THE YALE LAW JOURNAL FORUM
MARCH 18, 2019

Sovereign Difference and Sovereign Deference on the Internet

Jack Goldsmith

ABSTRACT. This Response to Andrew Woods makes two points. First, building on one of Woods's claims, and drawing on the work of Milton Mueller, it shows why the "fragmentation" charge frequently levied against sovereignty-based approaches to internet governance is misplaced. Second, it raises questions about the efficacy of Woods's normative theory of judicial comity.

INTRODUCTION

A theory of global internet governance underlies Andrew Woods's analysis of how judicial comity doctrines should apply to cross-border data disputes.[1] First is the principle of sovereignty.[2] Nations are sovereign in the sense that they wield legitimate and usually effective authority within a territory, including authority over data and data infrastructure in the territory, and over the people and firms in the territory that use the data and infrastructure. Second, national boundaries roughly reflect differences in the histories, commitments, cultures, norms, and individual and aggregate preferences that governments roughly want to preserve. This fact combined with the principle of national sovereignty generates what Woods calls the "*sovereign-difference* ideal that sees the internet operating differently in different places according to local norms, customs, and rules."[3]

1. Andrew Keane Woods, *Litigating Data Sovereignty,* 128 YALE L.J. 328 (2018).
2. *Id.* at 360-63.
3. *Id.* at 367.

I buy these two descriptive claims.[4] In Part I of this Response, I analyze what Woods's descriptive thesis means for so-called "internet fragmentation," a topic he touches on but about which there is more to say. The basic point is that respecting the principle of sovereign deference does not lead to or commit one to destructive fragmentation of the internet. In Part II, I raise questions about the efficacy of Woods's normative theory of judicial comity that he builds on top of his descriptive claims.

I. THE MYTH OF FRAGMENTATION

"The sovereign-difference ideal," says Woods, "is concerned principally with state control over the internet's local effects."[5] One objection to a governance system built on this ideal—and a charge one often hears these days—is that this approach entails the "balkanization" or "fragmentation" of the internet.[6] Woods has a brief response: "[the internet] 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."[7] This is right, but it doesn't tell the full story. The best of account of what more there is to say comes from Milton Mueller.[8]

Mueller distinguishes between an internet that is "technically fragmented" and one that is "technically compatible but heavily filtered."[9] Recall that the internet is defined and constituted by a common language: "a set of data formatting, naming, addressing, and routing standards collectively known as 'the Internet protocols,' the most basic of which is Internet Protocol (IP)."[10] These protocols are what allow every network on the internet, connected through every type of physical layer and using every type of higher-level transport and application standards, to communicate.

Those who worry about fragmentation do mean technical fragmentation in the sense of a permanent break in interoperable connectivity. As Mueller notes,

4. *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2008).

5. Woods, *supra* note 1, at 368.

6. *See* MILTON MUELLER, WILL THE INTERNET FRAGMENT?: SOVEREIGNTY, GLOBALIZATION AND CYBERSPACE 42-70 (2017); Anupam Chander, *Who Runs the Internet?*, *in* RESEARCH HANDBOOK ON THE POLITICS OF INTERNATIONAL LAW 418, 418-42 (Wayne Sandholtz & Christopher A. Whytock eds., 2017).

7. Woods, *supra* note 1, at 368.

8. MUELLER, *supra* note 6, at 42-70.

9. *Id.* at 49.

