Against Cyberanarchy

Jack L. Goldsmith†

The Supreme Court's partial invalidation of the Communications Decency Act on First Amendment grounds[1] raises the more fundamental question of whether the state can regulate cyberspace at all.[2] Several commentators, whom I shall call "regulation skeptics," have argued that it cannot.[3] Some courts have also expressed skepticism.[4] The popular and technical press are full of similar claims.[5]

---

† Associate Professor of Law, The University of Chicago. For their comments and discussion, I thank Bill Arms, Caroline Arms, Curtis Bradley, Stephen Choi, Richard Craswell, David Currie, Larry Downes, Richard Epstein, Michael Froomkin, Elizabeth Garrett, Andrew Guzman, Larry Kramer, Larry Lessig, Doug Lichtman, Richard Posner, David Post, Cass Sunstein, Tim Wu, and participants at workshops at the University of Chicago and the University of California (Boalt Hall). I also thank Kyle Gehrmann and Greg Jacob for excellent research, and the Arnold and Frieda Shure Research Fund for support.

[1] See Communications Decency Act of 1996 ("CDA"), Pub L No 104-104, 110 Stat 133, codified at 47 USCA §§ 223, 230, 303, 560-61, 609 (1991 & Supp 1998); *Reno v ACLU*, 117 S Ct 2329, 2346 (1997) (holding that CDA's prohibition on Internet transmission of indecent or offensive messages to minors violates the First Amendment).

[2] I shall use the terms "state," "nation," and "jurisdiction" interchangeably to refer to national, as opposed to subnational, legal authority. I shall indicate when the analysis differs for subnational units. Although the term "cyberspace" has a broader meaning, I shall use it here loosely as a synonym for the Internet—the transnational network of computer networks.

[3] See James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U Cin L Rev 177, 178 (1997) ("For a long time, the Internet's enthusiasts have believed that it would be largely immune from state regulation."). The leading regulation skeptics, and this Article's primary targets, are David Post and David Johnson. See David R. Johnson and David Post, *Law And Borders—The Rise of Law in Cyberspace*, 48 Stan L Rev 1367, 1367 (1996). See also David Post and David R. Johnson, *Borders, Spillovers, and Complexity: Rule-making Processes in Cyberspace (and Elsewhere)*, draft presented at the Olin Law & Economics Symposium on "International Economic Regulation" at Georgetown University Law Center (Apr 5, 1997) (copy on file with U Chi L Rev); David Post and David R. Johnson, *The New 'Civic Virtue' of the Internet* (also published in *The Emerging Internet*, Feb 1998, the Annual Review of the Institute for Information Studies), available online at <www.cli.org.paper4.htm> (visited Sept 28, 1998); David G. Post, *Governing Cyberspace*, 43 Wayne L Rev 155 (1996); David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J Online L, Article 3, available online at <www.wm.edu/law/publications/jol/post.html> (visited Sept 10, 1998). Commentators who have made similar arguments include John T. Delacourt, *The International Impact of Internet Regulation*, 38 Harv Intl L J 207 (1997); John Parry Barlow, *A Cyberspace Independence Declaration*, available online at <www.eff.org/barlow> (visited Sept 10, 1998); Dan L. Burk, *Federalism in Cyberspace*, 28 Conn L Rev 1095 (1996); Joel R. Reidenberg, *Governing Networks and Rule-making in Cyberspace*, 45 Emory L J 911 (1996).

[4] See, for example, *ACLU v Reno*, 929 F Supp 824, 832 (E D Pa 1995), affd, 117 S Ct

The regulation skeptics make both descriptive and normative claims. On the descriptive side, they claim that the application of geographically based conceptions of legal regulation and choice of law to a-geographical cyberspace activity either makes no sense or leads to hopeless confusion. On the normative side, they argue that because cyberspace transactions occur "simultaneously and equally" in all national jurisdictions, regulation of the flow of this information by any particular national jurisdiction illegitimately produces significant negative spillover effects in other jurisdictions. They also claim that the architecture of cyberspace precludes notice of governing law that is crucial to the law's legitimacy. In contrast, they argue, cyberspace participants are much better positioned than national regulators to design comprehensive legal rules that would both internalize the costs of cyberspace activity and give proper notice to cyberspace participants. The regulation skeptics conclude from these arguments that national regulators should "defer to the self-regulatory efforts of Cyberspace participants."[6]

This Article challenges the skeptics' arguments and their conclusion. The skeptics make three basic errors. First, they overstate the differences between cyberspace transactions and other transnational transactions. Both involve people in real space in one territorial jurisdiction transacting with people in real space in another territorial jurisdiction in a way that sometimes causes real-world harms. In both contexts, the state in which the harms are suffered has a legitimate interest in regulating the activity that produces the harms. Second, the skeptics do not attend to the distinction between default laws and mandatory laws. Their ultimate normative claim that cyberspace should be self-regulated makes sense with respect to default laws that, by definition, private parties can modify to fit their needs. It makes much less sense with respect to mandatory or regulatory laws that, for paternalistic reasons or in order to protect third parties, place limits on private legal ordering. Third, the skeptics underestimate the potential of traditional legal tools and technology to resolve the multijurisdictional regulatory problems impli-

---

2329, 2348 (1997); *Digital Equipment Corp v Altavista Technology, Inc*, 960 F Supp 456, 462 (D Mass 1997); *American Libraries Associations v Pataki*, 969 F Supp 160, 170 (S D NY 1997).

[5] See, for example, Thomas E. Weber, *The Internet (A Special Report): Debate: Does Anything Go? Limiting free speech on the Net*, Wall Street J (Dec 8, 1997); Vinton G. Cerf, *Building an Internet Free of Barriers*, NY Times § 3 p 12 (July 27, 1997); George Black, *Call for Controls: The Internet Must Regulate Itself*, Fin Times part 4 p 12 (Apr 1, 1998).

[6] Johnson and Post, 48 Stan L Rev at 1367 (cited in note 3).

cated by cyberspace. Cyberspace transactions do not inherently warrant any more deference by national regulators, and are not significantly less resistant to the tools of conflict of laws, than other transnational transactions.

Some caveats are in order up front. This Article argues only that regulation of cyberspace is feasible and legitimate from the perspective of jurisdiction and choice of law. It does not argue that cyberspace regulation is a good idea, and it does not take a position on the merits of particular regulations beyond their jurisdictional legitimacy. For example, it does not examine whether particular national regulations of the Internet promote democracy, or are efficient, or are good or bad for humanity. Similarly, the Article does not consider substantive limitations on cyberspace regulation such as may be found in the Bill of Rights or international human rights law. Resolution of these substantive regulatory issues turns in part on contested normative judgments and difficult context-specific, cost-benefit analyses that are far beyond this Article's scope. But resolution of these issues also turns on how we understand the jurisdictional confusions that arise when national regulation, which has traditionally been understood primarily in geographical terms, applies to a phenomenon that appears to resist geographical orientation. This jurisdictional puzzle is the focus of this Article.

In addition, the Article does not deny that the new communication technologies known as cyberspace will lead to changes in governmental regulation. Such changes are to be expected when the speed of communication dramatically increases and the cost of communication dramatically decreases. The invention of the telegraph, the telephone, the radio, the television, and the satellite, among many other communications advances, all possessed these characteristics. And they all gave rise to societal and regulatory changes.[7] So too will cyberspace. But the skeptics claim much more than that cyberspace necessitates changes in governmental regulation. They claim that cyberspace is so different from other communication media that it will, or should, resist all governmental regulation. My aim here is to show why this claim is flawed, and to explain in general terms how traditional tools of jurisdiction and choice of law apply to cyberspace transactions.

Section I of the Article summarizes the regulation skeptics' claims. Section II provides a richer account than the skeptics of

---

[7] See generally Irwin Lebow, *Information Highways and Byways: From the Telegraph to the 21st Century* (IEEE 1995); Dan Lacy, *From Grunts to Gigabytes: Communications and Society* (Illinois 1996).

the realities of real-space multijurisdictional conflicts, and of the tools available to manage such conflicts. Section III analyzes the skeptics' descriptive claim that national regulation of cyberspace is infeasible. Section IV analyzes their normative claim that such regulation is illegitimate. Section V sketches a model for grounding cyberspace transactions in real-space law.

I. THE REGULATION SKEPTICS' CLAIMS

People transacting in cyberspace do things that would be regulated by state, national, or international law if they occurred in person or by telephone or mail. They defame, invade privacy, harass, and commit business torts.[8] They make and breach contracts.[9] They distribute pornography and swap bombmaking tips.[10] They infringe trademarks, violate copyrights, and steal data.[11] They issue fraudulent securities and restrict competition.[12] And so on.

Are these and other cyberspace activities governed by the same laws that govern similar transnational activities mediated in person, or by phone, or by mail? If so, which jurisdiction's law governs? If not, what governs instead?

The regulation skeptics' analysis of these questions makes two sets of assumptions. The first concerns the nature of legal regulation of non-cyberspace events.[13] The skeptics tend to conceptualize a nation's legal authority as extending to its territorial borders and not beyond. This conception makes them skeptical about the legitimacy of one nation regulating activities that take place in another. And it leads them to believe that transnational

---

[8] See, for example, *Naxos Resources (U.S.A.) Ltd v Southam, Inc*, 1996 US Dist LEXIS 21757, *13-15 (C D Cal) (defamation); *Panavision International, LP v Toeppen*, 938 F Supp 616, 619 (C D Cal 1996) (interference with economic advantage); Sally Greenberg, *Threats, Harassment, and Hate Online: Recent Developments*, 6 BU Pub Intl L J 673, 673-75, 680-84 (1997) (harassment and threats).

[9] See, for example, *Thompson v Handa-Lopez, Inc*, 998 F Supp 738 (W D Tex 1998) (contract made online).

[10] See, for example, *United States v Thomas*, 74 F3d 701, 704-05 (6th Cir), cert denied, 117 S Ct 74 (1996) (pornography); <www.personal.psu.edu/users/j/m/jmf11/aterror.txt> (visited Sept 10, 1998) (bombmaking tips).

[11] See, for example, *Zippo Manufacturing Co v Zippo Dot Com, Inc*, 952 F Supp 1119, 1121 (W D Pa 1997) (trademark infringement); *Religious Technology Center v F.A.C.T.-NET, Inc*, 901 F Supp 1519, 1521-22 (D Colo 1995) (copyright infringement); *Anatomy of a Cyber Break-in*, Newsweek 63 (Feb 27, 1995) (data theft).

[12] See, for example, *Maritz, Inc v CyberGold, Inc*, 947 F Supp 1328, 1329 (E D Mo 1996) (unfair competition); Robert A. Robertson, *Personal Investing in Cyberspace and the Federal Securities Laws*, 23 Sec Reg L J 347, 397-405 (1996) (fraudulent securities).

[13] The arguments from this paragraph are drawn from Johnson and Post, 48 Stan L Rev at 1368-70 (cited in note 3); Post and Johnson, *The New 'Civic Virtue'* at 5-6 (cited in note 3); Reidenberg, 45 Emory L J at 912-16 (cited in note 3).

disputes must be resolved by choice-of-law rules that select a unique governing law on the basis of *where* an event occurs or *where* transacting parties are located. On this view, tort liability is governed by the law of the place where the tort occurred and the validity of a contract is governed by the law of the place where the contract was made. Such choice-of-law rules are thought to promote rule-of-law values like uniformity (that is, every forum will apply the same law in a given case), predictability, and certainty. And they are supposed to give the parties to transnational transactions reasonable notice of governing law.

The skeptics' second set of assumptions concerns the architecture of cyberspace. They view cyberspace as a unique "boundary-destroying" means of communication. Internet protocol addresses do not necessarily correlate with a physical location. As a result, the skeptics assert, persons transacting in cyberspace often do not, and cannot, know each other's physical location.[14] In addition, information mediated by certain cyberspace services appears "simultaneously and equally in all jursidictions" around the world.[15] A web page in Illinois can be accessed from and thus appear in any geographical jurisdiction that is plugged in to the World Wide Web. When I participate in an online discussion group, my messages can appear simultaneously in every geographical jurisdiction where persons participate in the group. In neither case can I control, or even know about, the geographical flow of the information that I upload or transmit.

It is against this background that the skeptics make their descriptive and normative claims. Descriptively, they claim that cyberspace is a borderless medium that resists regulation conceived in geographical terms.[16] One reason is that information transmitted via cyberspace can easily flow across national borders without detection.[17] Another reason is that it is senseless to apply geographically configured choice-of-law rules to a-geographical cyberspace activities.[18] A third reason is that regulation of the local effects of cyberspace information flows permits all nations simultaneously to regulate all web-based transactions.[19] The result is multiple and inconsistent regulation of the same ac-

---

[14] See Johnson and Post, 48 Stan L Rev at 1374-75 (cited in note 3); Burk, 28 Conn L Rev at 1098, 1110-12 (cited in note 3).

[15] Post and Johnson, *Borders, Spillovers, and Complexity* at 5 (cited in note 3).

[16] See Johnson and Post, 48 Stan L Rev at 1370-72 (cited in note 3); Post and Johnson, *Borders, Spillovers, and Complexity* at 6 (cited in note 3).

[17] See Johnson and Post, 48 Stan L Rev at 1372-73 (cited in note 3).

[18] See id at 1374-76.

[19] See id at 1374.

tivity. A final reason is that the architecture of cyberspace enables its users to route around or otherwise evade territorial regulation.[20]

The skeptics' normative arguments build on these assumptions. Their essential normative claim is that it is illegitimate for any particular nation to regulate the local effects of multijurisdictional cyberspace activity. This is so for three reasons. First, such regulation will often apply to acts abroad, and will thus be impermissibly extraterritorial.[21] Second, because cyberspace information flows appear in every jurisdiction simultaneously, unilateral regulation of these flows will illegitimately affect the regulatory efforts of other nations and the cyberspace activities of parties in other jurisdictions.[22] Third is the problem of notice. The skeptics argue that because a person transacting in cyberspace does not know when or whether her activity produces effects in a particular jurisdiction, she lacks notice about governing law and therefore cannot conform her behavior to it.[23] They claim that under these conditions, it is unfair to apply law to her cyberspace activities. The skeptics believe that all three of these problems can be avoided by cyberspace self-regulation.

To make these claims more concrete, consider the predicament of one of the scores of companies that offer, sell, and deliver products on the World Wide Web. Assume that the web page of a fictional Seattle-based company, Digitalbook.com, offers digital books for sale and delivery over the Web. One book it offers for sale is *Lady Chatterley's Lover*. This offer extends to, and can be accepted by, computer users in every country with access to the Web. Assume that in Singapore the sale and distribution of pornography is criminal, and that Singapore deems *Lady Chatterley's Lover* to be pornographic. Assume further that Digitalbook.com's terms of sale contain a term that violates English consumer protection laws, and that the publication of Digitalbook.com's *Lady Chatterley's Lover* in England would infringe upon the rights of the novel's English copyright owner. Digitalbook.com sells and sends copies of *Lady Chatterley's Lover* to two people whose addresses (say, anonymous@aol.com and anonymous@msn.com) do not reveal their physical location but who,

---

[20] See Post, 1995 J Online L, Article 3, para 39-40 (cited in note 3).

