The Internet and the Abiding Significance of Territorial Sovereignty

Indiana Journal of Global Legal Studies

Volume 5 | Issue 2 Article 6

4-1-1998

The Internet and the Abiding Significance of Territorial Sovereignty

Jack L. Goldsmith
University of Chicago Law School

The Internet and the Abiding Significance of Territorial Sovereignty

JACK L. GOLDSMITH*

INTRODUCTION

More than any other technology, the Internet facilitates cheap, fast, and difficult-to-detect multi-jurisdictional transactions. This in a nutshell is why so many believe that the Internet "undermin[es] the feasibility—and legitimacy—of laws based on geographical boundaries."[1] Dean Henry H. Perritt's essay is sanguine about the Internet's ability to facilitate national governance.[2] But even Perritt appears skeptical about the efficacy of territorial regulation of the Internet. His arguments for the Internet's potential to strengthen national and international governance are tempered by doubts about whether regulation conceived in territorial terms can effectively govern Internet transactions.[3]

This essay attempts to alleviate Perritt's doubt. It aims to show that from the perspective of jurisdiction and choice of law, territorial regulation of the Internet is no less feasible and no less legitimate than territorial regulation of non-Internet transactions.[4]

---

* Associate Professor, University of Chicago Law School. Thanks to Andrew Guzman for helpful comments, and Greg Jacob for excellent research assistance.

1. *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996).

2. *See* Henry H. Perritt, Jr., *The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance*, 5 IND. J. GLOBAL LEGAL STUD. 423, 436-37 (1998).

3. Perritt, *The Internet as a Threat to Sovereignty*, *supra* note 2, at 426-27. The Internet is "not susceptible to the same physical and regulatory controls as telegraph, telephone, radio, and television technologies." *Id.* at 426. Perritt notes the "difficulty in imposing border controls on Internet communications." *Id.* "The Internet may very well be a direct threat to certain types of conceptions about sovereignty—those that rely on maximum, centralized control over the life of a people." *Id.* *See also* Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 1 (1996) ("Conduct with potentially serious legal consequences is difficult for traditional sovereigns to control in the [Global Information Infrastructure] because it is ephemeral, invisible, and crosses geographical boundaries easily."). However, Perritt is a moderate on this issue. *Compare* Johnson & Post, *supra* note 1.

4. My arguments about the relevance of territorial sovereignty to Internet transactions apply with similar (but not identical) force to national sovereigns and sub-national quasi-sovereigns (such as the several states). Throughout this essay I will use focus on "national" territorial regulation as opposed to "sub-national" territorial regulation unless otherwise indicated.

I. TERRITORIAL SOVEREIGNTY

"Sovereignty" has many meanings. In this essay I analyze the relevance to the Internet of a particular conception of territorial sovereignty. A nation possesses territorial sovereignty in the sense that it exercises *the principal means of authority within a given territory.*[5] Territorial sovereignty so conceived does not commit one to the realist conception of sovereignty that Perritt criticizes.[6] It is consistent with the view that non-governmental organizations and extra-territorial factors significantly influence governmental options and other events within the territory, and that persons and firms can evade regulation by avoiding a territorial presence.[7]

Territorial sovereignty is relevant to Internet regulation in a straightforward fashion. The Internet is not, as many suggest, a separate place removed from our world. Like the telephone, the telegraph, and the smoke signal, the Internet is a medium through which people in real space in one jurisdiction communicate with people in real space in another jurisdiction. Territorial sovereignty supports national regulation of persons within the territory who use the Internet. It also supports national regulation of the means of communication—Internet hardware and software—located in the territory. Finally, a nation's prerogative to control events within its territory entails the power to regulate the local effects of extraterritorial acts.[8] When a person abroad uses the Internet to

---

5. *See* Stephen D. Krasner, *Sovereignty: An Institutional Perspective*, 21 COMP. POL. STUD. 66, 86 (1988) ("The assertion of final authority within a given territory is the core element in any definition of sovereignty."). *Id.* Janice E. Thomson, *Sovereignty in Historical Perspective: The Evolution of State Control over Extraterritorial Violence, in* THE ELUSIVE STATE: INTERNATIONAL AND COMPARATIVE PERSPECTIVES 227, 227 (James A. Caporaso ed., 1989) ("Despite their debate over whether the state is a withering colossus or a highly adaptive entity, international relations theorists agree on an even more fundamental point. Both liberal interdependence and realist theories rest on the assumption that the state controls at least the principal means of coercion."). *Id.* (citations omitted).

6. *See* Perritt, *The Internet as a Threat to Sovereignty, supra* note 2, at 425.

7. *See* Janice E. Thomson & Stephen D. Krasner, *Global Transactions and the Consolidation of Sovereignty, in* GLOBAL CHANGES AND THEORETICAL CHALLENGES: APPROACHES TO WORLD POLITICS FOR THE 1990S 195, 198-206 (Ernst-Otto Czempiel & James N. Rosenau eds., 1989).