10. *Id.* at 22-24.

given the incessant growth of the internet, and especially the onset of the Internet of Things, internet connectivity is "spreading virally."[11] It is doing so because both the network benefits of that growth and the costs of switching are unfathomably high. Mueller acknowledges that there are (dim) threats to interoperability, including a split DNS root and potential problems in the transition from IPv4 to IPv6.[12] But fragmentation in these senses is not typically what critics of the sovereign difference ideal have in mind. Nor are they talking about incompatibility at the application layer—for example, the inability of someone using FaceTime to communicate with someone using Skype. As Mueller correctly notes, "the very universality of Internet connectivity gives developers the freedom to offer any competing, incompatible applications they want," which is "a vital and unavoidable part of facilitating innovation and consumer choice."[13]

What the critics mean by "balkanization" or "fragmentation" are various forms of filtering, and especially content filtering, at national borders. China is the paradigm. It has powerful digital filters at the border and an intricate regime of surveillance, counter-speech, censorship, punishment, social credit ratings, and targeted disruption inside the country, that together allow the Chinese Communist Party to control unwanted speech.[14] China is also developing its own versions of important internet platforms and applications standards that differ and compete with those offered in the West. The internet as experi-

11. *Id.* at 68.

12. MUELLER, *supra* note 6, at 56-66. The Domain Name System serves as something like the internet's phone book. It converts readable text (e.g., http://www.yalelawjournal.org) into a machine-readable IP address. A split DNS root would create two zones (or phone books) for the same domain. IPv4 and IPv6 are two variants of the Internet Protocol, which identifies devices across the world according to their distinctive IP address. IPv4 is an older version that could support roughly 4.3 billion devices. The growth of the internet through smartphones, Internet of Things devices, and personal computers meant that the world risked running out of distinctive IP addresses on IPv4. The IPv6 protocol was designed and launched to support far more addresses. It also included major enhancements on several other metrics such as efficiency, processing speed, and security. The two protocols can and do coexist on the internet, but the world is moving towards adopting IPv6 and IPv4 will eventually phase out. *See* Keith Shaw, *What Is IPv6, and Why Aren't We There Yet?*, NETWORK WORLD (Sept. 27, 2018, 2:58 PM PDT), https://www.networkworld.com/article/3254575/lan-wan/what-is-ipv6-and-why-aren-t-we-there-yet.html [https://perma.cc/9KTQ-PMM2]; *What Is DNS?*, CLOUDFARE, https://www.cloudflare.com/learning/dns/what-is-dns [https://perma.cc/T959-E4HD].

13. MUELLER, *supra* note 6, at 67.

14. *See* Jack Goldsmith, *The Failure of Internet Freedom*, KNIGHT FIRST AMEND. INST. 9-10 (2018), https://knightcolumbia.org/sites/default/files/content/Emerging_Threats_Goldsmith.pdf [https://perma.cc/P2LU-75GS].

enced in China looks and feels very different from the internet in the United States—and not just in language and culture.

Filtering at the national border is just one instance of the universal and necessary practice of packet filtering on the internet. "Internet protocols . . . foster *both* universal interoperability *and* the ability to modulate and restrict the extent to which any given network opens itself up to traffic from other networks,"[15] Mueller notes. In other words, the internet protocols that allow machines and networks to exchange information packets also allow them to be programmed to refuse other packets. And there are all sorts of good reasons not to accept packets: to prevent access by those who would steal, disrupt, or spam; to enforce intellectual property or geographical identity rules; to filter search results in the language you want; to allow access to all manner of creative applications (which requires exclusion of others); to enable paid online services that could not otherwise operate; to enforce the DNS system; and so on.

Indeed, the very notion of an "Inter-Net" implies fragmentation. "The basic units of internetworking are known as Autonomous Systems," where "autonomy" means "the ability to set policies for naming, addressing and routing, and to control or manage many other aspects of network operations," writes Mueller.[16] The internet is "a federation of Autonomous Systems with an extensive capability for selective, fine-grained 'secession' from practically any other part of the federation."[17] Mueller is thus right that "the technical mechanisms that can monitor, limit, intermediate, condition, or block Internet traffic . . . are widely used and embedded in the Internet's infrastructure."[18] To some, the absence of filtering seems to be what the "open" internet essentially is, or at least should be. But an unfragmented internet is, as Mueller says, "terrifying"[19]—incompatible with all of the enormous pleasures and benefits fostered by the internet, and indeed incompatible with the internet as a coherent communications medium.