[21] See Johnson and Post, 48 Stan L Rev at 1376 (cited in note 3); Burk, 28 Conn L Rev at 1123-34 (cited in note 3).

[22] See Post and Johnson, *Borders, Spillovers, and Complexity* at 38 (cited in note 3); Post and Johnson, *The New 'Civic Virtue'* at 5-6 (cited in note 3); Burk, 28 Conn L Rev at 1123-34 (cited in note 3).

[23] See Johnson and Post, 48 Stan L Rev at 1370, 1379 & n 33 (cited in note 3).

unbeknownst to Digitalbook.com, live and receive the book in Singapore and London, respectively.

The skeptics claim that it is difficult for courts in Singapore or England to regulate disputes involving these transactions in accordance with geographical choice-of-law rules. In addition, they argue that English and Singaporean regulations will expose Digitalbook.com to potentially inconsistent obligations. Finally, the skeptics claim that Digitalbook.com can easily evade the Singaporean and English regulations by sending unstoppable digital information into these countries from a locale beyond their enforcement jurisdiction.

On the normative side, the skeptics are concerned that the application of English and Singaporean law to regulate Digitalbook.com's transactions constitutes an impermissible extraterritorial regulation of a U.S. corporation. Because Digitalbook.com might bow to the English and Singaporean regulations, and because the company cannot limit its cyberspace information flows by geography, the English and Singaporean regulations might cause it to withdraw *Lady Chatterley's Lover* everywhere or to raise its price. The English and Singaporean regulations would thus affect Digitalbook.com's behavior in the United States and adversely affect the purchasing opportunities of parties in other countries. The skeptics believe these negative spillover effects of the national regulations are illegitimate. They also think it is unfair for England and Singapore to apply their laws in this situation because Digitalbook.com had no way of knowing that it sold and delivered a book to consumers in these countries.

II. "REAL-SPACE" JURISDICTIONAL CONFLICT MANAGEMENT

The skeptics are in the grip of a nineteenth century territorialist conception of how "real space" is regulated and how "real-space" conflicts of law are resolved.[24] This conception was repudiated in the middle of this century.[25] The skeptics' first mistake, therefore, is to measure the feasibility and legitimacy of national regulation of cyberspace against a repudiated yardstick. This Sec-

---

[24] The skeptics' views about territorialism and choice of law are remarkably similar to Story's and Beale's. See, for example, Joseph Story, *Commentaries on the Conflict of Laws* 7 (Little, Brown 2d ed 1841); Joseph Henry Beale, *A Treatise on the Conflict of Laws or Private International Law* 118 (Harvard 1916).

[25] The claim that the territorialist premises of the traditional approach to choice of law were flawed does not necessarily mean that the traditional choice-of-law rules that were based on these premises cannot in some circumstances be justified on independent grounds. See Alfred Hill, *The Judicial Function in Choice of Law*, 85 Colum L Rev 1585, 1619-36 (1985).

tion offers a more accurate picture of real-space jurisdictional conflict management as a prelude to analysis of the skeptics' claims.

Three factors led to the overthrow of the traditional approach to choice of law.[26] The first was significant changes in the world. Changes in transportation, communication, and in the scope of corporate activity led to an unprecedented increase in multijurisdictional activity. These changes put pressure on the rigid territorialist conception, which purported to identify a single legitimate governing law for transborder activity based on discrete territorial contacts. So too did the rise of the regulatory state, which led to more caustic public policy differences among jurisdictions, and which pressured the interested forum to apply local regulations whenever possible.[27]

A second factor, legal realism, contributed to the demise of hermetic territorialism. All conflict-of-laws problems by definition have connections to two or more territorial jurisdictions. The legal realists showed that nothing in the logic of territorialism justified legal regulation by any one of these territories rather than another.[28] They also argued that a forum's decision to apply foreign law was always determined by local domestic policies.[29] This established the theoretical foundation for the *lex fori* orientation that has dominated choice of law ever since.

A third factor, legal positivism, exacerbated the problem of finding a unique governing law in transactional cases. Courts avoided many choice-of-law problems in such cases by applying universal customary laws tied to no particular sovereign authority, such as the law merchant, the law maritime, and the law of

---

[26] The classic criticisms of the traditional view are Brainerd Currie, *Selected Essays on the Conflict of Laws* (Duke 1963), and Walter Wheeler Cook, *The Logical and Legal Bases of the Conflict of Laws* (Harvard 1949).

[27] This is one reason why so many of the transformative midcentury constitutional choice-of-law decisions involved public regulations rather than private law. See, for example, *Clay v Sun Insurance Office, Ltd*, 377 US 179, 182-83 (1964) (insurance); *Watson v Employers Liability Assurance Corp*, 348 US 66, 72-73 (1954) (insurance); *United States v Aluminum Co of America*, 148 F2d 416, 444 (2d Cir 1945) (antitrust); *Pacific Employers Insurance Co v Industrial Accident Commission of California*, 306 US 493, 497 (1939) (workmen's compensation); *Alaska Packers Association v Industrial Accident Commission of California*, 294 US 532, 538 (1935) (workmen's compensation); *Bradford Electric Light Co v Clapper*, 286 US 145, 150-51 (1932) (workmen's compensation); *Home Insurance Co v Dick*, 281 US 397, 405-08 (1930) (insurance).

[28] See, for example, Cook, *The Logical and Legal Bases* at 311-22, 354-70, 433-37 (cited in note 26); Walter Wheeler Cook, *The Jurisdiction of Sovereign States and the Conflict of Laws*, 31 Colum L Rev 368, 372-80 (1931); Ernest G. Lorenzen, *Selected Articles on the Conflict of Laws* 305-21 (Yale 1947).

[29] See Cook, *The Logical and Legal Bases* at 35-36 (cited in note 26); Hessel E. Yntema, *The Hornbook Method and the Conflict of Laws*, 37 Yale L J 468, 478 (1928).

nations.[30] But positivism's insistence on a sovereign source for every rule of decision undermined judicial reliance on these laws.[31] It also contributed to the waning of universal choice-of-law rules that courts applied in circumstances in which transnational customary laws did not govern. In the United States, for example, the general uniformity of choice-of-law approaches that characterized the nineteenth century gave way in the twentieth century to a plethora of choice-of-law regimes.[32] As different jurisdictions adopted different choice-of-law regimes, the goal of a single governing law for transjurisdictional transactions was further frustrated.[33]

These factors did not completely undermine traditional views about territorial regulation. But they did lead to an expansion of the permissible bases for territorial jurisdiction. Today, 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 choice of its law is neither arbitrary nor fundamentally unfair."[34] In practice, this standard is notoriously easy to satisfy.[35] It prohibits the application of local law only when the forum state has no interest in the case because the substance of the lawsuit has no relationship to the state. Customary international law limits on a nation's regulation of extraterritorial events are less clear because there are few international decisions on point, and because state practice does not reveal a set-

---

[30] See Leon E. Trakman, *The Law Merchant: The Evolution of Commercial Law* 39-44 (Fred B. Rothman 1983); Bradford R. Clark, *Federal Common Law: A Structural Reinterpretation*, 144 U Pa L Rev 1245, 1280-81 (1996).

[31] See Friedrich K. Juenger, *American Conflicts Scholarship and the New Law Merchant*, 28 Vand J Transnatl L 487, 491 (1995).

[32] The main approaches used by the several states today are the traditional vested rights approach, interest analysis, the Second Restatement, comparative impairment, and the better law approach. See Lea Brilmayer, *Conflict of Laws: Cases and Materials* 203-314 (Little, Brown 4th ed 1995). Even states that purport to use the same methodology—for example, interest analysis or the Second Restatement—often do so in name only, with important differences in practice.

[33] In the United States, the horizontal nonuniformity fostered by different choice-of-law regimes in different states was exacerbated by the rule that federal courts sitting in diversity apply state choice-of-law rules. See *Klaxon Co v Stentor Electric Manufacturing Co, Inc*, 313 US 487, 496 (1941).

[34] *Phillips Petroleum Co v Shutts*, 472 US 797, 818 (1985), quoting *Allstate Insurance Co v Hague*, 449 US 302, 312-13 (1981).

[35] For example, in the case in which this modern standard was formulated, the Supreme Court held that Minnesota could apply its plaintiff-favoring insurance law to an accident in Wisconsin among Wisconsin residents based on the fact that the decedent worked in Minnesota, the insurance company did business there, and the beneficiary moved there from Wisconsin after the accident. See *Hague*, 449 US at 315-20. On the weaknesses and uncertainties of the *Hague* test, see Brilmayer, *Conflict of Laws* at 140-43 (cited in note 32).

tled custom. Nonetheless, it seems clear that customary international law, like the United States Constitution, permits a nation to apply its law to extraterritorial behavior with substantial local effects.[36] In addition, both the Constitution and international law permit a nation or state to regulate the extraterritorial conduct of a citizen or domiciliary.[37] In short, in modern times a transaction can legitimately be regulated by the jurisdiction where the transaction occurs, the jurisdictions where significant effects of the transaction are felt, and the jurisdictions where the parties burdened by the regulation are from.

This expansion of the permissible bases for the application of local law has revolutionized conflict of laws in the second half of this century. Any number of choice-of-law regimes are now consistent with constitutional and international law. The earlier belief in a unique governing law for all transnational activities has given way to the view that more than one jurisdiction can legitimately apply its law to the same transnational activity.[38] The uniformity promised by the traditional approach has thus been replaced by the reality of overlapping jurisdictional authority. This means that the application of one jurisdiction's law often comes at the expense of the nonapplication of the conflicting laws of other interested jurisdictions. Because choice-of-law rules often differ from jurisdiction to jurisdiction, and because a forum applies its own choice-of-law rules, the choice of forum is now often critical to the selection of governing law. In this milieu, *ex ante* notice of a specific governing law is no longer a realistic goal in many transnational situations. Not surprisingly, the Constitution and international law impose very weak notice requirements on the application of local law to extraterritorial activity.

---

[36] The Permanent Court of International Justice famously established a very weak effects test for extraterritorial jurisdiction and suggested a default rule that favored extraterritorial jurisdiction. See *The case of the S.S. "Lotus"*, 1927 P C I J (ser A) No 10 at 18-25. Section 403 of the Restatement (Third) of the Foreign Relations Law (ALI 1987), recognized the effects test as a basis for extraterritorial jurisdiction, but added the caveat that a state may not exercise such jurisdiction when it would be "unreasonable" to do so. This reasonableness requirement has little basis in state practice and does not reflect customary international law. See William S. Dodge, *Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism*, 39 Harv Intl L J 101, 139-40 & nn 241-42 (1998).

[37] See, for example, *Blackmer v United States*, 284 US 421, 436 (1932); *United States v Reeh*, 780 F2d 1541, 1543 n 2 (11th Cir 1986); Restatement (Third) of the Foreign Relations Law § 402(2). International law also permits a nation to regulate extraterritorial conduct that threatens local security, Restatement (Third) of the Foreign Relations Law § 402(3), and might permit a nation to regulate certain extraterritorial acts against its citizens, id at comment g.

[38] See *Shutts*, 472 US at 823; *Hague*, 449 US at 307; Restatement (Third) of the Foreign Relations Law § 403(3).

This modern world of jurisdictional conflict poses obvious difficulties for participants in transnational transactions. To understand these problems and their resolution, it is important to distinguish between default laws and mandatory laws. For present purposes, a default law can be understood as one that presumptively governs a particular relationship or transaction, but that can be modified or circumvented by the parties in the relationship or transaction. The default laws of different countries can create a conflict of laws. For example, the estate of a U.S. national who dies intestate in England, his domicile, could potentially be subject to the succession rules of either country. Similarly, a contract made in one country for delivery of products in another could be subject to the remedies regime of either country.

Parties in such transnational relationships can alleviate choice-of-law uncertainty with respect to default rules by contracting for specific terms, by selecting a governing law, or both.[39] Most contractual choice-of-law clauses govern the contracts within which they are embedded. But the scope of this private legal control is not limited to traditional contractual issues. In many circumstances, parties can agree to a governing law for torts and related actions that arise from their contractual relations.[40] They can also specify the governing law for matters ranging from intellectual property to trusts and estates to internal corporate affairs.[41]

The possibilities for private legal ordering are not limitless. Every nation has mandatory laws that govern particular transactions or relationships regardless of the wishes of the parties. The primary justifications for such laws are paternalism and protection of third parties.[42] Mandatory laws range from limits on con-

---

[39] Some courts will not enforce choice-of-law agreements in which the "chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice." Restatement (Second) of Conflict of Laws § 187(2)(a) (1971). This restriction has less force in transnational contexts in which there are often good reasons for parties to choose a neutral law unrelated to the parties. See id § 187 comment f.

[40] See, for example, *Moses v Business Card Express, Inc*, 929 F2d 1131, 1138 (6th Cir 1991).

[41] See, for example, Hague Convention on the Law Applicable to Succession to the Estates of Deceased Persons, Art 5, 28 ILM 146, 150 (1989) (providing that an individual may designate either the law of habitual residence or the law of nationality to govern succession); Hague Convention on the Law Applicable to Trusts and on Their Recognition, Art 6, 23 ILM 1389 (1984) ("A trust shall be governed by the law chosen by the settlor."); *McDermott Inc v Lewis*, 531 A2d 206, 215 (Del 1987) (holding that law of place of incorporation governs internal corporate affairs); William Grantham, Comment, *The Arbitrability of International Intellectual Property Disputes*, 14 Berkeley J Intl L 173, 190-95 (1996) (describing how parties' choice of law governs intellectual property disputes).

[42] See Michael J. Trebilcock, *The Limits of Freedom of Contract* 58-77, 145-63 (Har-

tractual capacity to criminal law to securities and antitrust law. Like default laws, they differ in content and scope from jurisdiction to jurisdiction. Unlike conflicts of default laws, conflicts of mandatory laws cannot be resolved easily by private contract.[43] They can, in theory, be resolved by *public* contract—international agreements that embrace uniform international rules[44] or uniform choice-of-law rules.[45] Such solutions are increasingly prominent but still relatively rare. Moreover, these attempts at international uniformity are often limited to default rules, and are littered with mandatory law exceptions.[46]

This discussion shows that conflicts of law can arise when parties to a transnational transaction do not specify the governing default law, or when the transaction implicates a mandatory law that conflicts with the otherwise-applicable law. Absent a governing international law, transnational activity in these contexts will usually be governed by the law of a single jurisdiction.[47] And absent international choice-of-law rules, the forum's choice-of-law rules will determine the governing law. In regulatory contexts, the forum will invariably apply local law.[48] But regardless of which substantive law the forum applies, the application of that law will frequently create spillover effects on activities in other countries and on the ability of other interested nations to apply their own law. In our increasingly integrated world, these spillover effects are likely to extend to many countries.[49]

---

vard 1993).

[43] See, for example, *Vimar Seguros y Reaseguros, SA v M/V Sky Reefer*, 515 US 528, 540-41 (1995) (noting that transnational parties cannot reduce their liability under the Carriage of Goods at Sea Act by contracting around its provisions); *Mitsubishi Motors Corp v Soler Chrysler-Plymouth, Inc*, 473 US 614, 637 n 19 (1985) (noting that transnational parties cannot contract around the Sherman Act). Private parties can, of course, circumvent mandatory laws to the extent that they can shift the location or effects of their activities beyond the mandatory law's enforceable scope. For further discussion, see note 178.