8. Some commentators suggest that this effects criterion for local regulation constitutes a rejection of territorial sovereignty as traditionally conceived. *See, eg.*, Larry Kramer, *Vestiges of Beale: Extraterritorial Application of American Law*, 1991 SUP. CT. REV. 179, 202 (1992). To the contrary, however, the traditional territorialists recognized that "[a]cts done outside a jurisdiction, but intended to produce and producing detrimental effects within it, justify a State in punishing the cause of the harm as if he had been present at the effect...." Strassheim v. Daily, 221 U.S. 280, 285 (1911) (Holmes, J.). This point flows from the traditional conception's emphasis on plenary sovereign power within the territory. It is true, however, that the effects test for territorial jurisdiction has greater prominence now than in the late-nineteenth and early-twentieth centuries. Several reasons explain this change. All conflicts of law problems by definition have connections to two or more territorial jurisdictions. A dominant version of traditional territorialism–best represented by Joseph Beale–used

produce harmful local effects, the local sovereign is justified in regulating these local effects.[9] These various forms of legitimate territorial regulation enable nations to significantly raise the cost of, and thus to regulate, proscribed Internet transactions.[10]

The arguments against this view begin with empirical assumptions about Internet architecture.[11] A distinguishing feature of the Internet is that protocol addresses do not necessarily correlate with physical location. This means that persons transacting in cyberspace sometimes cannot know each other's physical location and cannot control the geographical flow of content. In addition, information mediated by many Internet services can appear simultaneously in all jurisdictions around the world. Finally, information transmitted on the Internet can easily flow across national borders without detection.

There are many reasons to question these empirical and technological claims.[12] In this essay I want to focus instead on legal and conceptual arguments against territorial regulation of the Internet. There are three basic

---

undermined Beale's notion of a uniquely legitimate governing law in conflicts cases. The massive increase in transjurisdictional transactions during the late nineteenth and twentieth centuries exacerbated the number and scope of conflicts of law. The rise of the regulatory state led to more caustic public policy differences among states and pressured interested fora to apply local regulations whenever possible. These changes in the world combined with changes in legal and related conceptual understandings. The legal realists demolished Beale's intellectual edifice, and showed that nothing in the logic of territorialism justified legal regulation by any one of several territories that had connections to the transaction in question. *See* WALTER WHEELER COOK, THE LOGICAL AND LEGAL BASES OF THE CONFLICT OF LAWS 311-22, 351-70, 433-37 (1949); ERNEST G. LORENZEN, SELECTED ARTICLES ON THE CONFLICT OF LAWS (1947). The realists successfully argued that any jurisdiction with a sufficient connection to a case can with justification apply its law to the case. This, in a nutshell, is the effects criterion, a criterion that constitutes an expanded conception of territorial sovereignty, not a rejection of the conception.

9. This effects criterion is a pervasive and well-settled feature of domestic and international conflicts of law. *See* Allstate Ins. Co. v. Hague, 449 U.S. 302 (1981). The Constitution permits a state to apply its law if it has a "significant contact or significant aggregation of contacts, creating state interests, such that the choice of its law is neither arbitrary nor fundamentally unfair." *Id.* at 313. Similarly, "[i]nternational law permits nations to regulate extraterritorial activity with local effects." RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE U.S. § 403 (1987).

10. For my more comprehensive analysis, see Jack Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. (forthcoming 1998).

11. *See* Perritt, *Jurisdiction in Cyberspace*, *supra* note 3, at 1-2; Johnson & Post, *supra* note 1, at 1370-76.

12. For example, the central empirical assumption that Internet content providers cannot control where and to whom their content flows is either misleading or wrong. *See* Goldsmith, *Against Cyberanarchy*, *supra* note 10. Content providers can control these flows through a variety of means ranging from conditioning access on presentation of age or geographical identification to labeling and rating for filtering software. These and other forms of information flow control are neither perfect nor costless. But neither is control over the transjurisdictional effects of non-Internet activities. Moreover, the accuracy of Internet content control is rapidly rising, and the costs of such control are rapidly diminishing. Although technological predictions in this context are perilous, there is presently every reason to believe these trends will continue. For further analysis, see *id.*

arguments to this effect.[13] First, territorial regulation of the Internet is not feasible because the source of Internet transactions can easily be located outside of the regulating sovereign's territory. Second, unilateral territorial regulation of the Internet leads to overlapping and often inconsistent regulation of the same transaction. Third, unilateral territorial regulation of the Internet produces significant, normatively problematic spillover effects. I consider each argument in turn.

II. REGULATION EVASION

The first argument against territorial regulation of the Internet concerns regulatory leakage. This is an argument about the infeasibility of territorial regulation of the Internet. Because Internet information flows cross territorial borders without detection, and because Internet content providers can shift with relative ease the source of their information flows outside of any regulating territory,[14] much of the content of the Internet is beyond the regulatory scope of any particular territorial sovereignty.