Internet filtering, and thus internet "fragmentation," are inevitable and omnipresent on endless dimensions, only one of which is the geographical space controlled by national governments. There is no more threat to the internet *as a communications medium* from filtering along this dimension than from any other. Every nation filters at the border to different degrees. In some respects, this is because governments demand it (think of U.S. restrictions on in-

15. MUELLER, *supra* note 6, at 15.

16. *Id.* at 22.

17. *Id.*

18. *Id.* at 177.

19. *Id.* at 17.

tellectual property and child pornography, or of European privacy rules). In most respects it is because internet users have sharply different general preferences based on where they live, and they "seek out, and content providers want to provide, congenial content that reflects these differences."[20] The internet would be significantly impoverished if we insisted on borderless experiences that defied important local differences and local controls.

But of course, there are large downsides to this reality, one of which is that governments like China can regulate the internet in normatively unattractive ways.[21] What to do about these downsides is a large and difficult subject. First, the optimal mix of internet control and freedom is deeply contested, both within the West and especially on a global basis. As Woods notes, and as I too have argued, the rest of the world largely rejects the American conception of global "Internet Freedom."[22] Second, it is not at all clear that anything can be done about authoritarian state control of the internet at an acceptable cost to the internet or to international order. The normative challenges of internet governance are hard to resolve. But they are not challenges that can fruitfully be addressed or even understood through the scary-sounding but in fact empty notion of "fragmentation," which is a universal condition of the internet.

II. UNCERTAINTIES ABOUT COMITY

Sovereign difference does not destroy or even degrade internet communications. But regulation in accord with sovereign difference can happen in many ways, and how one nation regulates the internet can have a large effect on how people in other nations experience the internet. This raises the question of what set of rules best accommodates sovereign difference. Against the background of a conventional wisdom that demands international agreement in crafting solutions to these problems, Woods usefully reminds readers that courts have many tools for managing clashes of regulatory sovereignty, including the cluster of deference and accommodation doctrines known as comity.

Woods thinks that U.S. courts should follow judicial comity in data litigation cases by, for example, issuing geography-based as opposed to global remedies, production orders that consider foreign sovereign interests, judicious use

20. GOLDSMITH & WU, *supra* note 4, at 149.

21. Woods acknowledges this issue and says (in a nutshell) that "[e]mbracing regional or state differences does not mean sacrificing human rights," and that "deference does not mean endorsement or celebration." Woods, *supra* note 1, at 370.

22. *Id.* at 367-68; Goldsmith, *supra* note 14, at 4.

of the *Charming Betsy* doctrine, and recognition of foreign judgments.[23] He argues that this approach has at least the following potential benefits: (1) it might dissuade nations from asserting physical control over (as opposed to judicial compulsion about) the local effects of internet transactions;[24] (2) it might induce other nations' courts to cooperate by exercising reciprocal constraint;[25] and (3) it might maximize global sovereign preferences.[26]

Maybe, but maybe not.

A. Cooperation by Courts in Different Countries Is Hard

Woods says in passing that deference via comity "may encourage reciprocity from the courts of foreign sovereigns."[27] He doesn't rest much weight on this argument; most of his analysis assesses the effect of judicial comity doctrines on the actions of foreign governments, not foreign courts. But it might be worth emphasizing why reciprocity from foreign courts is unlikely.

Actual cooperation—mutual restraint in order to achieve larger reciprocal benefits—is *really* hard for nations to achieve.[28] In the treaty context, it takes painstaking negotiations about how each nation will restrain itself, written specifications about what restraints each side assumes, penalties for noncompliance, verification mechanisms, and the like. And even then, nations often fail to achieve or sustain cooperation.

