Att'y Gen., to Hon. Joseph R. Biden, President, U.S. Senate (July 15, 2016) (on file with author).

458. *See Data Stored Abroad*, *supra* note 177, at 6 (statement of Andrew Keane Woods, Assistant Professor, University of Kentucky College of Law).

459. *See id.* at 7.

of those firms. Scholars have likened these firms to railroads[460] and public utilities.[461] Both of these examples suggest that some scholars feel the need for break-their-back regulation and submission to the state. With this same dynamic playing out in other countries, it may make sense for technology firms to tread lightly with states.

When should an intermediary resist the state? This is a complex question with no easy answer, but over the long run, we can see that resisting state rules *while* taking advantage of the state's market is likely to be unsuccessful for the company and, worse, is likely to produce harmful consequences for internet users. In the short run, individual firms have an incentive to operate under a single set of rules globally, without tailoring their services to different state rules. But over time, as states bear down on firms to comply with local rules, states may take extreme self-help measures when firms resist—making everyone worse off.

Not all states can force a company to comply with their wishes, of course; just those with a big enough market to warrant the firm's attention. Smaller markets and weaker states may have less power to compel a firm to submit to local rules. Larger markets, however, are another story. Google famously left China in protest over the People's Republic's censorship practices, only to develop later a censorship tool designed explicitly to place the firm in a position to reenter the Chinese market.[462] Firms can protest or ignore sovereign differences for a time but apparently not forever.

CONCLUSION

The cosmopolitan ideal for the internet—whether the product of naivete, utopian dreams, or strategic interest—is dead. States, being jealous of their sovereignty, and users, wanting to make the digital world their own, will inevitably resist the idea of a single, shared online experience. What is appropriate in New York may not be appropriate in Bangkok and vice versa. This trend is only likely to continue as the physical and digital worlds merge: the more the internet becomes embedded in our everyday lives and the more it is constituted by data that reflect our real-world experiences, the more likely it is that the internet will need to reflect the very real differences in those experiences.

---

460. *See* Rozenshtein, *supra* note 28, at 144.

461. *See* Peter Swire, *Should the Leading Online Tech Companies Be Regulated as Public Utilities?*, LAWFARE (Aug. 2, 2017, 9:00 AM), https://www.lawfareblog.com/should-leading-online-tech-companies-be-regulated-public-utilities [https://perma.cc/P548-3A9Z] ("[T]here are some reasonably strong arguments that the biggest online services today are similar to traditional public utilities due to their high market share, network effects, and difficulty for consumers to live without the service.").

462. Gallagher, *supra* note 211.

This means that the internet governance question of the day is *not* whether the internet should be more or less cosmopolitan, a global internet or splinternet. (Indeed, the more that policymakers push for cosmopolitanism, the more they accelerate trends in the other direction.) Rather, the key question is *how* the internet will bend to accommodate sovereign differences. Do we want an internet that reflects sovereign differences in sensible, mutually agreeable ways—with providers and users left to decide how to comply with local laws—or do we want an internet where states can only achieve their aims by taking physical control of the network architecture?

If we prefer the former, as we should, then we must defer to sovereign differences in ways that encourage the development of a global internet we can all use. Rather than invent new forms of deference, courts especially, but also other actors, should look to the foreign affairs doctrines as a ready-made set of guidelines—doctrines of recognition and deference, as well as doctrines of abstention and restraint. This, in turn, will entail occasional extraterritorial exercises of authority, contrary to what a number of courts and litigants in high-profile internet disputes have argued. A familiarity with foreign affairs case law suggests that this is both normal and even welcome.