It is true that it is costly (but not impossible)[15] to arrest the flow of Internet protocol packets over territorial borders. It is also true that these information flows often have an extraterritorial source. But these features do not distinguish the Internet from real space transnational transactions for which territorial regulation is a common and effective tool. Persons acting abroad often do things that cause adverse effects within the regulating jurisdiction that cannot be intercepted at the border. For example, when English reinsurers conspire in England to limit the types of reinsurance sold in the United States, U.S. customs

13. An extreme statement of these arguments is found in Johnson & Post, *supra* note 1. For a more nuanced assessment, see Perritt, *Jurisdiction in Cyberspace*, *supra* note 3.

14. Content providers can do this by, among other ways, locating physically beyond the regulating jurisdiction or by employing technology like telnet or anonymous remailers.

15. For example, China regulates access to the Internet through (among other means) centrally regulated servers. *See China Tightens Control Over Internet*, INDEPENDENT (UK), Dec. 31, 1997 ("All locally-dialed internet servers available in China must send traffic leaving the country through nodes controlled by the Ministry of Post and Telecommunications and there is widespread belief that targeted screening of this internet use is routine."). Perritt acknowledges this point. *See* Perritt, *The Internet as a Threat to Sovereignty*, *supra* note 2, at 426. *See also* Timothy S. Wu, *Cyberspace Sovereignty? – The Internet and the International System*, 10 HARV. J. L. & TECH. 647, 652 (1997).

officials cannot stop the harm to American insurers and insureds at the border.[16] The local economic harm of foreign activity is similarly impossible to stop at the border when a foreign corporation makes a fraudulent tender offer on foreign soil for a foreign corporation owned in very small part by Americans.[17] In the modern interdependent international economy, these economic effects are oblivious to border control. The point is not limited to economic effects. Harmful pollution that wafts from one state into another is also difficult to intercept at the state line.[18]

Does the inability of governments to stop these harmful effects at the border mean that the extraterritorial sources of these local harms are beyond local regulation? Of course not. Some harmful effects cannot be intercepted at the border and thus must be regulated *ex post* through legal sanctions (or *ex ante* through the threat of such sanctions). In each of the three non-Internet examples above, for example, the jurisdiction that suffered the harmful effects applied its laws to the extraterritorial activity. Internet activities are functionally identical to these non-Internet activities. People in one jurisdiction do something—upload pornography, facilitate gambling, offer a fraudulent security, send spam, etc.—that is costly to stop at another jurisdiction's border and that produces effects within that jurisdiction deemed illegal there. The territorial effects rationale for regulating these harms is the same as the rationale for regulating similar harms in the non–Internet cases. The medium by which the harm is transmitted into the regulating jurisdiction—be it economic interdependence, postal mail, wind currents, or the Internet—is not relevant to the justification for regulating it.

The effects criterion tells us that it is legitimate for a nation to apply its regulation to an extraterritorial act with harmful local effects. It does not tell us whether such a regulation will be efficacious. In most instances, regulation of extraterritorial activity is efficacious only to the extent that the agents of the acts have a local presence or local property against which local laws can be enforced. In this sense, the concept of the extraterritoriality can be misleading. It does not (usually) mean that a nation enforces its law abroad. Rather, it means that a nation uses the threat of force against local persons or property to punish, and thus regulate, extraterritorial acts that cause local harms. If the

---

16. *See* Hartford Fire Ins. Co. v. California, 509 U.S. 764 (1993).

17. *See* Consolidated Gold Fields PLC v. Minorco, S.A., 871 F.2d 252, *modified* 890 F.2d 569 (2d Cir. 1989).

18. *See* Georgia v. Tennessee Copper Co., 237 U.S. 474 (1915). *Cf.* Trail Smelter Case (U.S. v. Canada), 3 R.I.A.A. 1911 (1949).

extraterritorial source has no local presence or property, the efficacy of the local regulation is diminished (but, as we shall see in a moment, not eliminated). In this sense the enforceable scope of a local regulation is much more significant than its putative scope. And the enforceable scope is largely limited by the old-fashioned conception of territorial sovereignty: a nation has plenary enforcement jurisdiction over persons and property within its borders but little if any beyond.[19]

The relative importance of the enforceable (as opposed to the putative) scope of a regulation is often not noticed with respect to extraterritorial regulation of non-Internet activities. Nor are the largely territorial limitations on this scope. This is probably because in non-Internet cases the extraterritorial source of local harm is frequently a firm with some local presence (property, employees, business contracts) against which the local regulating jurisdiction can assert leverage in trying to alter extraterritorial behavior. For example, the United States can apply its antitrust laws to alter the acts of English reinsurers in London because these reinsurers have widespread contractual relations with American firms that they want to preserve.[20] Similarly, the European Community can impose strict and almost deal-breaking conditions on a Federal Trade Commission-approved merger between two U.S. companies with no manufacturing facilities in Europe because of the many offices, agents, and contracts that the U.S. companies have in Europe.[21] In both cases the foreign company subject to local regulation has a local business presence that is more beneficial than the costs of local regulation; otherwise, the foreign company would eliminate its presence in the regulating jurisdiction and avoid the regulation.