Courts that exercise comity doctrines have no way of communicating with foreign counterparts on any of these issues other than through their decisions. Assuming a foreign court wants to cooperate (a very big undefended assumption), how often or carefully does it pay attention to what other nations' courts are doing? Assuming it pays attentions and cares, how does it identify an act of restraint by the U.S. court, and how will it know how to reciprocate? Unless the parties to a cooperative scheme have a clear sense of what counts as cooperation and what counts as defection, the scheme will break down if the parties

---

23. Woods, *supra* note 1, at 374-81. The *Charming Betsy* canon holds that "an act of Congress ought never to be construed to violate the law of nations if any other possible construction remains." Murray v. Schooner Charming Betsy, 6 U.S. (2 Cranch) 64, 118 (1804).

24. *Id.* at 364-66.

25. *Id.* at 371.

26. *See, e.g.*, *id.* at 369 (arguing that comity "allows maximal sovereign difference with minimal harm to other sovereigns").

27. *Id.* at 371.

28. *See* Robert Axelrod & Robert O. Keohane, *Achieving Cooperation Under Anarchy: Strategies and Institutions*, 38 WORLD POL. 226, 226 (1985).

are rational.[29] And of course the problem of cooperation in this sense is significantly harder when we move from a bilateral to a multilateral context, which encompasses a lot of digital litigation.[30]

B. Comity Is Unlikely to Prevent Regulation by Control

Most of Woods's normative case rests on the likelihood that comity will affect actions abroad not by courts, but by foreign governments. Woods distinguishes foreign sovereign internet regulation by *compulsion* from sovereign internet regulation by *control*.[31] The former involves state orders to companies to turn over data, but lets companies choose the means of compliance and permits them to organize and secure their data as they wish. The latter involves orders about how companies must organize and operate their internet services—where they must locate data (for example, in the country), what security protocols they must use (for example, ones that allow for direct government access), and the like. Woods argues, plausibly, that control requires firms to "spend considerably more money developing bespoke network architecture in each

---

29. *See* JACK L. GOLDSMITH & ERIC A. POSNER, THE LIMITS OF INTERNATIONAL LAW 30-31 (2005). There are other conditions for cooperation in the standard prisoner's dilemma. *Id.* at 31-32. What counts as cooperation need not be written down, and it can emerge spontaneously. *Id.* at 84. But the parties of cooperation—in this case, courts—must know the others' preferences, and must know what counts as cooperation, among other things. These conditions are not realistic in the context of the congeries of issues that arise in international data litigation.

30. Woods's notion of reciprocity draws on Larry Kramer's domestic conflicts of law work. Woods, *supra* note 1, at 371 n.245 (citing Larry Kramer, *Rethinking Choice of Law*, 90 COLUM. L. REV. 277 (1990)). Kramer's idea was to model clashes of sovereign interests on a prisoner's-dilemma game. Kramer, *supra*, at 339-44; *see* LEA BRILMAYER, CONFLICT OF LAWS: FOUNDATIONS AND FUTURE DIRECTIONS 145-90 (1991). One state will decline to apply its law when the other state has a superior claim to regulating the cross-border matter. The other state will do the same, and both states will be better off because their mutual restraint maximizes sovereign interests in the aggregate. Kramer, *supra*, at 342-43. The theory does not capture reality, as anyone familiar with the mess of interest analysis in the United States knows. Courts applying interest analysis simply do not see themselves in a cooperative enterprise with courts in others states. They communicate with one another, if at all, only dimly and haphazardly. And, even when courts in one state seek to break a true conflict by weighing local and foreign sovereign interests, they tend to overstate local interests and understate foreign interests—a phenomenon that highlights why, in the absence of clear specification of what counts as restraint and cooperation, decentralized cooperation is so hard in this context. And if it is hard in the domestic interstate context where the sovereigns share a common legal culture and a common constitutional law framework, however loose, it is all the more unlikely to work in the international context.