[44] See, for example, United Nations Convention on Contracts for the International Sale of Goods ("CISG"), UN Doc A/CONF.97/18, reprinted at 19 ILM 671 (1980). A related solution is to develop uniform laws like the Uniform Commercial Code, which minimize choice-of-law difficulties by ensuring that every jurisdiction's local law is (in theory) the same.

[45] See, for example, Convention on the Law Applicable to Contractual Obligations ("Rome Convention"), June 19, 1980 (80/934/EEC) 1980 OJ (L266/1), p 1.

[46] See, for example, id Arts 3(3), 5(2), 6(1), and 7(1)-(2) (acknowledging various mandatory law restrictions on choice of law governing contracts).

[47] I say "usually" because sometimes there will be parallel litigation of the same matter in two nations, each of which attempts to apply its own law. See, for example, *Laker Airways Ltd v Sabena*, 731 F2d 909, 917-20 (DC Cir 1984).

[48] See Andreas F. Lowenfeld, *International Litigation and the Quest for Reasonableness: Essays in Private International Law* 5 (Clarendon 1996).

[49] In my discussion here and throughout the Article, I shall follow the skeptics in assuming that the spillovers produced by unilateral regulation of transnational activity are

Consider, for example, the Supreme Court's decision in *Hartford Fire Insurance Co v California*.[50] The Court held that the concerted refusal by London reinsurers to sell certain types of reinsurance to insurers in the United States violated the Sherman Act. The reinsurers' acts in England were legal under English law. But the Court determined that the reinsurers were nonetheless subject to U.S. regulation because their actions "produced substantial effect[s]" in the United States.[51] U.S. law thus regulated the activities of English companies in England at the expense of the nonapplication of English law. Similarly, had an English court applied English law to adjudge the reinsurers' acts to be legal, it would have produced spillover effects on consumers in the United States, and would have come at the expense of the nonapplication of U.S. law. No matter which law governed the reinsurers' acts, the application of that law would have produced spillover effects on the English reinsurers' activities in other jurisdictions, and on the activities of persons in other jurisdictions adversely affected by the reinsurers' acts.

A similar phenomenon occurs in many domestic and international conflicts contexts. For example, the European Commission recently imposed strict conditions on a merger (already approved by the Federal Trade Commission) between two American companies with no manufacturing facilities in Europe.[52] Minnesota applied its pro-plaintiff stacking rules for automobile insurance coverage to an accident in Wisconsin among Wisconsin residents.[53] A United States federal grand jury ordered the local branch of a foreign bank, a nonparty, to disclose bank records in the Bahamas in possible violation of Bahamian law.[54] California applied its workmen's compensation law to benefit an employee of a California corporation who suffered a tort while working in Alaska—even though Alaska purported to make its worker's compensation scheme exclusive, and even though the employment contract specified that Alaska law governed.[55] New York

---

negative spillovers. This will not always be true, but it will usually be true in situations in which one state regulates extraterritorial conduct that the territorial government would regulate differently.

[50] 509 US 764 (1993).

[51] Id at 796.

[52] See *McDonnell Douglas-Boeing Link Gets Europe Approval*, NY Times D4 (July 31, 1997).

[53] See *Hague*, 449 US at 306, 319-20.

[54] See *In re Grand Jury Proceedings United States v Bank of Nova Scotia*, 691 F2d 1384, 1391 (11th Cir 1982).

[55] See *Alaska Packers*, 294 US at 539-44.

applied its tort law to a car accident in Canada.[56] California taxed a British corporation based on the California portion of its world profits.[57]

In these situations and countless others, one jurisdiction regulates extraterritorial conduct in a way that invariably affects individual behavior and regulatory efforts in other jurisdictions. These spillover effects constitute the central problem of modern conflict of laws. The problem is pervasive. It is also inevitable, because the price of eliminating these spillovers—abolishing national or subnational lawmaking entities, or eliminating transnational activity—is prohibitively high. Most of the dizzying array of modern choice-of-law methodologies are devoted to minimizing these spillovers while at the same time preserving the sovereign prerogative to regulate effects within national borders.[58] International harmonization efforts seek to achieve similar aims, often at the expense of national prerogatives.[59]

There is widespread debate about which approach, or combination of approaches, is preferable. Resolution of this debate is less important for present purposes than two uncontested assumptions that underlie it. The first assumption is that in the absence of consensual international solutions, prevailing concepts of territorial sovereignty permit a nation to regulate the local effects of extraterritorial conduct even if this regulation produces spillover effects in other jurisdictions. The second assumption is that such spillover effects are a commonplace consequence of the unilateral application of any particular law to transnational activity in our increasingly interconnected world. It is against this background that the skeptics' descriptive and normative claims must be assessed.

III. IS CYBERSPACE REGULATION FEASIBLE?

This Section argues that the skeptics' claims about the infeasibility of national regulation of cyberspace rest on an underap-

---

[56] See *Babcock v Jackson*, 12 NY2d 473, 240 NYS2d 743, 191 NE2d 279, 284-85 (1963).

[57] See *Barclays Bank PLC v Franchise Tax Board*, 512 US 298, 310-15 (1994).

[58] This is the goal, for example, of such different approaches as the Restatement of the Foreign Relations Law's interest-balancing approach, see Restatement (Third) of the Foreign Relations Law § 403; William Baxter's comparative impairment approach, see William F. Baxter, *Choice of Law and the Federal System*, 16 Stan L Rev 1, 4-20 (1963); Larry Kramer's multistate canons of construction, see Larry Kramer, *Rethinking Choice of Law*, 90 Colum L Rev 277, 319-38 (1990); and Lea Brilmayer's strategy to maximize state policy objectives, see Brilmayer, *Conflict of Laws* at 169-218 (cited in note 32).

[59] See David W. Leebron, *Lying Down with Procrustes: An Analysis of Harmonization Claims*, in Jagdish N. Bhagwati and Robert E. Hudec, eds, 1 *Fair Trade and Harmonization* 41, 43-50 (MIT 1996).

preciation of the realities of modern conflict of laws, and of the legal and technological tools available to resolve multijurisdictional cyberspace conflicts. From the perspective of jurisdiction and choice of law, regulation of cyberspace transactions is no less feasible than regulation of other transnational transactions.

A. Default Laws and Private Ordering in Cyberspace

Cyberspace transactions that implicate default laws, like other transnational transactions that implicate such laws, are subject to private legal ordering. The architecture of cyberspace facilitates this private ordering and thus enables cyberspace participants to avoid many transnational conflicts of law.

At the most basic level, private ordering is facilitated by the technical standards that define and limit cyberspace.[60] To participate in the Internet function known as the World Wide Web, users must consent to the TCP/IP standards that define the Internet as well as to the HTML standards that more particularly define the Web. Similarly, sending e-mail over the Internet requires the sender to use TCP/IP standards and particular e-mail protocols. One's experience of cyberspace is further defined and limited by the more particular communication standards embedded in software.[61] For example, within the range of what TCP/IP and HTML permit, an individual's communication via the World Wide Web will be shaped and limited by (among many other things) her choice of browsers and search engines. These and countless other technical standard choices order behavior in cyberspace. In this sense, access to different cyberspace networks and communities is always conditioned on the accessors' consent to the array of technical standards that define these networks and communities.

Technical standards cannot comprehensively specify acceptable behavior in cyberspace. Within the range of what these standards permit, information flows might violate network norms or territorial laws. Many network norms are promulgated and en-

---

[60] For more general discussions of this point, see Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 Tex L Rev 553 (1998); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 Emory L J 869, 895-99 (1996); M. Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, 1996 U Chi Legal F 335, 339-47; Post, 1995 J Online L, Article 3, paras 20-21 (cited in note 3).

[61] Of course, computer hardware—keyboards, monitors, modems, disk drives, processors, and the like—also affects how individuals experience cyberspace. Many software instructions that are interpreted by a computer could be instantiated in hardware rather than software. For the most part, however, hardware is less significant than software in creating and shaping one's experience of cyberspace. See Katsh, 1996 U Chi Legal F at 339-43 (cited in note 60).

forced informally. A more formal method to establish private legal orders in cyberspace is to condition access to particular networks on consent to a particular legal regime.

This regime could take several forms. It could be a local, national, or international law. When you buy a Dell computer through the company's web page from anywhere in the world, you agree that "[a]ny claim relating to, and the use of, this Site and the materials contained herein is governed by the laws of the state of Texas."[62] Alternatively, the chosen law could be a free-standing model law attached to no particular sovereign but available to be incorporated by contract. For example, parties to a commercial transaction over the Internet could agree that their transaction is governed by UNIDROIT Principles or the Uniform Customs and Practice for Documentary Credits.[63] Or the governing law could be the contractual terms themselves.[64] Waivers and exclusions operate as private law in this way. So too do chat rooms, discussion lists, and local area networks that condition participation on the user's consent to community norms specified in a contract.

Cyberspace architecture can also help to establish other aspects of a private legal order. Through conditioned access, cyberspace users can consent to have subsequent disputes resolved by courts, arbitrators, systems operators, or even "virtual magistrates."[65] They can also establish private enforcement regimes. Technical standards operate as an enforcer of sorts by defining and limiting cyberspace activity. For example, software filters can block or condition access to certain information, and various technologies perform compliance monitoring functions.[66] In addition, the gatekeeper of each cyberspace community can cut off entry for noncompliance with the community rules, or punish a user for bad acts by drawing on a bond (perhaps simply a credit card) put up as a condition on the user's entry.[67]

---

[62] <www.dell.com/dell/legal/disclwww.htm> (visited Apr 1, 1998).

[63] International Institute for the Unification of Private Law ("UNIDROIT"), *Principles of International Commercial Contracts* (UNIDROIT 1994); ICC, *Uniform customs and practice for documentary credits*, ICC Pub No 500 (1993).

[64] Such a regime will invariably be underspecified and will require supplementation by some default law regime.

[65] "Virtual Magistrate" is the name of the decisionmaker in a relatively new online project "for resolving disputes that arise on worldwide computer networks about online messages, postings, and files . . . ." *The Virtual Magistrate Project Concept Paper*, available online at <vmag.vcilp.org/docs/vmpaper.html> (visited Apr 1, 1998).

[66] See Reidenberg, 76 Tex L Rev at 558-68 (cited in note 60).

[67] See Jack Goldsmith and Lawrence Lessig, *Grounding the Virtual Magistrate* 4, available online at <www.law.vill.edu/ncair/disres/groundvm.htm> (visited Apr 1, 1998). For further development of these points, see Section V.

Many have proposed a structure for private legal ordering of cyberspace along the lines just sketched.[68] There is nothing remarkable about this structure. It differs little from the legal structure of other private groups, such as churches, merchants, families, clubs, and corporations, which have analogous consent-based governing laws, dispute resolution mechanisms, and private enforcement regimes.[69] But just as private ordering is often not a comprehensive solution to the regulation of "real-space" private groups, it will not be a comprehensive solution to the regulation of cyberspace either.

In part this is because it remains an open question how to generate consent across cyberspace networks. Conditioning access on consent to a governing legal regime is relatively easy at the entry point of a cyberspace network. In theory, it is just as easy to generate such consent at the interface between networks. It is commonplace to click on a hypertext link and be greeted by a message that conditions further access on presentation of an identification code, or credit card number, or personal information such as age and address. A similar demand for consent to a particular legal regime could be added as a condition for access. However, this process might become confusing; the technological and conceptual details of consenting to and coordinating different legal regimes as one works one's way through dozens of cyberspace networks remain to be worked out.[70] In addition, the generation of legal consent across networks will impose time and other costs that are anathema to many cyberspace users.

An important additional difficulty is that many cyberspace activities affect non-cyberspace participants with whom *ex ante* consent to a private legal regime will not be possible. Cyberspace is not, as the skeptics often assume, a self-enclosed regime. A communication in cyberspace often has consequences for persons outside the computer network in which the communication took place. For example: a book uploaded on the Net can violate an author's copyright; a chat room participant can defame someone outside the chat room; terrorists can promulgate bomb making or kidnapping tips; merchants can conspire to fix prices by e-mail; a corporation can issue a fraudulent security; a pornographer can

---

[68] See, for example, Johnson and Post, 48 Stan L Rev at 1387-91 (cited in note 3); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U Pitt L Rev 993, 1028-33 (1994).

[69] See generally Eric A. Posner, *The Regulation of Groups: The Influence of Legal and Nonlegal Sanctions on Collective Action*, 63 U Chi L Rev 133, 165-97 (1996).

[70] See Goldsmith and Lessig, *Grounding the Virtual Magistrate* at 3-4 (cited in note 67); Johnson and Post, 48 Stan L Rev at 1395-1400 & nn 102-03 (cited in note 3).

sell kiddie porn; Internet gambling can decrease in-state gambling revenues and cause family strife; and so on. In these and many other ways, communications via cyberspace produce harmful, real-world effects on those who have not consented to the private ordering of the cyberspace community.

Finally, even if the hurdles to consent can be surmounted, consent-based legal orders are limited by a variety of national mandatory law restrictions.[71] These mandatory laws define who may consent to these private regimes. For example, they prevent persons of certain ages from entering into certain types of contracts. They also limit the form and scope of such consent. The consideration requirement and limitations on liquidated damages clauses fall into this category, as do requirements that the law chosen by the parties have a reasonable relationship to the subject matter of the contract. Some mandatory laws also limit the internal and external activities of the group's activities. Criminal law, for example, falls in this category.

Private legal ordering thus has the potential to resolve many, but not all, of the challenges posed by multijurisdictional cyberspace activity. Cyberspace activities for which *ex ante* consent to a governing legal regime is either infeasible or unenforceable are not amenable to private ordering. Such activities remain subject to the skeptics' concerns about multiple or extraterritorial national regulation.[72]

B. The Limits of Enforcement Jurisdiction

The skeptics' concerns are further attenuated, however, by limitations on every nation's ability to enforce its laws. A nation can purport to regulate activity that takes place anywhere. The Island of Tobago can *enact* a law that purports to bind the rights of the whole world.[73] But the effective scope of this law depends on Tobago's ability to *enforce* it. And in general a nation can only enforce its laws against: (i) persons with a presence or assets in the nation's territory; (ii) persons over whom the nation can obtain personal jurisdiction and enforce a default judgment against abroad; or (iii) persons whom the nation can successfully extradite.[74]

---

[71] The skeptics challenge the normative basis for nations to apply mandatory laws to regulate the private legal regimes of cyberspace. I consider these arguments in Section IV.

[72] I discuss private legal ordering in cyberspace in greater detail in Section V.

[73] See *Buchanan v Rucker*, 9 East 192, 103 Eng Rep 546, 547 (KB 1808) ("Can the Island of Tobago pass a law to bind the rights of the whole world?").