At first glance, the architecture of the Internet transactions appears to differ from real space in a way that makes regulatory leakage a more serious problem. For the Internet makes it very easy and very inexpensive for *individuals* outside the regulating jurisdiction to send harmful content into the regulating jurisdiction that is difficult to intercept at the border. Since individuals abroad rarely have local presence or assets, it appears that many local regulations of Internet activity will be inefficacious. As James Boyle puts the point: "If the king's writ reaches only as far as the king's sword, then much of the content of

---

19. I set aside for present purposes one relatively rare method of extraterritorial enforcement: military invasion. *See, e.g.*, United States v. Noriega, 746 F. Supp. 1506 (S.D. Fl. 1990).

20. *See Hartford Fire*, 509 U.S. at 796.

21. *See McDonnell Douglas-Boeing Link Gets Europe Approval*, N.Y. TIMES, July 31, 1997, at D4; Edmund L. Andrews, *Boeing Concession Averts Trade War With Europe*, N.Y. TIMES, July 24, 1997, at D1.

the Net might be presumed to be free from the regulation of any *particular* sovereign."[22]

This phenomenon—which we might label *offshore regulation evasion*—is not limited to the Internet. For example, corporations reincorporate in jurisdictions with favorable internal affairs laws, and drug lords send cocaine into the United States from South America. Closer to point, offshore regulation evasion has been a prominent characteristic of other communication media.[23] For example, Radio-Free Europe broadcast into the U.S.S.R. but lacked a regulatory presence there; television signals are sometimes broadcast from abroad by an entity with no local presence; and a person living in one country can libel a person in another via telephone. Like the content source of many Internet transactions, the extraterritorial source of these and many other non-Internet activities is often beyond the enforceable scope of local regulation. However, this does not mean that local regulation is inefficacious. In cyberspace, as in real space, offshore regulation evasion does not prevent a nation from indirectly regulating extraterritorial activity that has local effects.

The reason once again has to do with territorial sovereignty as traditionally conceived. A nation retains the ability to regulate the extraterritorial sources of local harms through regulation of persons and property within its territory. This form of indirect extraterritorial regulation is how nations have, with various degrees of success, regulated local harms caused by other communications media with offshore sources and no local presence.[24] It is also how nations have begun to regulate local harms caused on the Internet by extraterritorial content providers. For example, nations penalize in-state end-users who obtain and use illegal content or who otherwise participate in an illegal cyberspace transaction.[25] They also regulate the local means through which foreign content is transmitted. For example, they regulate in-state entities

---

22. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors*, 66 U. CIN. L. REV. 177, 179 (1997).

23. *See generally* Stephen D. Krasner, *Global Communications and National Power: Life on the Pareto Frontier*, 43 WORLD POL. 336 (1991).

24. *See id.* at 340.

25. *See, e.g.*, *Computer Information Network and Internet Security, Protection and Management Regulations* (Approved by the State Council on Dec. 11, 1997 and promulgated by the Ministry of Public Security on Dec. 30, 1997) (visited Apr. 6, 1998) http://www.gilc.org/speech/china/net-regs-1297.html (describing Chinese law proscribing criminal punishment for in-state users who access or transmit prohibited conduct); Internet Gambling Prohibition Act, H.R. 2380, S. 474, 105th Cong. (1997) (pending bill that provides for punishment of persons in the United States who engage in Internet gambling).

that supply or transmit information.[26] Or they regulate in-state hardware and software through which Internet transmissions are received.[27] These and related local regulations affect the cost and feasibility within the regulating nation of obtaining content from, or participating with, offshore regulation evaders. In these ways, local regulations indirectly regulate extraterritorial content supply.

In both the Internet and non-Internet contexts, such indirect regulation will rarely be perfect in the sense of eliminating evasion. But of course few if any regulations are perfect in this sense. And regulation need not be perfect to be effective.[28] The question is always whether the regulation will heighten the costs of the activity sufficiently to achieve its acceptable control from whatever normative perspective is deemed appropriate. Whether indirect regulation of Internet content transmitted from abroad will achieve acceptable control depends on one's normative commitments and on empirical and technological questions that remain unresolved.

There are several reasons to believe that Internet regulation will be at least

---

26. For example, a new German law imposes liability on Internet access providers "if they are aware of [illegal] content" and fail to use "reasonable and technically possible" means to block it. *Germany to Enforce Child-Friendly Internet*, CHI. TRIB., July 5, 1997, at 4. Australia is about to implement a similar law. *See* Electronic Foundation Frontier, *Internet Regulation in Australia* (visited Apr. 6, 1998) http://www.efa.org.au /Issues/Censor/cens1.html. Similarly, Internet service providers have been held liable in the United States for facilitating the transmission of content deemed illegal in the regulating jurisdiction. *See* Stratton-Oakmont, Inc. v. Prodigy Service Co., 1995 WL 323710 (Sup. Ct. N.Y. May 24, 1995). *See also* Internet Gambling Prohibition Act, H.R. 2380, S. 474 (authorizing federal authorities to order Internet service providers to shut down offending gambling sites).