31. Woods, *supra* note 1, at 364.

market" and to turn over more customer data to governments with resulting losses "to autonomy, privacy, and entrepreneurship."[32]

So far, so good. But at this point, Woods makes two arguments that I question. First, he says that we should prefer a world of compulsion to a world of control. And second, he says that sovereign deference by courts through comity might deter nations from moving from regulation by compulsion to regulation by control.

On the first point, Woods thinks global internet governance should prefer national regulation by compulsion rather than by control *because* compulsion is less expensive for firms and is autonomy-enhancing for individuals. This represents a subtle but crucial shift in his article from an effort to maximize *sovereign* preferences to an effort to maximize *firm and individual* preferences. At one level, Woods's argument for comity is based on sovereign difference and sovereign deference, including deference toward nations like China that exercise maximum control over firms and that have relatively little respect for individual freedom. But at another level, we learn, the reason sovereign deference (comity) is good is that it saves money for firms, makes the internet more efficient, and promotes freedom. One wonders what the ultimate normative touchstone is for Woods's theory of global internet governance. If the touchstone is internet and firm efficiency and individual freedom, it is not clear that the theory can be grounded (as it appears to be) in a theory of *sovereign* difference where sovereigns are treated as black boxes with preferences independent of how they treat firms and people within their borders.

On this second point, I am skeptical that comity doctrines will do much of anything to prevent nations from shifting to regimes of control from regimes of compulsion. Extraterritorial orders by U.S. courts were contributing causes, but not the main cause, of control efforts like data localization, digital trade restrictions, and demands for encryption backdoors and related access.[33] The main cause of these control trends was the Edward Snowden revelations, which made clear that the United States was leveraging its home-field advantage—the fact that most of the world's data travels through its borders and the ability to secretly collect data from U.S. firms that dominate global internet communications—to engage in massive surreptitious surveillance of communications and data transfers in foreign countries. Foreign governments understandably took offense at these sovereign intrusions, and also wanted to maximize their opportunities for access to data as well. They have enormous incentives to exercise control within their borders since U.S. surveillance practices continue regard-

32. *Id.*

33. On these control efforts, see *id.* at 341-51.

less of whether U.S. courts exercise comity. Comity by U.S. courts is unlikely to change this calculus.

Courts can, of course, do things that cause the political branches of sovereign governments—the usual entities that work out international cooperation—to negotiate, and thus affect foreign sovereign behavior with respect to digital issues abroad in this indirect manner. But in prominent cases, it was not comity, but rather aggressive extraterritoriality (or the threat of it), that brought about the change. This is what happened with the CLOUD Act.[34] U.S. litigation over foreign data requests, including the threat of a noncomity ruling by the Supreme Court, induced the political branches to enact a foreign data request scheme that embodied principles of comity and mutual accommodation Woods favors, *and* that authorized the executive branch to negotiate agreements with foreign countries to further deepen cooperation in this area. Another example is the complicated (and fragile) cooperative arrangement known as EU-U.S. Privacy Shield, which emerged from a political negotiation that responded to a decision of the European Court of Justice with a sharp extraterritorial impact on U.S. firms.[35]

These examples suggest, contra Woods, that in some circumstances, courts might best promote sovereign accommodation of regulatory interests related to the cloud not through comity, but by sparking international conflict and inducing governments to act. This point is akin to the idea of preference-eliciting default rules in statutory interpretation, where courts interpret statutes contrary to the probable preferences of the legislature in order to elicit a response by the legislature that is in the best position to decide or clarify the correct rule.[36]

Jack Goldsmith is the Henry L. Shattuck Professor of Law at Harvard Law School. *He thanks Rishabh Bhandari for research assistance.*

34. Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. § 2523 (2018).

35. *See* U.S. Dep't of Commerce, *EU-U.S. Privacy Shield Framework Principles*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [https://perma.cc/H4PA-MK46].

36. *See* Einer Elhauge, *Preference-Eliciting Statutory Default Rules*, 102 COLUM. L. REV. 2162 (2002).