[74] I set aside for present purposes two other relatively rare methods of extraterritorial enforcement: military invasion, see, for example, *United States v Noriega*, 746 F Supp

A defendant's physical presence or assets within the territory remains the primary basis for a nation or state to enforce its laws. The large majority of persons who transact in cyberspace have no presence or assets in the jurisdictions that wish to regulate their information flows in cyberspace. Such regulations are thus likely to apply primarily to Internet service providers and Internet users with a physical presence in the regulating jurisdiction. Cyberspace users in other territorial jurisdictions will indirectly feel the effect of the regulations to the extent that they are dependent on service or content providers with a presence in the regulating jurisdiction.[75] But for almost all users, there will be no threat of extraterritorial legal liability because of a lack of presence in the regulating jurisdictions.

A nation or state can also enforce its laws over an entity with no local presence or assets if it can obtain personal jurisdiction over the entity and enforce a local default judgment against that entity abroad. The domestic interstate context presents a much greater threat in this regard than does the international context. This is because the Full Faith and Credit Clause requires a state to enforce the default judgment of a sister state that had personal jurisdiction over the defendant.[76] This threat is attenuated, however, by constitutional limits on a state's assertion of personal jurisdiction. The Due Process Clauses prohibit a state from asserting personal jurisdiction over an entity with no local presence unless the entity has purposefully directed its activities to the forum state and the assertion of jurisdiction is reasonable.[77]

Application of this standard to cyberspace activities presents special difficulties. Under standard assumptions about cyber-

---

1506 (S D Fla 1990), and secondary boycotts, see, for example, Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996 ("Helms-Burton Act"), Pub L No 104-114, 110 Stat 785, codified at 22 USCA §§ 6021-91 (1994 & Supp 1998) (sanctioning nations that engage in certain transactions with Cuba).

[75] I explain below why local regulation of service or content providers that produces multijurisdictional spillover effects is legitimate and fair, see Section IV.B; my goal for now is to show that the scope of national regulation of cyberspace is much narrower than the skeptics claim.

[76] See US Const, Art IV, § 1; Roger C. Crampton, et al, *Conflict of Laws: Cases-Comments-Questions* 735-37 (West 5th ed 1993).

[77] See *Asahi Metal Industry Co v Superior Court*, 480 US 102, 108-09 (1987). This is the test for specific jurisdiction; such jurisdiction is limited to cases in which the cause of action arises out of or relates to the defendant's contacts with the forum. A court may also assert general personal jurisdiction over a defendant for a cause of action that accrued anywhere. General jurisdiction is normally limited to the defendant's domicile and anywhere else where it may have "continuous and systematic . . . contacts." *Helicopteros Nacionales de Columbia v Hall*, 466 US 408, 414-16 (1984). Courts are unanimous that a web page accessible in a jurisdiction does not by itself establish general jurisdiction there. See, for example, *Weber v Jolly Hotels*, 977 F Supp 327, 333-34 (D NJ 1997).

space architecture, persons can upload or transmit information knowing that it could reach any and all jurisdictions, but not knowing which particular jurisdiction it might reach. Can every state where these transmissions appear assert specific personal jurisdiction over the agent of the information under the purposeful availment and reasonableness tests?

Full consideration of this issue is far beyond this Article's scope.[78] I simply wish to point out why there is relatively little reason at present, and even less reason in the near future, to believe that the mere introduction of information into cyberspace will *by itself* suffice for personal jurisdiction over the agent of the transmission in every state where the information appears. Most courts 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.[79] For a variety of reasons, these decisions have limited specific personal jurisdiction to cases in which there are independent indicia that the out-of-state defendant knowingly and purposefully directed the effects of out-of-state conduct to a particular state where the acts were deemed illegal.

Given the skeptics' assumptions about cyberspace architecture, this conclusion appears appropriate. It seems unfair to expose a content provider to personal jurisdiction in all fifty states for the mere act of uploading information on a computer if she cannot take affordable precautions to avoid simultaneous multijurisdictional effects. But we shall see below that the skeptics' architectual assumptions are inaccurate. It is already possible for content providers to take measures to achieve significant control over information flows. And filtering and identification technology promise greater control at less cost.[80] In cyberspace as in real space, the ultimate meaning of "purposeful availment" and "reasonableness" will depend on the cost and feasibility of information flow control.[81] As such control becomes more feasible and less costly, personal jurisdiction over cyberspace activities will become

---

[78] For broader treatments, see Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 Vill L Rev 1, 13-25 (1996); Burk, 28 Conn L Rev at 1107-23 (cited in note 3).

[79] See, for example, *Cybersell, Inc v Cybersell, Inc*, 130 F3d 414, 419-20 (9th Cir 1997); *Weber*, 977 F Supp at 334; *Panavision International, LP v Toeppen*, 938 F Supp 616, 622 (C D Cal 1996). For more comprehensive analyses of the many Internet personal jurisdiction cases, see Howard B. Stravitz, *Personal Jurisdiction in Cyberspace: Something More is Required on the Electronic Stream of Commerce*, 49 SC L Rev 925 (1998); Christopher W. Meyer, Note, *World Wide Web Advertising: Personal Jurisdiction Around the Whole Wide World?*, 54 Wash & Lee L Rev 1269 (1997).

[80] See Section III.D.

[81] See Burk, 28 Conn L Rev at 1117-20 (cited in note 3).

functionally identical to personal jurisdiction over real-space activities.

This detour into the technicalities of personal jurisdiction was necessitated by a worry about the extraterritorial enforcement of local default judgments against nonlocal cyberspace users within the American federal system. Such concerns are less pronounced in the international context. In contrast to the domestic interstate context, customary international law imposes few enforceable controls on a country's assertion of personal jurisdiction, and there are few treaties on the subject.[82] However, also in contrast to domestic law, there is no full faith and credit obligation to enforce foreign judgments in the international sphere.[83] If one country exercises personal jurisdiction on an exorbitant basis, the resulting judgment is unlikely to be enforced in another country.[84] In addition, local public policy exceptions to the enforcement of foreign judgments are relatively commonplace in the international sphere, especially when the foreign judgment flies in the face of the enforcing state's regulatory regime.[85] For these reasons, there is little concern that a foreign default judg-

---

[82] I should emphasize the term "enforceable" here, because many commentators talk as if there are (or should be) customary international law limits on exorbitant assertions of personal jurisdiction. See, for example, Restatement (Third) of the Foreign Relations Law § 421. This talk does not appear to be supported by state practice followed from a sense of legal obligation, the usual requirements for a rule of customary international law. The Brussels and Lugano Conventions are treaties that specify the legal bases for personal jurisdiction among members of the European Union. See Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commerical Matters, Sept 27, 1968, 1990 OJ (C 189) 2 (consolidated); Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, Sept 16, 1988, 1988 OJ (L 319) 9. These rare treaties on the subject prove the point that there is no effective or established customary international law that regulates personal jurisdiction, for the Brussels-Lugano regime permits exorbitant assertions of personal jurisdiction against defendants from non-European countries. See Friedrich Juenger, *Judicial Jurisdiction in the United States and in the European Communities: A Comparison*, 82 Mich L Rev 1195, 1211 (1984).

[83] The U.S. Constitution's Full Faith and Credit obligation does not extend to judgments of foreign nations. See US Const, Art IV, § 1 (requiring states to give full faith and credit to acts, records, and proceedings "of every other *State*") (emphasis added). The enforceability of these judgments is generally regulated by state law and is weaker than the obligation imposed by the Full Faith and Credit Clause. See Gary B. Born, *International Civil Litigation in United States Courts: Commentary & Materials* 938-62 (Kluwer 3d ed 1996). In Europe, the Brussels and Lugano Conventions, which regulate the enforcement of foreign judgments among European Union members, are again an exception to the general rule.

[84] See Born, *International Civil Litigation* at 942-43 (cited in note 83) (discussing examples from Japan, Germany, and England).

[85] See, for example, *Bachchan v India Abroad Publications Inc*, 154 Misc 2d 228, 585 NYS2d 661, 664-65 (NY Sup Ct 1992) (declining to enforce English money judgment for libel against a newspaper whose activities would have been protected by the First Amendment in the United States). See generally Born, *International Civil Litigation* at 942-43 (cited in note 83).

ment will be enforceable against cyberspace users who live outside the regulating jurisdiction.

The final way that a nation can enforce its regulations against persons outside its jurisdiction is by seeking extradition. In the United States, extradition among the several states is regulated by Article IV of the Constitution and the federal extradition law.[86] As a general matter, State A must accede to the proper demand of State B for the surrender of a fugitive who committed an act in State B that State B considers a crime. Nonetheless, a person who in State A transmits information flows that appear in and constitute a crime in State B will not likely be subject to extradition to State B under these provisions. This is because the extradition obligation only extends to fugitives who have fled State B, and these terms have long been limited to persons who were *physically present* in the demanding state at the time of the crime's commission.[87] A different, but equally forceful, limitation applies to international extradition. International extradition is governed largely by treaty.[88] A pervasive feature of modern extradition treaties is the principle of double criminality. This principle requires that the charged offense be criminal in both the requesting and the requested jurisdictions.[89] This principle, and its animating rationale, make it unlikely that there will be international cooperation in the enforcement of exorbitant unilateral criminal regulations of cyberspace events.

This review of transnational enforcement jurisdiction makes clear that the skeptics exaggerate the threat of multiple regulation of cyberspace information flows. This threat must be measured by a regulation's enforceable scope, not by its putative scope. And the enforceable scope is relatively narrow. It extends only to individual users or system operators with presence or assets in the enforcement jurisdiction, or (in the U.S.) to entities that take extra steps to target cyberspace information flows to states where such information flows are illegal. Such regulatory exposure is a significant concern for cyberspace participants. But it is precisely how regulatory exposure operates in "real space." And it is far

---

[86] See US Const, Art IV, § 2, cl 2; 18 USC § 3182 (1994).

[87] See *Innes v Tobin*, 240 US 127, 131 (1916); *Hyatt v People*, 188 US 691, 711-12 (1903); *Gee v Kansas*, 912 F2d 414, 418 (10th Cir 1990). This jurisdictional limitation does not apply, of course, when a person in one state commits a federal crime in another. See *United States v Thomas*, 74 F3d 701, 709-10 (6th Cir 1996).

[88] For an overview, see I.A. Shearer, *Extradition in International Law* (Manchester 1971).

[89] See John T. Soma, Thomas F. Muther, Jr., and Heidi M.L. Brissette, *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?*, 34 Harv J Leg 317, 323-26 (1997).

less significant than the skeptics' hyperbolic claim that *all* users of the Web will be simultaneously subject to *all* national regulations.[90]

Even with these limitations, the skeptics worry that an individual cyberspace content provider in one jurisdiction faces *potential* liability in another jurisdiction when she places information on the Internet. 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 affects the providers' activities at home and thus can be viewed as a weak form of extraterritorial regulation. This form of regulation is a theoretical possibility, but it should not be exaggerated. No nation has as yet imposed liability on a content provider for unforeseen effects in an unknown jurisdiction. The threat of such liability will lessen as content providers continue to gain means to control information flows.[91] It is also conceivable that weak normative limitations might exist or develop to prevent a jurisdiction from regulating local effects that were truly unforeseeable or uncontrollable.[92] The point for now is that even in the absence of such limits, this potential threat of liability is relatively insignificant and does not come close to the skeptics' broad descriptive claims about massive multiple regulation of individual users.

C. Indirect Regulation of Extraterritorial Activity

Indeed, if the limits on enforcement jurisdiction support any of the skeptics' descriptive claims, it is their somewhat different claim that because of the potential for regulation evasion, cyberspace transactions are beyond the regulatory powers of territorial governments.[93] Cyberspace content providers can, at some cost, shift the source of their information flows to jurisdictions beyond the enforceable scope of national regulation and thus continue information transmissions into the regulating jurisdiction.[94] For example, they can relocate in geographical space, or employ telnet or anonymous remailers to make the geographical source of their

---

[90] See, for example, Johnson and Post, 48 Stan L Rev at 1374 (cited in note 3).

[91] This is the topic of the next Section.

[92] I examine this normative question in Section IV.C.

[93] This component of the skeptics' argument is in tension with their concerns about the threat of multiple regulation. If, as they claim, cyberspace users can easily relocate the source of their transmissions to evade legal enforcement, and if, as they further claim, the physical location of parties transacting in cyberspace is "*indeterminate* both *ex ante* and *ex post*," see Post and Johnson, *Borders, Spillovers, and Complexity* at 3 (cited in note 3), then cyberspace users have little to fear from multiple national regulation.

[94] See Post, 1995 J Online L, Article 3 at para 40 (cited in note 3).

content difficult to discern.[95] These and related regulatory evasion techniques can make it difficult for a nation to regulate the extraterritorial supply side of harmful cyberspace activity.

Regulation evasion of this sort is not limited to cyberspace. For example, corporations reincorporate to avoid mandatory laws and criminals launder money offshore. Closer to point, offshore regulation evasion has been a prominent characteristic of other communication media. For example, Radio-Free Europe broadcast from western Europe into the former Soviet Union but lacked a regulatable presence there.[96] Similarly, television signals are sometimes broadcast from abroad by an entity with no local presence. The extraterritorial source of these and many other non-cyberspace activities is beyond the enforceable scope of local regulation. But this does not mean that local regulation is inefficacious. In cyberspace as in real space, offshore regulation evasion does not prevent a nation from regulating the extraterritorial activity.

This is so because a nation can regulate people and equipment in its territory to control the local effects of the extraterritorial activity. Such indirect regulation is how nations have, with varying degrees of success, regulated local harms caused by other communications media with offshore sources and no local presence.[97] And it is how nations have begun to regulate local harms caused by offshore Internet 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.[98] They also regulate the local means through which for-

---

[95] Telnet allows a computer user to log into a remote computer over the Internet. Once connected to the foreign computer, the user can perform any Internet function, such as sending e-mail or "telnetting" to yet other servers, as though she were logged on to a terminal at the foreign computer's location. An anonymous remailer is a service that allows the sender of an e-mail to remain anonymous by sending the message through an intermediary that strips the message of the identifying characteristics of the original sender. The receiver of the e-mail can respond to the e-mail by sending an e-mail to the intermediary, which then forwards it to the sender.

[96] See generally Stephen D. Krasner, *Global Communications and National Power: Life on the Pareto Frontier*, 43 World Pol 336, 343-46 (1991).

[97] Id.

[98] Consider two of many examples. Pending legislation in the United States Congress would impose criminal penalties on persons in the United States who gamble on the Internet. See Internet Gambling Prohibition Act of 1998, S Amend 3266 to S 2260, 105th Cong, 2d Sess (July 22, 1998); Internet Gambling Prohibition Act of 1998, HR 4427, 105th Cong, 2d Sess (Aug 6, 1998). Chinese law punishes in-state Internet users who access or transmit a broader array of prohibited information. See Computer Information Network and Internet Security, Protection and Management Regulations (approved by the State Council on December 11, 1997 and promulgated by the Ministry of Public Security on December 30, 1997), available online at <www.gilc.org/speech/china/net-regs-1297.html>

eign content is transmitted. For example, they impose screening obligations on in-state Internet service providers and other entities that supply or transmit information.[99] Or they regulate in-state hardware and software through which such transmissions are received.[100] Or they regulate the local financial intermediaries that make commercial transactions on the Internet possible.[101]

These and related regulations of domestic persons and property make it more costly, and thus more difficult, for in-state users to obtain content from, or transact with, regulation evaders abroad. In this fashion a nation can indirectly regulate the extraterritorial supply of prohibited content even though the source of the content is beyond its enforcement jurisdiction and even though it cannot easily stop transmission at the border. These various forms of indirect regulation will not be perfect in the sense of eliminating regulation evasion. But few regulations are perfect in this sense, and regulation need not be perfect in this sense to be effective.[102] The question is always whether the regulation will heighten the costs of the activity sufficiently to achieve

---

(visited Sept 11, 1998).