27. Several Middle Eastern and Asian countries have taken these steps. *See* Madanmohan Rao, *Persian Gulf Net Censorship: Governments Force Server Blockades*, (visited March 23, 1998) http://mediainfo. elpress.com/ephome/news/newshtm/webnews/glob1003.htm (discussing how Middle Eastern states have set up "software blockades and proxy servers" to control Internet content flows); Wu, *supra* note 15 (describing similar measures in Singapore and China). Many believe that the United States will impose similar, but perhaps more modest, restraints. *See* Boyle, *supra* note 22, at 179. *See also* Lawrence Lessig, *What Things Regulate Speech* (visited Oct. 22, 1997) <http://www/si.umich.edu/prie/tprc/abstracts97/lessig.pdf>. The FCC has already required the television V-chip to be placed in all computers capable of receiving broadcast transmissions. *See FCC Ruling Gives Go-ahead to Tri-Vision's V-Chip*, FINANCIAL POST, Mar. 13, 1998, at 3.

28. As Lessig correctly argues:

> A regulation need not be absolutely effective to be sufficiently effective. It need not raise the cost of the prohibited activity to infinity in order to reduce the level of that activity quite substantially. If regulation increases the cost of access to this kind of information, it will reduce access to this information, even if it doesn't reduce it to zero. That is enough to justify the regulation. If government regulation had to show that it was perfect before it was justified, then indeed there would be little regulation of cyberspace, or of real space either. But regulation, whether for the good or the bad, has a lower burden to meet.

See Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1405 (1996).

modestly successful. Territorial regulatory regimes governing pornography, encryption, and trademark (among many other things) have significantly affected Internet activity to date, and the vehement opposition to various forms of territorial regulation of the Internet suggests that such regulation will continue to make certain Internet activities prohibitively costly. In addition, governments have successfully "embed[ed] or hardwire[d] the legal regime in the technology itself" in numerous other communications contexts.[29] Again, the impassioned opposition to various attempts at this latter form of Internet regulation suggests that a similar strategy might have efficacy here as well.[30] In addition, many nations have a common interest in regulating many types of Internet transactions such as fraud, criminal activity, certain forms of anti-competitive activity, and so forth. If other communications media are any guide, international regulatory harmonization is likely under these conditions and might minimize regulatory leakage.[31] And, as Perritt notes, the Internet likely facilitates rather than undermines this international harmonization process.[32]

III. SIMULTANEOUS UNIVERSAL REGULATION

I have focused thus far on the claim that territorial regulation of the Internet is unfeasible. My arguments might appear to support a somewhat different type of anti-regulation claim. This is the claim that because Internet content can simultaneously appear in every territorial jurisdiction in the world, all Internet activity is simultaneously subject to all national regulations. This appears to lead to the normatively problematic conclusion that all "Web-based activity .

29. Boyle, *supra* note 22, at 180. *See also* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996).

30. *See* American Civil Liberties Union, *Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet* (visited April 12, 1998) http://www.aclu.org/issues/cyber/burning.html; Lawrence Lessig, *Tyranny in the Infrastructure*, WIRED, July 1997, at 46.

31. *See* Krasner, *supra* note 5.

32. *See* Perritt, *Jurisdiction in Cyberspace*, *supra* note 3. To some extent the need for international harmonization is an acknowledgment of the limitations of a purely territorial approach to regulation. These limitations inhere in territorial regulation of just about all transnational transactions. The demand for international harmonization is not new to the Internet.

. . must be subject simultaneously to the laws of all territorial sovereigns."[33]

We shall see in a moment that territorial regulation of Internet transactions does not in fact lead to simultaneous universal regulation of the Internet. It is worth noting, however, that one jurisdiction's legitimate regulation of the harmful local effects of extraterritorial activity does not become normatively problematic simply because the harm-producing activity also produces harmful effects in many other jurisdictions and is thus subject to territorial regulation there as well. It is uncontroversial that pollution emitted in State A that wafts into State B can be regulated by State B. State B's regulation does not become less legitimate because the pollution also causes damage in States C-Z. This is true even if the agent of the pollution does not know which way the wind blows and thus does not know the states into which the pollution will travel.

The same analysis applies to the Internet. A government's regulation of the harmful local effects of an Internet transaction does not become less legitimate because the effects of the same transaction are regulated differently in other jurisdictions where these effects appear. These multiple regulation scenarios raise a normative concern because of the spillover effects of each nation's Internet regulation. As we will examine below, these spillovers might call for multijurisdictional harmonization. But by themselves they do not make unilateral regulation illegitimate.

The problem of notice presents another apparent normative quagmire for Internet regulation. Many fear that content providers do not know where in the world their information goes, and thus do not have notice of the laws they might be violating. This problem too is greatly exaggerated. First, the limits on enforcement jurisdiction mean that most individual content providers never have to worry about violating foreign laws. Second, content providers can take steps—such as conditioning access to content on presentation of geographical identification—to control content flows geographically. As digital signature and filtering technology continues to develop to facilitate such geographical identification, the Internet content provider will look like any other "real space" content provider who must take care not to send his content into a jurisdiction where it is illegal. Third, even in the absence of such technology, a content provider is on notice that his information might flow into a jurisdiction where it is illegal. It is a complicated question beyond the scope of this essay whether this notice suffices to make it fair to impose an obligation on the content provider to learn whether this information is illegal in the regulating territory.