[99] For example, a new German law imposes liability on Internet service providers if they knowingly offer a venue for content illegal in Germany and fail to use technically possible and reasonable means to block it. See *Germany to Enforce Child-Friendly Internet*, Chi Trib 4 (July 5, 1997). Australia is about to implement a similar law. See *Electronic Frontiers Australia, Internet Regulation in Australia*, available online at <www.efa.org.au/Issues/Censor/cens1.html> (visited Sept 10, 1998). In the United States, pending federal Internet gambling legislation would authorize the federal government to order service providers, at risk of penalty, to discontinue the availability of illegal gambling sites. See Internet Gambling Prohibition Act of 1998, S Amend 3266 to S 2260 (cited in note 98). Legislation is also pending that would require senders of unsolicited commercial e-mail to identify themselves in a way that would enable Internet service providers to filter such messages. See Jeri Clausing, *Compressed Data; House E-Mail Effort Raises Censorship Issues*, NY Times D3 (Aug 10, 1998). And some states have held Internet service providers liable for facilitating the transmission of illegal extraterritorial content into the regulating jurisdiction. See, for example, *Stratton Oakmont, Inc v Prodigy Services Co*, 1995 WL 323710, *4-5 (NY Sup Ct).

[100] This form of regulation is explored in detail in Section III.D.

[101] Compare Matt Beer, *The wagers of the Web; Lawsuit could unravel on-line gaming industry*, San Fran Examiner B1 (Aug 17, 1998) (describing lawsuit by Internet bettor against credit card companies that financed online gambling).

[102] As Lessig notes:

> 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. . . . 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.

Lawrence Lessig, *The Zones of Cyberspace*, 48 Stan L Rev 1403, 1405 (1996).

its acceptable control from whatever normative perspective is appropriate.

In the cyberspace regulation context, the answer to this question depends on empirical and technological issues that are unresolved and that will vary from context to context. The prodigious criticism of and lobbying efforts against proposed regulation of (among other things) digital goods, Internet gambling, and encryption technology suggest that governments can raise the costs of many cyberspace transactions to a significant degree. And of course unilateral national regulation is one of many regulation strategies at a nation's disposal.[103] The point for now is simply that offshore regulation evasion does not, as the skeptics think, undermine a nation's ability to regulate cyberspace transactions. Although a nation will sometimes have difficulty in imposing liability on extraterritorial content providers, it can still significantly regulate the local effects of these providers' activities through laws aimed at local persons and entities.

D. Filtering

We have seen that the skeptics' worries about multiple or extraterritorial regulation of cyberspace activity do not extend to matters for which it is feasible and legal for cyberspace communities to establish private legal regimes, or to matters beyond a nation's enforcement jurisdiction.

But the possibility of extraterritorial and multiple regulations remains. Consider the Bavarian Justice Ministry's threat in December of 1995 to prosecute CompuServe for carrying online discussion groups containing material that violated German anti-pornography laws.[104] CompuServe responded by blocking access to these discussion groups in Germany. Because of the state of then-available technology, this action had the effect of blocking access to these discussion groups for all CompuServe users worldwide.[105] This is precisely what the skeptics fear from unilateral regulation of cyberspace. Germany enforced a mandatory law against an international access provider with a presence (office, staff, servers, etc.) in Germany. Faced with multiple regulatory regimes in the many places where it did business, CompuServe bowed to the most restrictive. The consequence was massive extraterritorial regulation, for the German regulation interrupted

---

[103] As we shall see in Section III.E, nations can further regulate extraterritorial supply through international harmonization.

[104] See Nathaniel Nash, *Holding Compuserve Responsible*, NY Times D4 (Jan 15, 1996).

[105] See id.

the flow and availability of the discussion groups for CompuServe clients everywhere in the world.

The skeptics frequently recount this story to show how unilateral national regulation of cyberspace can have multijurisdictional consequences.[106] But the rest of the story suggests a somewhat different lesson. After closing down transmission of the offending discussions, CompuServe offered its German users software that enabled them to block access to the offending discussion groups.[107] The company then began to search for a more centralized way to filter the illegal newsgroups in Germany alone. German prosecutors subsequently indicted a CompuServe executive, alleging that the company failed to implement such national-level filtering technology to prevent dissemination of other illegal information in Germany.[108] At about the same time, the German parliament enacted a law clarifying that cyberspace access providers are liable "if they are aware of the content" and fail to use "*technically possible and reasonable*" means to block it.[109]

The subsequent events of the CompuServe controversy, like the response to the Supreme Court's invalidation of the Communications Decency Act in *Reno*,[110] make clear the growing importance of information discrimination technology to the cyberspace regulation debate. Many jurisdictional challenges presented by cyberspace result from the purported inability of content providers to prevent information flows from appearing simultaneously in every jurisdiction. Thus far I have assumed, with the skeptics, that this is a necessary (and accurate) feature of cyberspace architecture. But it is not.[111] Cyberspace information can only ap-

---

[106] See, for example, Johnson and Post, 48 Stan L Rev at 1373 & n 20 (cited in note 3).

[107] See Edmund L. Andrews, *Germany's Efforts to Police Web Are Upsetting Business*, NY Times A1 (June 6, 1997).

[108] See id; *Germany Brings Criminal Charges Against CompuServe Manager*, Eurowatch (May 2, 1997). The CompuServe executive was later convicted, even though at trial's end the prosecution sought acquittal because it agreed with the defense that, at the time of the indictment, CompuServe lacked the technological means to block the illegal material. *Battle of the Somm* (May 29, 1998), available online at <www.wired.com/news/news/politics/story/12607.html> (visited Sept 10, 1998).

[109] Jordan Bonfante, *The Internet Trials: Germany Makes an Early Attempt at Taming the Wide, Wild Web. But Many are Crying Foul—or Folly*, Time 30 (Intl ed July 14, 1997) (emphasis added).

[110] See ACLU White Paper, *Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet* (1997), available online at <www.aclu.org/issues/cyber/burning.html> (visited Apr 1, 1998) (warning of censorship threats posed by rating and filtering proposals that flourished in wake of *Reno*); Lawrence Lessig, *Tyranny in the Infrastructure*, Wired (July 1997), available online at <www.wired.com/wired/5.07/cyber_rights.html> (visited Apr 1, 1998) (same).

[111] See Lessig, *Tyranny in the Infrastructure*, Wired (cited in note 110); Boyle, 66 U Cin L Rev at 191-96 (cited in note 3).

pear in a geographical jurisdiction by virtue of hardware and software physically present in the jurisdiction. Available technology already permits governments and private entities to regulate the design and function of hardware and software to facilitate discrimination of cyberspace information flows along a variety of dimensions, including geography, network, and content.[112] This technology is relatively new and still relatively crude, but it is growing very quickly in both sophistication and effectiveness. This technology facilitates discrimination and control of information flows at any of several junctures along the cyberspace information stream.

At the most basic level, the content provider can take steps to control the flow of the information. This happens, for example, whenever a web page operator conditions access to the page on the users' presentation of information. Consider the many precautions taken by adult web pages. Some pages simply warn minors or persons from certain geographical locations not to view or enter, and disclaim legal liability if they do.[113] Others condition access on proof of age or on membership in one of dozens of pri-

---

[112] In addition to the discussion below, see Jonathan Weinberg, *Rating the Net*, 19 Hastings Comm/Enter L J 453 (1997); Paul Resnick, *Filtering Information on the Internet*, Scientific Am 62-64 (Mar 1997); Reidenberg, 76 Tex L Rev at 556-68 (cited in note 60).

[113] For example, Sexroulette.com includes the following conditions upon entry to its pages:

> WARNING: You are about to enter an ADULT ONLY area. You must agree to the following terms before proceeding: . . . . If you are under the age of eighteen years . . . you are not authorized to download any materials from XPICS and any and all such downloading shall constitute intentional infringement of XPICS's rights in such materials.
>
> All materials, messages, and other communications contained at XPICS are intended for distribution exclusively to consenting adults in locations where such materials, messages and other communications do not violate any community standards or any federal, state or local law or regulation of the United States or any other country. No materials from any parts of XPICS designated as "XXX" are authorized to or otherwise may be downloaded to persons located in the following areas: Alabama, Florida, except Ft. Lauderdale, Miami, and St. Petersburg, Georgia, except Atlanta, Kansas, except Kansas City, Kentucky, Minnesota, Missouri, Mississippi, North Carolina, Ohio, except Cleveland and Cincinnati, Pennsylvania, except Philadelphia and Pittsburgh, South Carolina, Tennessee, except for Nashville, Utah, Afghanistan, Kuwait, Iran, Iraq, Japan, Jordan, Libya, Pakistan, The Republic of China, Singapore, Saudi Arabia, Syria, The United Arab Emirates, or any other place in which to do so would constitute a violation of any law, regulation, rule or custom. Any and all unauthorized downloading of materials from XPICS shall constitute intentional infringement of XPICS's rights in such materials.
>
> . . .
>
> If you agree with the above, you may ENTER. If you don't agree, you must EXIT.

<members.sexroulette.com> (visited Apr 1, 1998).

vate age-verification services.[114] Others require potential end-users to send by fax or telephone information specifying age and geographical location.[115] Still others label or rate their pages in order to accommodate end-use filtering software, as described below. Finally, digital identification technology developed for Internet commerce provides a way to authenticate the identity of a party in a cyberspace transaction.[116] Although digital identification is usually used to verify who someone is, it can also be used to verify other facts about cyberspace users, such as their nationality, domicile, or permanent address.

At the other end of the distribution chain, end-users can employ software filters to block out or discriminate among information flows.[117] Parental control software is the most prominent example of an end-user filter, but many businesses and other local area networks also employ these technologies. Content filters also can be imposed at junctures along the cyberspace information stream between content providers and end-users. They can be imposed, for example, at the network level or at the level of the Internet service provider. They can also assist governments in filtering information at the national level.[118] A government can choose to have no Internet links whatsoever and to regulate tele-

---

[114] See, for example, The Adult Check System, <www.adultcheck.com> (visited Sept 10, 1998).

[115] In many of the well-known cyberspace regulation cases, the defendants knew that they were sending content into the regulating jurisdiction because they had conditioned the users' request for the content on the presentation of information (including geographical identification) by fax or mail. See, for example, *Thomas*, 74 F3d at 705; *Playboy Enterprises, Inc v Chuckleberry Publishing, Inc*, 939 F Supp 1032, 1035 (S D NY 1996); *State v Granite Gate Resorts, Inc*, 1996 WL 767431, *4 (Minn Dist Ct), affd, 568 NW2d 715 (Minn App 1997).

[116] See generally *Introduction to Client Digital ID's*[SM], available online at <www.verisign.com/repository/brwidint.htm> (visited Apr 1, 1998); A. Michael Froomkin, *The Essential Role of Trusted Third Parties In Electronic Commerce*, 75 Or L Rev 49, 55-60 (1996).

[117] First generation software filters blocked access to individually compiled lists of prohibited Internet addresses. See Weinberg, 19 Hastings Comm/Enter L J at 457 (cited in note 112). More recently, a much more sophisticated industry-wide standard for labeling, rating, and filtering Internet information has emerged. This standard, known as PICS, establishes content-neutral labeling formats and distribution methods. The PICS format does not specify a labeling vocabulary or what should be done with the labels. Instead, the PICS format allows both content providers and independent entities to label content along several dimensions. Selection software then decides what to do with these labels—whether to block them, restrict access, highlight them, organize them in certain ways, or whatever else the software is designed for.

[118] See Timothy S. Wu, Note, *Cyberspace Sovereignty?—The Internet and the International System*, 10 Harv J L & Tech 647, 649-56 (1997); Delacourt, 38 Harv J Intl L at 208-19 (cited in note 3); Paul Resnick, *PICS, Censorship, & Intellectual Freedom FAQ*, version 1.14, available online at <www.si.umich.edu/~presnick/pics/intfree/faq.htm> (visited Apr 1, 1998).

phone and other communication lines to access providers in other countries.[119] China, Singapore, and the United Arab Emirates have taken the somewhat less severe steps of (i) regulating access to the Net through centralized filtered servers, and (ii) requiring filters for in-state Internet service providers and end-users.[120] We have seen that Germany has chosen to hold liable Internet access providers who have knowledge of illegal content and fail to use "technically possible and reasonable" means to filter it.[121] The Federal Communications Commission recently required V-chip blocking technology to be placed in computers capable of receiving video broadcasting,[122] and pending anti-spam legislation would impose identification requirements on commercial e-mail senders and filtering requirements on Internet service providers.[123] There are numerous other possibilities.[124]

Although technological predictions are precarious, it seems likely that the techniques and technologies for controlling cyberspace information flows will continue to develop in scope and sophistication, and will play an important role in resolving the jurisdictional quandaries presented by the "borderless" medium. Information is not particularly useful unless people can organize, select, and block it.[125] This is one reason why information filtering is an essential component of all communications media.[126] Filtering is especially important for cyberspace, where the costs of information production and dissemination are extremely low, and thus information overload is a serious concern. Indeed, the explosive growth of the World Wide Web is directly attributable to the

---

[119] See Wu, Note, 10 Harv J L & Tech at 651 (cited in note 118) ("As of July 1996, at least thirty-three states were completely unconnected.").

[120] See id at 652-54 (China, Singapore); Madanmohan Rao, *Persian Gulf Net Censorship: Governments Force Server Blockades* (Oct 3, 1997), available online at <media info.elpress.com/ephome/news/newshtm/webnews/glob1003.htm> (visited Apr 1, 1998) (United Arab Emirates).

[121] See text accompanying notes 104-09.

[122] See Christopher Stern, *V-chip on fast track as FCC ok's tech spex*, Variety 27 (Mar 16-22, 1998); Brooks Boliek, *Television sharpens bite: V-chip wins FCC approval*, Hollywood Reporter 15 (Mar 13, 1998).

[123] See Clausing, *Compressed Data*, NY Times D3 (cited in note 99).

[124] Many predict that Congress will more broadly require filtering or digital identification technology to be built into the architecture of cyberspace. See Boyle, 66 U Cin L Rev at 193, 202-04 (cited in note 3); Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 Jurimetrics J 629 (forthcoming 1998). Even in the absence of direct governmental mandates, the threat of such regulation has already spurred the development and adoption of an array of private de facto Internet discrimination standards that facilitate extensive private regulation of the Net.

[125] See J.M. Balkin, *Media Filters, the V-Chip, and the Foundations of Broadcast Regulation*, 45 Duke L J 1131, 1141-44 (1996) (describing the filtering of information in print and broadcast media).