---

33. Johnson & Post, *supra* note 1, at 1374.

Ignoring for the moment the limits on enforcement jurisdiction and the availability of geographical flow control devices, such a regime places enormous burden on content providers that might significantly curtail Internet activity. But there is nothing sacrosanct about Internet speed, or about a foreign content provider's right to send information everywhere in the world with impunity. From the perspective of the regulating jurisdiction, the content provider is knowingly sending information into a jurisdiction; like all persons who do the same in real space, the content provider benefits from this in-state activity, is deemed to know the law of the territory, and is subject to penalties for non-compliance (assuming that enforcement is possible).[34]

In any event, this quagmire is much less significant than it appears. The claim that unilateral national regulation of the Internet invariably leads to simultaneous (and oft-conflicting) regulation of the Internet is as exaggerated as the claim about the unfeasibility of territorial regulation of the Internet. And for the same reason: traditional territorial sovereignty. As explained above, a nation cannot enforce its laws against an individual content provider from another country unless the content provider has a local presence. The vast majority of individuals who transact on the Internet have no presence or assets in the jurisdictions that wish to regulate their information flows. Such regulations will apply mainly to service providers and users with a physical presence in the regulating jurisdiction. And indeed this has been the focus of regulation to date.[35]

There is another class of content providers that have been subject to territorial regulation. These are extraterritorial content providers over whom a nation or state can legitimately obtain personal jurisdiction *and* against whom a nation or state can enforce a default judgment in a jurisdiction where the

34. For a more comprehensive analysis of this point, see Goldsmith, *Against Cyberanarchy*, *supra* note 10.

35. Even with these limitations, an individual content provider in one jurisdiction faces *potential* liability in another jurisdiction when she places information on the web. This potential liability can become an unforeseen reality when the provider travels to the regulating jurisdiction, or moves assets there. Such potential liability in turn might affect the providers' activities at home. This form of regulation is a theoretical possibility, but should not be exaggerated. No nation has as yet imposed liability on a content provider for unforeseen effects in an unknown jurisdiction; and the threat of such liability will lessen as content providers continue to gain cost-effective means to control information flows. Even this potential threat of liability is relatively insignificant and does not approach the feared claims of massive multiple regulation of individual Internet users.

provider has assets or presence.[36] In the international context this will happen rarely for, among other reasons, nations do not usually enforce foreign default judgments based on the application of foreign regulations to activity that was legal where it took place.[37] The situation is more complicated in the domestic interstate context, because the Full Faith and Credit Clause requires one state to enforce default judgments rendered by another state with personal jurisdiction over the defendant. This threat is attenuated, however, by constitutional limits on a state's ability to assert personal jurisdiction. The large majority of courts that have considered the issue have required something more than mere placement of information on a web page in one state as a basis for personal jurisdiction in another state where the web page is accessed.[38] This effectively means that a content provider in one state will not be subject to personal jurisdiction in another unless she knowingly directs content to a particular jurisdiction where the content is illegal. In this circumstance, the rationale for asserting personal jurisdiction is precisely the same as in real space—the person subject to jurisdiction directed activity toward a jurisdiction and gained benefits from those contacts. It is thus fair to require that entity to adjudicate disputes arising out of these contacts in that jurisdiction.

In sum, the largely territorial limits on enforcement jurisdiction attenuate the concern that individual content providers will be exposed to multiple regulatory regimes. A nation can indirectly regulate extraterritorial content providers through laws aimed at local entities or property; but direct regulation of extraterritorial providers—in the sense of imposing liability or punishment on such providers—will rarely succeed.

---

36. A jurisdiction can also enforce its laws against persons whom it can successfully extradite. However, extradition in Internet contexts will likely be rare. In the domestic interstate context, the obligation for one state to extradite to another only extends to persons who were *physically present* in the demanding state at the time of the crime's commission. This jurisdictional limitation does not apply, of course, when a person in one state commits a federal crime in another. *See, e.g.*, United States v. Thomas, 74 F.3d 701 (6th Cir. 1996). A different, but equally forceful, limitation applies to international extradition. The principle of double criminality that pervades modern extradition treaties requires that the offense charged be criminal in both the requesting and the requested jurisdiction; this makes it unlikely that there will be international cooperation in the enforcement of exorbitant unilateral criminal regulations of cyberspace events. For elaboration of these points, see Goldsmith, *Against Cyberanarchy, supra* note 10.

37. *See* GARY BORN, INTERNATIONAL CIVIL LITIGATION IN UNITED STATES COURTS (1996).

38. *See* Eric Schneiderman & Ronald Kornreich, *Personal Jurisdiction and Internet Commerce*, N.Y. L.J., June 4, 1997, at A1; Note, *World-Wide Volkswagen, Meet the World Wide Web: An Examination of Personal Jurisdiction Applied to the New World*, 71 ST. JOHN'S L. REV. 403 (1997).

IV. SPILLOVER EFFECTS

My basic claims so far have been that (a) territorial regulation of persons and property are a legitimate and effective way to regulate local harms caused from abroad via the Internet, but that nonetheless (b) the limits of territorial sovereignty mean that individual content providers abroad have little to fear from violating local laws in jurisdictions where their content might appear. Proposition (b) should not be taken to mean that Internet users outside of the regulating jurisdiction are immune from the effects of local regulation. As the preceding discussion of indirect regulation suggests, Internet users outside the regulating jurisdiction can be affected by the local regulation to the extent that they are dependent on users, service providers, or content providers with a presence in the regulating jurisdiction. In this way local regulation of the Internet produces spillover effects on persons outside of the regulating jurisdiction, as well as on the regulatory efforts of other countries.[39]

A prominent example of these spillover effects is Germany's threat to prosecute CompuServe for carrying on-line discussion groups that violated German anti-pornography laws.[40] CompuServe responded to the threat by blocking access to these discussion groups in Germany. However, because of the state of the Internet's architecture, this action had the effect of blocking access to these discussion groups for CompuServe users in other jurisdictions where these discussion groups were legal. The German regulation thus produced massive spillover effects. Most normative perspectives frown on a nation that exports the costs of its regulation to other nations whose citizens have no voice in the enactment or enforcement of the regulation. These spillovers make territorial regulation of the Internet appear normatively unattractive.

The spillover concern is genuine. But on several grounds its significance should not be overstated. As an initial matter, spillovers like those produced in the CompuServe episode are premised to a great degree on the empirical claim that content providers and Internet service providers cannot control the real space geographical flow of Internet content. This claim is false. Content flow is today controlled geographically through a variety of means ranging from

---

39. I will assume for purposes of argument that these spillover effects are negative.

40. *See* Edmund L. Andrews, *Germany's Efforts to Police Web are Upsetting Business*, N.Y. TIMES, June 6, 1997, at A1; *Sex on the Internet: When Bavaria Wrinkles its Nose, Must the Whole World Catch a Cold?*, ECONOMIST, Jan. 6, 1996, at 18.

conditioning access to content on geographical identification, to centralized servers, to mandated end-user filtering, to the imposition of the severe penalties for uploading or downloading prohibited information. The question is not whether the architecture of the Internet can be modified to permit greater geographical content discrimination; the question is the cost of modification and the degree of effectiveness. The intense demand by Internet users, content providers, service providers, and regulating jurisdictions to reduce such spillovers is driving the development of technologies that lower the costs of discrimination and increase its effectiveness. The sufficiency of these developments will depend on yet unanswered empirical and technological issues. The point is that it is wrong to say that control is impossible; here as elsewhere the feasibility of control is a question of the importance to the sovereign of control and the costs of imposing such control.

Even assuming the worst about the feasibility of geographic content control of Internet information flows, spillover effects caused by territorial regulation of the Internet do not undermine the legitimacy of such regulation. As the traditional territorialists realized,[41] spillover effects are an inevitable consequence of unilateral territorial regulation of transnational transactions. For example: When a security sold legally in Japan violates U.S. securities laws, the application of the anti-fraud provisions of the U.S. securities regulations produce spillover effects by making this extraterritorial activity more costly, and by diminishing the force of Japanese law on Japanese soil. If instead Japanese law governed the situation, persons in the United States would have been harmed and U.S. regulations undermined. The same point applies to unilateral regulation of the Internet. Spillovers are present when activity deemed legal in one country causes harm deemed illegal in another, regardless of which nation's law applies. These spillovers can be diminished through international harmonization. But they can only be eliminated by abolishing national (as opposed to international) lawmaking entities altogether, or by eliminating transnational activity. Neither option is remotely plausible. In this

41. Both Joseph Story and Ulrich Huber, for example, contemplated that purely territorial regulations would have indirect extraterritorial effects. *See* JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS § 20 (3d ed. 1846) (arguing that no state can "*directly* affect or bind property out of its own territory) (emphasis added); Ulrich Huber, *De Conflictu Legum Diversarum in Diversis Imperiis [Of the Conflict of Diverse Laws in Diverse Governments]* (1689), *translated in* ERNEST LORENZEN, *supra* note 8, at 163-64 ("laws of one nation can have no force *directly* within another.") (emphasis added).

sense the spillovers from territorial regulation of the Internet are inevitable.[42]

Of course the spillover effects from territorial regulation can be great or small, and one might think that they will be especially great when territorial sovereigns regulate the Internet. The size of the spillover effects from territorial regulation of Internet information flows ultimately depends on the development of filtering and identification technology, and on the scope of international harmonization. Independent of these factors, however, it is important to see why the existence of spillovers alone does not undermine the legitimacy of territorial regulation.