[126] Id at 1143.

invention of identification and filtering technologies that made it possible to organize and select from the morass of available information.[127]

An additional reason that techniques for controlling cyberspace information flows are likely to be at least moderately successful is that so many participants in the cyberspace regulation debate—parents, businesses, content suppliers, service providers, governments, and even some anticensorship civil libertarians[128]—desire such control. As Resnick has pointed out, "meta-data systems . . . are going to be an important part of the Web, because they enable more sophisticated commerce . . . , communication, indexing, and searching services."[129] Many jurisdictions have already mandated the use of filtering and identification mechanisms.[130] Even in the absence of government mandates, content filtering and digital identification technologies have flourished for commerical reasons and in response to the threat of regulation, and have become de facto standards in many cyberspace contexts.

Many commentators are skeptical about these filtering and identification technologies.[131] They argue that content filters invariably both over- and under-filter; that identification technologies sometimes misidentify; and that some hackers will access prohibited information. These worries are to some degree well-founded. What is not well-founded, however, is the belief that imperfect regulation means ineffective regulation.[132] Real space is filled with similarly imperfect filtering and identification techniques: criminals crack safes and escape from jail, fifteen year olds visit bars with fake IDs, secret information is leaked to the press, and so on. In cyberspace as in real space, imperfections in filtering and identification regimes do not render the regimes ineffective.[133] Although the ultimate accuracy of cyberspace filtering

---

[127] See Robert H. Reid, *Architects of the Web: 1000 Days that Built the Future of Business* xxiii-xxiv (Wiley 1997).

[128] Some civil libertarians favor information filtering technologies because they allow individuals—rather than the government—to decide what information is appropriate for their own (or their children's) consumption. See, for example, Brief of Feminists for Free Expression as Amicus Curiae in support of Appellees, *Reno v ACLU*, 117 S Ct 2329 (1997), available at 1997 WL 74382, *15-16.

[129] Resnick, *PICS, Censorship & Intellectual Freedom* at 3 (cited in note 118).

[130] See Johnson and Post, 48 Stan L Rev at 1373-74 & n 20 (cited in note 3); notes 122-24 and accompanying text.

[131] See, for example, Weinberg, 19 Hastings Comm/Enter L J at 459-70 (cited in note 112); Johnson and Post, 48 Stan L Rev at 1373-74 (cited in note 3); Electronic Privacy Information Center, *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet*, available online at <www2.epic.org/reports/filter_report.htm> (visited Apr 1, 1998).

[132] See, for example, Johnson and Post, 48 Stan L Rev at 1372-74 (cited in note 3).

[133] See note 102 and accompanying text.

and identification technologies remains an open question, there is little doubt that such technologies will contribute significantly to cyberspace regulation by enabling governments, content providers, end-users, and service providers to raise significantly the cost of accessing certain information. Indeed, this has already happened throughout cyberspace, where content filtering, conditioned access, and identification codes are pervasive.

The ability to control information flows alleviates the many cyberspace regulation problems that are premised on the assumption that information in cyberspace appears simultaneously in every jurisdiction. To see why, consider one set of differences between a newspaper publisher and a cyberspace content provider. It is relatively uncontroversial that a newspaper publisher is liable for harms caused wherever the newspaper is published or distributed. This seems appropriate because, among other reasons, we think the publisher can control the geographical locus of publication and distribution. Requiring such control imposes modest costs on the publisher; she must, for example, keep abreast of regulatory developments in different jurisdictions and take steps to exclude publication and distribution in places where she wants to avoid liability.

Now consider the cyberspace content provider. Many have an intuition that such content providers should not be liable for harms caused wherever the content appears.[134] The primary basis for this intuition is that the content provider cannot control the geographical and network distribution of his information flows. But this latter point is groundless. Content providers already have several means to control information flows.[135] As the cost of such control continues to drop, and the accuracy and ease of this control increases, cyberspace content providers will come to occupy the same position as the newspaper publisher. It will thus be appropriate in cyberspace, as in real space, for the law to impose small costs on both types of publisher to ensure that content does not appear in jurisdictions and networks where it is illegal.

E. International Harmonization

Private legal ordering, the limitations on enforcement jurisdiction, indirect regulation, and effective information flow control, taken together, go a long way toward redressing the skeptics' descriptive claims about the infeasibility of cyberspace regulation. These techniques will not resolve all conflict of laws in cyberspace

---

[134] See, for example, Johnson and Post, 48 Stan L Rev at 1375-76 (cited in note 3).

[135] See notes 113-16 and accompanying text.

any more than they do in real space. Nor will they definitively resolve the problem of the relative ease by which information suppliers can "relocate" into a safe haven outside of the regulating jurisdiction, a problem that also has many real-space analogies.[136] When similar spillover and evasion problems have occurred with respect to non-cyberspace transactions, nations have responded with a variety of international harmonization strategies.

The same harmonization strategies are being used today to address the challenges presented by cyberspace transactions. A few examples will suffice. Several recent treaties and related multinational edicts have strengthened digital content owners' right to control the distribution and presentation of their property online.[137] These harmonization efforts grow out of an international copyright regime that is over one hundred years old.[138] The G8 economic powers have recently begun to coordinate regulatory efforts concerning cyberspace-related crimes in five areas: pedophilia and sexual exploitation; drug-trafficking; money-laundering; electronic fraud; and industrial and state espionage.[139] These initiatives mirror similar efforts to redress similar regulatory leakage problems in real-space contexts such as environmental policy, banking and insurance supervision, and antitrust regulation.[140] Several international organizations have drafted model laws and guidelines to facilitate Internet commerce and related digital certification issues.[141] There are scores of other international efforts in a variety of cyberspace-related contexts.

---

[136] See discussion in Section II.

[137] In December 1996, the World Intellectual Property Organization ("WIPO") reached agreement on a treaty that significantly extended international copyright protection for digital property. See WIPO Copyright Treaty, adopted Dec 20, 1996, WIPO Pub No 226(E) (WIPO 1997); Seth Schiesel, *Global Agreement Reached to Widen Law on Copyright*, NY Times 1 (Dec 21, 1996). Within a year, the European Commission issued a draft directive to bring European law into line with these international obligations. See *Draft EC Directive Provides Strong Online Copyright Protection, Outlaws Devices Facilitating Infringement*, BNA Electronic Commerce and L Rep (Mar 13, 1998), available online at <www.bna.com/e-law/main.htm> (visited Apr 1, 1998). The United States is in the process of enacting similar legislation. See WIPO Copyright Treaties Implementation Act, HR 2281, 105th Cong, 1st Sess (July 29, 1997); Digital Millenium Copyright Act of 1998, S 2037, 105th Cong, 2d Sess (May 6, 1998).

[138] The digital protection treaty signed in Geneva operates as a protocol to the Berne Convention for the Protection of Literary and Artistic Works, a treaty regime that began in 1886. See *Berne Convention for the Protection of Literary and Artistic Works* (WIPO 1970).

[139] See Clifford Krauss, *8 Countries Join in an Effort To Catch Computer Criminals*, NY Times A12 (Dec 11, 1997).

[140] See Anne-Marie Slaughter, *The Real New World Order*, Foreign Affairs 183, 189-92 (Sep/Oct 1997).

[141] For example, in February 1997, the United Nations Commission on International Trade Law ("UNCITRAL") began to draft model international digital signature legislation.

International harmonization is not always (or even usually) the best response to the spillovers and evasions that result from unilateral regulation.[142] And harmonization is often not easy to achieve. However, the proliferation of international organizations, in combination with modern means of communication and transportation, has helped to facilitate international harmonization. Harmonization is especially likely in those contexts—like many aspects of criminal law enforcement—where nations' interests converge and the gains from cooperation are high. But nations sometimes lack the incentive to participate in international regimes, and there are often international and domestic political economy obstacles to harmonization.[143] It is too early to tell how successful international efforts will be in addressing the challenges of cyberspace. It is clear, however, that international harmonization will play an important role in nations' overall cyberspace-regulation strategy.

F. Residual Choice-of-Law Tools

The skeptics' implicit goal of eliminating all conflicts of laws that arise from cyberspace transactions is unrealistic. Private legal ordering, the limits of enforcement jurisdiction, indirect regulation of extraterritorial activity, filtering and identification technology, and international cooperation facilitate and rationalize legal regulation of cyberspace. These tools, however, will not eliminate all conflicts of laws in cyberspace any more than they do in real space. Transnational activity is too complex. As mentioned above, the elimination of conflict of laws would require the elimination of decentralized lawmaking or of transnational activity.[144] In this light, the enormous increases in the pervasiveness and complexity of conflict of laws in this century can be viewed as

---

See *Report of the Working Group on Electronic Commerce*, Thirty-First Session (New York, Feb 12-28, 1997). See also UNCITRAL Working Group on Electronic Commerce, *Planning Of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues* A/CN.9/WG.IV/WP.71 (Dec 31, 1996). Similarly, in November 1997, the International Chamber of Commerce issued the General Usage for International Digitally Ensured Commerce ("GUIDEC"), a set of guidelines for ensuring trustworthy digital transactions over the Internet, available online at <www.iccwbo.org/guidec2/htm> (visited Apr 5, 1998). And the Organisation for Economic Co-operation and Development ("OECD") recently adopted principles to guide countries in formulating their own policies and legislation relating to the use of cryptography. See *OECD Cryptography Policy: The Guidelines and the Issues*, Unclassified OCDE/GD(97)204 (1997), available online at <www.oecd.org/dsti/sti/it/secur/prod/GD97-204.htm> (visited Apr 2, 1998).

[142] See Leebron, *Lying Down with Procrustes* (cited in note 59).

[143] See, for example, Krasner, 43 World Pol at 337-60 (cited in note 96); Andrew T. Guzman, *Is International Antitrust Possible?*, 73 NYU L Rev (forthcoming 1998).

[144] See text accompanying notes 58-59.

an acceptable cost to a world that wishes to expand transnational activity while retaining decentralized lawmaking. As persistent conflicts become prohibitively costly to private parties and regulating nations, public or private international coordination or technological innovation becomes more attractive and thus more likely.

Short of these developments, transnational transactions in cyberspace, like transnational transactions mediated by telephone and mail, will continue to give rise to disputes that present challenging choice-of-law issues. For example: "Whose substantive legal rules apply to a defamatory message that is written by someone in Mexico, read by someone in Israel by means of an Internet server located in the United States, injuring the reputation of a Norwegian?"[145] Similarly,

> [w]hich of the many plausibly applicable bodies of copyright law do we consult to determine whether a hyperlink on a World Wide Web page located on a server in France and constructed by a Filipino citizen, which points to a server in Brazil that contains materials protected by German and French (but not Brazilian) copyright law, which is downloaded to a server in the United States and reposted to a Usenet newsgroup, constitutes a remediable infringement of copyright?[146]

It would be silly to try to formulate a general theory of how such issues should be resolved. One lesson of this century's many failures in top-down choice-of-law theorizing is that choice-of-law rules are most effective when they are grounded in and sensitive to the concrete details of particular legal contexts. This does not mean that standards are better than rules in this context. It simply means that in designing choice-of-law rules or standards, it is better to begin at the micro rather than macro level, and to examine recurrent fact patterns and implicated interests in discrete legal contexts rather than devise a general context-transcendent theory of conflicts.[147]

With these caveats in mind, I want to explain in very general terms why the residual choice-of-law problems implicated by cy-

---

[145] Perritt, 41 Vill L Rev at 3 (cited in note 78).

[146] Post and Johnson, *Borders, Spillovers, and Complexity* at 2-3 (cited in note 3).

[147] Many European conflict systems demonstrate that it is both possible and useful to design choice-of-law rules that are context-sensitive and not beholden to any grand choice-of-law theory. See, for example, Swiss Private International Law Statute of December 18, 1987, translated in Andreas Bucher and Pierre-Yves Tschanz, *International Arbitration in Switzerland* 225 (Helbing & Lichtenhahn 1988).

berspace are not significantly different from those that are non-cyberspace conflicts. Cyberspace presents two related choice-of-law problems. The first is the problem of *complexity*. This is the problem of how to choose a single governing law for cyberspace activity that has multijurisdictional contacts. The second problem concerns *situs*. This is the problem of how to choose a governing law when the locus of activity cannot easily be pinpointed in geographical space. Both problems raise similar concerns. The choice of any dispositive geographical contact or any particular law in these cases will often seem arbitrary because several jurisdictions have a legitimate claim to apply their law. Whatever law is chosen, seemingly genuine regulatory interests of the nations whose laws are not applied may be impaired.

The problems of complexity and situs are genuine. They are not, however, unique to cyberspace. Identical problems arise all the time in real space. In fact, they inhere in every true conflict of laws. Consider the problem of complexity. The hypotheticals concerning copyright infringements and multistate libels in cyberspace are no more complex than the same issues in real space.[148] They also are no more complex or challenging than similar issues presented by increasingly prevalent real-space events such as airplane crashes, mass torts, multistate insurance coverage, or multinational commercial transactions, all of which form the bread and butter of modern conflict of laws.[149] Indeed, they are no more complex than a simple products liability suit arising from a two-car accident among residents of the same state, which can implicate the laws of several states, including the place of the accident, the states where the car and tire manufacturers are headquartered, the states where the car and tires were manufactured, and the state where the car was purchased.[150]

Resolution of choice-of-law problems in these contexts is challenging. But the skeptics overstate the challenge. Not every geographical contact is of equal significance. For example, in the copyright hypothetical above, the laws of the source country and the end-use countries have a much greater claim to governing the copyright action than the laws of the country of the person who

---

[148] See *London Film Productions v Intercontinental Communications, Inc*, 580 F Supp 47, 48-49 (S D NY 1984) (involving a British corporation suing an American corporation for copyright infringement in Chile, Venezuela, Peru, Equador, Costa Rica, and Panama); Eugene F. Scoles and Peter Hay, *Conflict of Laws* 631 (West 2d ed 1992) (describing choice-of-law rules for multistate libel).

[149] See generally Larry Kramer, *Choice of Law in Complex Litigation*, 71 NYU L Rev 547, 551-65 (1996).

[150] See, for example, *Rutherford v Goodyear Tire and Rubber Co*, 943 F Supp 789, 790-91 (W D Ky 1996), affd, 142 F3d 436 (6th Cir 1998).

built the server and the country of the server whose hyperlink pointed to the server that contained the infringing material.[151] The limits on enforcement jurisdiction may further minimize the scope of the conflict.[152] In addition, even in extraordinarily complex cases where numerous laws potentially apply, these laws will often involve similar legal standards, thus limiting the actual choice of law to two or perhaps three options.[153] Finally, these complex transactions need not be governed by a single law. Applying different laws to different aspects of a complex transaction is a perfectly legitimate choice-of-law technique.[154]

The application of a single law to complex multijurisdictional conflicts will sometimes seem arbitrary and will invariably produce spillover effects. But as explained above, the arbitrariness of the chosen law, and the spillovers produced by application of this law, inhere in all conflict situations in which two or more nations, on the basis of territorial or domiciliary contacts, have a legitimate claim to apply their law. When in particular contexts the arbitrariness and spillovers become too severe, a uniform international solution remains possible. Short of such harmonization, the choice-of-law issues implicated by cyberspace transactions are no more complex than the issues raised by functionally identical multijurisdictional transactions that occur in real space all the time.