Consider a hypothetical Arkansas statute that bans Internet gambling and imposes very large criminal fines on Internet Access providers that facilitate transmission of Internet gambling services into the state. When zealous local officials in West Memphis, Arkansas use America Online (AOL) to gain access to Internet gambling web pages that violate the statute, they threaten to prosecute the company. The company decides to shut down access to the offending Web page rather than face prosecution. Because of the state of Internet technology, this has the consequence of shutting off access to the page by all AOL users around the globe. West Memphis officials seem justified in applying the Arkansas law on territorialist grounds. They would be able to regulate this gambling if the roulette wheel or poker table were physically present in Arkansas, or if the gambling were facilitated by interstate telephone; the medium that transmits the effects of gambling into the state does not appear relevant to the territorialist justification of the regulation. But is it *fair* for West Memphis officials to govern the world in this way?[43]

I believe so. As for fairness to AOL: the company receives financial and other benefits from its presence (servers, offices, clients) in Arkansas. Without this presence, West Memphis enforcement threats would be empty. AOL need not remain in Arkansas. It could leave. Its decision to stay and comply with Arkansas regulations might increase the price of its services in Arkansas and elsewhere. For AOL, this is a cost of doing business via the Internet. Such

---

42. Most prominent academic choice-of-law methodologies aim to minimize these spillovers while at the same time preserving the sovereign prerogative to regulate effects within national borders. This is the goal, for example, of such different approaches as the interest-balancing approach, RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW, *supra* note 9, § 403, William Baxter's comparative impairment approach, William Baxter, *Choice of Law and the Federal System*, 16 STAN. L. REV. 1 (1963), Larry Kramer's multistate canons of construction, Larry Kramer, *Rethinking Choice of Law*, 90 COLUM. L. REV. 277 (1990), and Lea Brilmayer's strategy to maximize state policy objectives, LEA BRILMAYER, CONFLICT OF LAWS 169-218 (2d ed. 1995).

43. *Cf.* Buchanan v. Rucker, 9 East 192 (King's Bench 1808) ("Can the Island of Tobago pass a law to bind the rights of the whole world?").

costs are driving development of Internet filtering technology that will enable geographical and related discrimination on the Internet. But in the absence of such technology, application of the Arkansas law appears to fall within traditional reciprocity-based justifications for regulating local effects. AOL voluntarily chooses to do business in Arkansas and receives many benefits from this business; it must therefore accept the burdens of Arkansas's (non-discriminatory) state regulation.

As for fairness to AOL users outside of Arkansas: the Arkansas regulation does not unfairly burden them either. They remain free to choose among scores of Internet access providers that are not affected by the Arkansas regulation. More importantly, the spillover concern cuts in both directions. The Arkansas regulation produces spillover effects abroad; but extraterritorial acts of providing gambling services to in-state users produces spillover effects in Arkansas. Even if spillover minimization were the criterion of legitimacy for territorial regulation of harmful local effects (which it is not), the Arkansas regulation would not be illegitimate unless the costs of the regulation, including the balance of positive and negative spillover effects abroad, were greater than the costs of non-regulation (including the in-state costs of the gambling).

There is a final important point about the spillover effects of territorial regulation of the Internet. Spillover minimization is not the criterion measure of a territorial regulation's legitimacy. Even if it were, it would not follow that Internet transactions should be self-regulated rather than regulated by territorial sovereigns.[44] This is so for two reasons. First, the most effective way to reduce or eliminate these spillovers is through international harmonization. Second, in the absence of international harmonization it will often be the case that Internet self-regulation produces more significant negative spillover effects on non-Internet participants than the national regulations designed to minimize these spillovers. The Internet is not a self-contained medium. It produces real world harms—harms that Internet users have failed to internalize, and that governments legitimately regulate.

---

44. For arguments to this effect based on the spillover-reduction criterion, see David Post, *Governing Cyberspace*, 43 WAYNE ST. L. REV. 155 (1996); David Post, *"Chaos Prevailing on Every Continent": A New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L. REV. (forthcoming 1998).

CONCLUSION

Beginning with the invention of the telegraph in the nineteenth century, commentators have predicted that each new communication advance would undermine the nation-state. None of these predictions has proven to be true. Like other communications breakthroughs, the Internet will affect the way individuals interact and thus the way nations regulate. However, for many of the reasons expressed in Dean Perritt's article, the Internet is no more likely to undermine national sovereignty than did the telephone or satellite or television. I have tried to alleviate Perritt's residual concerns about the legitimacy and effectiveness of territorial legal regulation of the Internet. Territorial regulation faces pressure from a variety of modern factors. But it remains the dominant method for regulating all transnational transactions in our interdependent world, including Internet transactions.

Such territorial regulation is invariably messy. I have tried to explain why regulatory leakage, though inevitable to some degree, does not undermine the effectiveness of territorial regulation. I have also tried to show why spillover effects, though also inevitable, do not undermine the legitimacy of territorial regulation. International harmonization is a solution to both problems. But harmonization is not a perfect solution because it is sometimes hard to achieve and, more broadly, because it defeats the benefits of decentralized national lawmaking. For these reasons, among others, territorial regulation will remain a central component of Internet regulation.