Like the problem of complexity, the situs problem is a pervasive and familiar feature of real-space jurisdictional conflicts. A classic difficulty is the situs of intangibles like a debt or a bank deposit.[155] More generally, the situs problem arises whenever legally significant activity touches on two or more states. For example, when adultery committed in one state alienates the affections of a spouse in another, the situs of the tort is not self-evident. It depends on what contact the forum's choice-of-law rule deems dispositive. Similar locus difficulties arise when the tort takes place over many states, such as when poison is adminis-

---

[151] For an excellent analysis of how traditional choice-of-law rules might apply to copyright violations in cyberspace, see Jane C. Ginsburg, *Copyright Without Borders?: Choice of Forum and Choice of Law for Copyright Infringement in Cyberspace*, 15 Cardozo Arts & Enter L J 153, 168-74 (1997).

[152] See Section III.B.

[153] See Kramer, 71 NYU L Rev at 583 (cited in note 149).

[154] This is known as "depecage." See Brilmayer, *Conflict of Laws* at 366 (cited in note 32).

[155] See Peter S. Smedresman and Andreas F. Lowenfeld, *Eurodollars, Multinational Banks, and National Laws*, 64 NYU L Rev 733, 734-37 (1989) (discussing the bank deposit problem); Andreas F. Lowenfeld, *In Search of the Intangible: A Comment on* Shaffer v. Heitner, 53 NYU L Rev 102, 115-17, 122-24 (1978) (exploring situs of debt problem largely in context of personal jurisdiction).

tered in one state, takes effect in another, and kills in a third. The situs problem even arises when a bodily injury occurs in one state based on negligence committed in another, for there is no logical reason why the place of injury should be viewed as *the place* of the tort any more than should the place of negligence.[156] In all of these situations, the importance of any particular geographical contact is never self-evident; it is a *legal* rather than a *factual* consideration that is built into the forum's choice-of-law rules. As the geographical contacts of a transaction proliferate, the choice of any one contact as dispositive runs the risk of appearing arbitrary. But again, this problem pervades real-space conflicts of law and is not unique to cyberspace conflicts.

So the complexity and situs problems inhere to some degree in all transnational conflicts, and are exacerbated in real space and cyberspace alike as jurisdictional contacts proliferate. No choice-of-law rule will prove wholly satisfactory in these situations. However, several factors diminish the skeptics' concerns about the infeasibility of applying traditional choice-of-law tools to cyberspace. For example, the skeptics are wrong to the extent that they believe that cyberspace transactions must be resolved on the basis of geographical choice-of-law criteria that are sometimes difficult to apply to cyberspace, such as where events occur or where people are located at the time of the transaction. But these are not the only choice-of-law criteria, and certainly not the best in contexts where the geographical locus of events is so unclear. Domicile (and its cognates, such as citizenship, principal place of business, habitual residence, and so on) are also valid choice-of-law criteria that have particular relevance to problems, like those in cyberspace, that involve the regulation of intangibles or of multinational transactions.

The skeptics are further mistaken to the extent that their arguments assume that all choice-of-law problems must be resolved by *multilateral* choice-of-law methodologies. A multilateral methodology asks which of several possible laws governs a transaction, and selects one of these laws on the basis of specified criteria. Multilateral methods accentuate the situs and complexity problems. But the regulatory issues that are most relevant to the cyberspace governance debate almost always involve *unilateral*

---

[156] See Larry Kramer, *Vestiges of Beale: Extraterritorial Application of American Law*, 1991 S Ct Rev 179, 190 n 36. A similar problem is presented by multistate contracts. When contractual negotiations and signings take place in two states, the place of the contract might be either state, depending on what contact the forum's choice-of-law rule deems dispositive for this purpose.

choice-of-law methods that alleviate these problems.[157] A unilateral method considers only whether the dispute at issue has close enough connections to the forum to justify the application of local law.[158] If so, local law applies; if not, the case is dismissed and the potential applicability of foreign law is not considered. For example, a jurisdiction typically does not apply foreign criminal law. If a Tennessee court has personal jurisdiction over someone from across the Virginia border who shot and killed an in-stater, the court does not consider whether Tennessee or Virginia law applies. It considers only whether Tennessee law applies. If so, the case proceeds; if not, it is dismissed.[159]

Unilateral choice-of-law methods make the complexity and situs problems less significant. They do not require a determination of which of a number of possible laws apply. Nor do they require a court to identify where certain events occurred. What matters is simply whether the activity has local effects that are significant enough to implicate local law. By failing to recognize that courts can and will use unilateral rather than multilateral choice-of-law methods to resolve cyberspace conflicts, the skeptics again exaggerate the challenge of cyberspace regulation.

G. Number and Velocity of Transactions

The skeptics' final descriptive claim is that even if cyberspace transactions appear like real-space transnational transactions in other respects, they differ significantly with respect to the velocity and number of transactions.[160] Cyberspace dramatically lowers the costs of multinational communication. With only a computer and Internet access, anyone in the world can communicate with anyone, and potentially everyone, in the world. The skeptics believe communications via cyberspace will be so prevalent that governments will not find it cost-effective to regulate them.[161]

A dramatic increase in the number and speed of transactions might well multiply the aggregate harms from such transactions. But this increases rather than decreases a nation's incentives to regulate. Consider Internet gambling. In pre-Internet days, indi-

---

[157] See Lowenfeld, *International Litigation and the Quest for Reasonableness* at 5 (cited in note 48).

[158] See Dodge, 39 Harv Intl L J at 108-10 (cited in note 36).

[159] The same analysis applies in the international context for the extraterritorial application of other regulatory laws like RICO and the antitrust and securities laws. The question in these cases is whether Congress intended for federal law to apply to conduct abroad. If so, these laws apply. If not, the court dismisses the case without considering the application of foreign law.

[160] See Johnson and Post, 48 Stan L Rev at 1372-73 (cited in note 3).

[161] See id.

viduals in the United States could gamble from home or work via telephone with domestic and offshore bookies. Although this form of gambling was regulated by a variety of state and federal statutes, the statutes were filled with loopholes and rarely enforced because transactions were relatively infrequent.[162] Internet gambling makes it significantly easier to gamble from home or work. This has led to a dramatic increase in gambling and a related rise in the costs of gambling that governments worry about: fraud, diminution in local gambling and other entertainment expenditures, loss of tax revenues, decreased productivity, gambling by children, and so on. Not surprisingly, federal and state governments are beginning to regulate gambling much more extensively, and seriously, than ever.[163]

Even with governments' heightened incentives to regulate Internet transactions, some believe that the sheer number of transactions will overwhelm governments' ability to regulate. A related argument is that because *individuals* can so easily engage in transnational communications via the Internet, governmental regulation will be less effective; for individuals operating on the Internet are hard to identify, isolate, and thus sanction. Once again, the conclusion that regulation is infeasible simply does not follow from these premises. The mistake here is the belief that governments regulate only through direct sanctioning of individuals. But of course this is not the only way, or even the usual way, that regulation works. Governments regulate an activity by raising the activity's costs in a manner that achieves desired ends. This can be accomplished through several means other than individual sanctions. Governments can, for example, try to alter the social meaning of the activity, regulate the hardware and software through which the activity takes place, make individual penalties severe and notorious, or impose liability on intermediaries like Internet service providers or credit card companies.

In short, a dramatic increase in the number and velocity of transactions by itself says very little about the feasibility of governmental regulation. Numerous communication advances, beginning with the telegraph, dramatically increased the velocity and number of communications, and lowered their costs. The

---

[162] See Britta Gordon, *Gaming on the Internet: The Odds are on the House, But How Long Will it Last?* 5, available online at <www.cyberlaw.law.ttu.edu/cyberspc/jour9.htm> (visited Apr 1, 1998).

[163] There is currently legislation pending in Congress that would extensively regulate Internet gambling by, among other things, penalizing online bettors and authorizing governmental officials to order Internet service providers to shut down offending online cites. See note 98.

skeptics have provided no reason to think that the differences between cyberspace and prior communication technology are so much greater than the differences between pre- and post-telegraph technology (which reduced communication time from weeks and months to hours and minutes), or between pre- and post-telephone technology (which also dramatically reduced the cost and enhanced the frequency and privacy of transjurisdictional communication) to justify the conclusion that governmental regulation will be nonefficacious.

IV. IS CYBERSPACE REGULATION LEGITIMATE?

Section III explored some of the many ways that nations might regulate cyberspace transactions. This Section considers the skeptics' normative claim that such regulation is illegitimate. This claim is directed primarily to the application of mandatory laws. The skeptics argue that cyberspace should be self-regulated, and that national mandatory laws should not limit these private legal orders. This argument subsumes three closely related claims: (i) unilateral regulation of cyberspace is extraterritorial; (ii) unilateral regulation of cyberspace produces significant spillover effects; and (iii) the structure of cyberspace makes effective notice of territorial regulation impossible. I address each claim in turn.

A. Extraterritoriality

In the Digitalbook.com example above, Singapore and England regulated the local effects of Digitalbook.com's activities in the United States.[164] In the CompuServe example, Germany regulated transmission flows from other countries.[165] These are the types of extraterritorial regulation that worry the skeptics. But such extraterritorial regulation is commonplace in the modern world. As we saw above, it is settled with respect to real-space activity that a nation's right to control events within its territory and to protect its citizens permits it to regulate the local effects of extraterritorial acts.[166]

The same rationale applies to cyberspace because cyberspace is for these purposes no different than real space. Transactions in cyberspace involve real people in one territorial jurisdiction either (i) transacting with real people in other territorial jurisdictions or (ii) engaging in activity in one jurisdiction that causes

---

[164] See text following note 23.

[165] See text accompanying notes 104-09.

[166] See notes 34-37 and accompanying text.

real-world effects in another territorial jurisdiction. To this extent, activity in cyberspace is functionally identical to transnational activity mediated by other means, such as mail or telephone or smoke signal. The new medium of communication is richer, more complex, and much more efficient. But in terms of real-space acts in one jurisdiction that produce real-space effects in another, it is no different from other forms of transnational transaction and communication. And the justification for and legitimacy of regulating local effects is no different. Under current conceptions of territorial sovereignty, a jurisdiction is allowed to regulate extraterritorial acts that cause harmful local effects unless and until it has consented to a higher law (for example, international law or constitutional law) that specifies otherwise.

B. Spillover Effects

The skeptics argue that unilateral extraterritorial regulation of cyberspace differs from similar regulation of real-space activities because of the regulation's spillover effects in other jurisdictions. These effects are inevitable, they think, because information flows in cyberspace appear simultaneously in all territorial jurisdictions. As a result, unilateral territorial regulation of the local effects of cyberspace transmission flows will sometimes affect the flow and regulation of web information in other countries. This is especially true when the regulation is directed at a multijurisdictional access provider, as was the case with Germany's regulation of CompuServe.

Section III described how technology and international cooperation can diminish these spillover effects. But even without these mitigating factors, there is nothing extraordinary or illegitimate about unilateral regulation of transnational activity that affects activity and regulation in other countries. Germany's regulation of CompuServe is no less legitimate than the United States' regulation of the competitiveness of the English reinsurance market, which has worldwide effects on the availability and price of reinsurance.[167] Nor is it any different in this regard from national regulation of transborder pollution, or from national consumer protection regulation of transnational contracts, or from national criminal prohibitions on transnational drug activities, all of which produce spillovers. In many contexts, there are powerful reasons for nations to surrender their regulatory prerogatives in order to reduce spillover and other costs. But at least

[167] See *Hartford Fire Insurance Co*, 509 US at 795-99.

under our current conceptions of territorial sovereignty, such reforms must proceed by national consent. The need for such consent begins from the premise that in its absence, national regulation of local effects is a legitimate incident of sovereignty, even if such regulation produces spillover effects.

Germany's regulation of CompuServe is not just a legitimate incident of territorial sovereignty. It is also fair to CompuServe under a straightforward reciprocal benefits rationale. CompuServe reaps financial and other benefits from its presence in Germany.[168] Without this presence, German enforcement threats would be largely empty. CompuServe need not remain in Germany; it could close its shop there. Its decision to stay in Germany and comply with German regulations might increase the price of its services in Germany and elsewhere. For CompuServe this is a cost of doing business via a new communication medium. The desire to reduce this and related costs is driving the development of technology that permits geographical and other forms of discrimination on the Internet.[169] But even in the absence of such technologies, Germany's local regulation of CompuServe remains within traditional reciprocity-based justifications for regulating local effects.

What about CompuServe users in other countries who are affected by the German regulation? It is hard to see how the German regulation unfairly burdens them. They remain free to choose among dozens of Internet access services that are not affected by the German regulation. Consider further the German perspective. Germany bans certain forms of pornography within its borders. If the medium of this pornography were paper, there would be no fairness-based jurisdictional objection to a German prohibition on the pornography's entry at the border or to German punishment of those who are later discovered to have smuggled it in.[170] From Germany's perspective, it makes no difference whether the pornography enters the nation via cyberspace or the postal service. The rationale for the regulation is the same in both cases: something is happening within Germany that implicates the government's paternalistic concerns or that harms third parties within its borders. The fact that the local regulation might affect the cost or availability of pornography in other coun-

---

[168] In late 1996, CompuServe had 335,000 German subscribers and employed over 250 workers there. *Compuserve May Curb German Operations*, NY Times D6 (Nov 19, 1996).

[169] See Section III.D.

[170] There might of course be substantive objections akin to the First Amendment found either in German law or in international human rights law. As I mentioned at the outset, such substantive limitations on cyberspace regulation are not my concern here.

tries is, from this perspective, irrelevant. Fairness does not require Germany to yield local control over its territory in order to accommodate the users of a new communication technology in other countries. Nor does it require Germany to absorb the local costs of foreign activity because of the costs that the German regulation might impose on such activity.

This latter point sheds light on one of the major fallacies of the skeptics' normative project. The skeptics argue that the spillover effects caused by territorial regulation of cyberspace justify cyberspace self-regulation. Spillover-minimization is not the criterion of legitimacy for national regulation of harmful local effects.[171] But even if it were, the skeptics' conclusions would not follow. For the skeptics completely ignore the spillover effects of cyberspace activity itself. They do not consider these effects because they take it as an article of faith that cyberspace participants form a self-contained group that can internalize the costs of its activity.[172] But this assumption is false. Cyberspace participants are no more self-contained than telephone users, members of the Catholic Church, corporations, and other private groups with activities that transcend jurisdictional borders. They are real people in real space transacting in a fashion that produces real-world effects on cyberspace participants and nonparticipants alike. Cyberspace users solicit and deliver kiddie porn, launder money, sexually harass, defraud, and so on. It is these and many other real-space costs—costs that cyberspace communities cannot effectively internalize—that national regulatory regimes worry about and aim to regulate.

So the spillover argument runs in both directions. Cyberspace activity outside of Germany produces spillovers in Germany, and German regulation produces spillovers on cyberspace activity beyond its borders. The legitimacy and fairness of Germany's territorial regulation does not depend on minimization of these costs. But even if it did, the skeptics' desired normative conclusion that cyberspace should be self-regulated would only follow if the costs of cyberspace self-regulation were less significant than the costs of territorial regulation. The skeptics have not begun to try to demonstrate that this is true. And any such attempt is very unlikely to succeed at the level of generality at which their arguments are invariably pitched.

---

[171] See discussion in Section II.

[172] See Johnson and Post, 48 Stan L Rev at 1378-91 (cited in note 3).

C. Notice

The skeptics' final normative argument against mandatory law regulation of cyberspace concerns notice. In real space, parties can direct the flow of their transnational transactions and can in most cases avoid jurisdictions that prohibit the transactions. The skeptics claim that this cannot be done in cyberspace. They worry that cyberspace participants therefore lack notice about governing mandatory law and hence cannot conform their behavior to it. The skeptics claim this lack of notice violates basic norms of fairness.

This argument rests on a number of empirical assumptions that have been questioned in Section III. The assumption that cyberspace involves uncontrollable universal information flows is inaccurate today and will become even less accurate with time. Information flows can be directed and controlled in a variety of ways, with varying costs that will almost certainly decrease in the future.[173] Concerns about notice are further attenuated by the many limitations on enforcement jurisdiction that effectively limit the application of mandatory laws to entities with a local presence.[174] In none of the many cases in which regulations have been enforced against cyberspace transactions has an out-of-state defendant had a basis to claim unfair surprise.

It is nonetheless worth considering how the notice issue will play out in cyberspace. The Constitution and international law impose weak notice requirements on the application of local law to extraterritorial conduct. The Constitution permits a state with significant contacts to the case to apply its law if the defendant could have reasonably foreseen its application.[175] International law might impose a similar restraint on legislative jurisdiction.

This requirement of reasonable foreseeability does not mean that harmful local effects of extraterritorial activity are automatically immune from local regulation just because they were accidental, or because the agent of the activity did not know the precise locus of the effects. "Reasonable foreseeability" is a dy-

---

[173] See Section III.D.

[174] See Section III.B.

[175] I glean this formulation from *Phillips Petroleum Co v Shutts*, 472 US 797, 807 (1985); *Allstate Insurance Co v Hague*, 449 US 302, 312-13 (1981) (plurality opinion); *Clay v Sun Insurance Office, Ltd*, 377 US 179, 182 (1964); *Watson v Employers Liability Assurance Corp*, 348 US 66, 72-73 (1954); and *Home Insurance Co v Dick*, 281 US 397, 410 (1930). Like all formulations of constitutional limitations on choice of law, this one is open to debate because the Court's analysis in these decisions is maddeningly vague, and because the Court has mixed due process and full faith and credit concerns. See note 34 and accompanying text. But at the very least, the formulation in the text is close enough to the constitutional requirement of notice to consider the application of this test to cyberspace.

namic concept. A manufacturer that pollutes in one state is not immune from the antipollution laws of other states where the pollution causes harm just because it cannot predict which way the wind blows. Similarly, a cyberspace content provider cannot necessarily claim ignorance about the geographical flow of information as a defense to the application of the law of the place where the information appears. At first glance it appears unfair to expose Digitalbook.com to the antipornography laws of Singapore. But it would not seem unfair if Digitalbook.com could at a small cost prevent its information from entering Singapore. Nor would it seem unfair to expose Digitalbook.com to liability for the damage caused in Singapore by a virus that it released into cyberspace that destroyed every Apple computer hard drive connected to the Internet.

These intuitions show that, like the related personal jurisdiction question,[176] the standard of foreseeability depends on a complex mixture of what the content provider knows or reasonably should have known about the geographical consequences of its acts, the significance of the extrajursidictional harms caused by the acts, and the costs of precautions.[177] Content providers can already achieve pretty reliable information flow control by conditioning access to content on telephone or facsimile proof of geographical location. To many this is an unacceptable burden on Internet communication. But there is nothing sacrosanct about Internet speed and ease, and dimunitions in speed and ease might be warranted by the social costs imposed by uncontrolled information flows. And in any event, as filtering and identification technologies continue to raise the feasibility and lower the costs of information flow control, the problem of notice in cyberspace will look much like the problem of notice in real space.

V. GROUNDING CYBERSPACE IN REAL-SPACE LAW

I have argued that national and international regulations of cyberspace transactions are legitimate and feasible. I have not argued for any particular regulation, or that such regulation should be pervasive. I have tried to show only that the skeptics' global arguments against national and international regulation of cyberspace are unfounded. Cyberspace self-regulation will often

---

[176] See text accompanying notes 78-85.

[177] What is foreseeable will also be informed, in a circular fashion, by what the law requires. If the law permits one jurisdiction to hold a content provider in another jurisdiction strictly liable for the mere act of placing information on a web page, then this result is foreseeable. The pertinent question is what level of foreseeability the law *should* require, and this analysis is informed by the factors listed in the text.

be difficult to achieve. And like non-cyberspace transactions, cyberspace transactions will in any event be limited by national mandatory rules.

The challenging issue from a jurisdictional perspective is to develop a legal structure that both facilitates private legal ordering of cyberspace transactions and accommodates national mandatory law limitations. Consider the predicament of a person in England who wants to buy a security from a web page on a server in Japan. The parties want the sale to circumvent U.S. securities regulations, and, more broadly, the interference of national courts. The parties thus agree that the sale will be governed by Japanese law and that any disputes will be resolved by private arbitration in Japan. Will this contract be enforceable? This example involves a commercial transaction. But the problem is generic, for, as we saw above, parties can by contract create governing legal structures for a variety of non-commercial activities. Thus, for example, the same basic problem arises when chat room participants from different countries agree that the tort law principles of the state of Illinois govern chat room activities, and that all disputes will be resolved privately. Will the parties' *ex ante* consent be respected when a chat room participant from France claims in his national court that he suffered a tort in the chat room in violation of French law?

To avoid national court litigation and minimize national regulation, the parties to these transactions need to satisfy the following conditions. They must consent *ex ante* to a governing law, a private method of dispute resolution, and a private enforcement regime. The consent must be consistent with the mandatory law applied by any national court where a defector from the contract might seek to have any part of the contract declared invalid.[178] To ensure the sanctity of the private order and to dis-

---

[178] There are of course some private legal orders that are relatively immune from this requirement, either because the costs of defecting from the private order are greater than the costs of continued participation, see Lisa Bernstein, *Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J Legal Stud 115 (1992); Posner, 63 U Chi L Rev at 165-97 (cited in note 69), or, relatedly, because the members of the order structure their affairs to circumvent mandatory laws. See Frank H. Easterbrook and Daniel R. Fischel, *The Economic Structure of Corporate Law* 3 (Harvard 1991) (corporate context). Even these prominent examples of mandatory law circumvention, however, are not clear-cut. For example, Bernstein's paradigmatic examples of private legal orders are sometimes subject to mandatory law interventions. See Bernstein, 21 J Legal Stud at 125 & n 24, 129 & n 35 (noting that arbitration awards can be vacated for procedural irregularity and that the group's actions must conform with antitrust regulations). Similarly, a corporation's ability to circumvent mandatory law restrictions is dependent in large part on the settled but by no means inevitable choice-of-law rule that the law of the place of incorporation governs internal corporate affairs. Mandatory corporate laws would

courage such defection, the national court must be willing to (i) treat the consent to the private order as valid, (ii) enjoin litigation in derogation of the contract, and, sometimes, (iii) specifically enforce the defector's agreement to abide by the private order. Moreover, it is not enough that the courts of a single country will enforce the contract. There must be coordinated enforcement among national courts in every country in which the recalcitrant party might go to seek to avoid the obligation. Finally, national courts must subsequently recognize the validity of the private dispute resolution process. They must enjoin subsequent litigation in derogation of the results of the private dispute resolution, and enforce any judgments that cannot be done so privately.

Such a structure might appear hopelessly complicated and thus fanciful. But this appearance is deceiving. The essentials for such a regime already exist in the system that governs international commercial arbitration.[179] This system works through the interplay of three layers of law. The first layer is the private law of the parties' contract. In the contract, the parties specify the law governing the transaction (in the examples above, the laws of Japan and Illinois), agree to use private arbitration to resolve certain disputes that arise out of or relate to the transaction, and choose the place for the arbitration and the procedures that govern it.[180] The second layer is the national arbitration law.[181] A national arbitration law defines the scope of permissible arbitration within the country, renders arbitration agreements within this scope valid, and provides various forms of judicial assistance for, and judicial review of, arbitration. Most nations have generally similar national arbitration laws that ensure harmonization of enforcement across jurisdictions. This harmonization is substantially bolstered by the third layer of legal regulation: the interna-

---

be harder to avoid if nations and states instead applied local corporate law on the basis of the local effects of corporate transactions. See, for example, *Western Airlines, Inc v Sobieski*, 191 Cal App 2d 399, 12 Cal Rptr 719, 727-29 (1961) (applying California cumulative voting rule to Delaware corporation doing significant business in California). Because for a variety of reasons it frequently will be difficult for cyberspace communities to completely circumvent mandatory law restrictions, I will set aside this possibility in the analysis.

[179] Two excellent introductions to international commercial arbitration are Gary B. Born, *International Commercial Arbitration in the United States: Commentary and Materials* (Kluwer 1994), and Alan Redfern and Martin Hunter, *Law and Practice of International Commercial Arbitration* (Sweet & Maxwell 2d ed 1991).

[180] The most prominent international arbitration rules are those promulgated by the International Chamber of Commerce, the American Arbitration Association, the London Court of International Arbitration, and the UNCITRAL. These rules are generally similar but contain important differences. See Born, *International Commercial Arbitration* at 10-16, 50-96 (cited in note 179).

[181] In the United States, this law is the Federal Arbitration Act, Pub L No 282, 61 Stat 669 (1947), codified at 9 USC §§ 1 et seq (1994).

tional enforcement treaty. By far the most important such treaty is the New York Convention on the Recognition and Enforcement of Arbitral Awards, which almost every nation has signed.[182] The Convention obligates the national courts of signatory states to recognize and enforce arbitration agreements and awards, subject to limited exceptions.[183]

The basic structure of international commercial arbitration could easily be modified to cyberspace. As explained above, the law of the contract—both the substantive law and the dispute resolution mechanism—could be agreed to as an incident of the securities transaction or as a condition of access to the chat room.[184] National arbitration laws could be modified to include dispute resolution in cyberspace. For example, the Federal Arbitration Act ("FAA") would require modification in only two important respects. First, the FAA's requirement that the arbitration agreement be made in writing might need to be amended to accommodate cyberspace realities.[185] Second, FAA rules that turn on the place of the arbitration[186] require modification for virtual arbitrations that lack a geographical locus.[187] The New York Convention would likely require similar amendment.

---

[182] The Convention is reproduced at 9 USC § 201 (1994). For general commentary, see Born, *International Commercial Arbitration* at 18-20 (cited in note 179); A. Jan van den Berg, *The New York Arbitration Convention of 1958: Towards a Uniform Judicial Interpretation* (Kluwer 1981).

[183] The exceptions, which are narrowly construed, can be grouped in four categories. First, the Convention has certain jurisdiction prerequisites. For example, it does not apply to oral arbitration agreements, to domestic arbitrations, or to noncommercial arbitrations. New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, Arts I, II, June 10, 1958, 330 UNTS 38. Second, the obligation to enforce arbitration agreements and awards does not extend to matters that, under national law, are nonarbitrable or violate a strong public policy. Id at Arts II(1), V(2). I discuss this exception further below. See note 188. Third, the duty to enforce arbitral awards does not extend to awards rendered without minimal due process protections (such as notice). Id at Art V(1)(b). And fourth, the duty to enforce arbitral awards does not extend to ultra vires awards. Id at Art V(1)(c).

[184] See Section III.A.

[185] It is possible, however, that an agreement in cyberspace constitutes an agreement in writing. For an overview of various responses to this problem, see Michael E. Schneider and Christopher Kuner, *Dispute Resolution in International Electronic Commerce*, 14 J Intl Arb 5, 13-15 (1997); Jasna Arsic, *International Commercial Arbitration on the Internet: Has the Future Come Too Early?*, 14 J Intl Arb 209, 215-17 (1997).

[186] See, for example, 9 USC § 4 (1994) (authorizing federal court to order arbitration "within the district in which the petition for an order directing such arbitration is filed"); 9 USC § 10(b) (1994) (providing for limited judicial review by "[t]he United States district court for the district wherein an award was made").

[187] Under the current international arbitration legal regime, national arbitration laws govern many issues of judicial assistance other than enforcement of the agreement and award. These issues include, for example, certain aspects of discovery, the selection of arbitrators when the parties have not done so, and provisional relief. National court jurisdiction over these issues is almost always determined by the fact that the arbitration takes

The accommodation of mandatory laws presents special challenges. In the securities example, assume that the English purchaser is unhappy with the security, and defects from the contractual agreement to arbitrate by bringing a private securities action in a U.S. court that alleges that the sale was fraudulent and in violation of U.S. securities law. This raises two basic mandatory law issues. The first is whether the U.S. court will enforce the agreement to arbitrate, or will instead adjudicate the mandatory law (and perhaps other) claims. Assuming the court enforces the arbitration agreement, the second question is whether the arbitrator can apply the U.S. mandatory law consistent with the jurisdictional limits imposed by the parties' contractual choice of Japanese law.

Both difficulties frequently arise with respect to non-cyberspace transnational transactions, and can be addressed within the framework of international commercial arbitration. As for the first problem, national courts increasingly permit private arbitrators to resolve claims involving economic regulation and quasi-criminal laws subject to subsequent, deferential judicial review.[188] The deferential nature of such review, combined with the costs of seeking it, mean that private arbitrators will often have the final say. As for the second problem, arbitrators have established a number of devices grounded in (often fictional) party con-

---

place within the jurisdiction. Because the locus of an arbitration in cyberspace is difficult to identify, many jurisdictions might assert the power of judicial review and assistance. One answer to this problem is coordination of the judicial assistance function. Such enforceable coordination could be accomplished most effectively by international treaty. Indeed, the New York Convention's judicial enforcement provisions could be modified to cover judicial assistance. Another (less effective) possibility is to make national arbitration laws uniform, so that it doesn't matter which court provides judicial assistance. This is the basic strategy of the UNCITRAL model arbitration law. See generally Born, *International Commercial Arbitration* at 37-38 (cited in note 179). For an overview of other solutions to these difficulties, see Arsíc, 14 J Intl Arb at 217-20 (cited in note 185).

[188] The Supreme Court, for example, has ruled that antitrust, RICO, and securities claims are arbitrable. *Shearson/American Express, Inc v McMahon*, 482 US 220, 242 (1987) (holding RICO claims to be arbitrable); *Mitsubishi Motors Corp v Soler Chrysler-Plymouth, Inc*, 473 US 614, 632-40 (1985) (holding Sherman Act claims to be arbitrable); *Scherk v Alberto-Culver Co*, 417 US 506, 518-20 (1974) (holding claims under the Securities and Exchange Act of 1934 to be arbitrable). See generally Born, *International Commercial Arbitration* at 322-66 (cited in note 179). These decisions are not required by the New York Convention. To the contrary, The New York Convention and national arbitration laws permit an exception to national courts' obligation to enforce arbitration agreements and awards when the arbitration involves a nonarbitrable subject. See New York Convention, Arts II(1), V(2) (cited in note 183). But this exception has been construed in an increasingly narrow fashion, as nations increasingly delegate the task of enforcing mandatory laws to private arbitrators.

sent that permit them to apply a mandatory law of a country other than the one specifically chosen by the parties' contract.[189]

To many it will seem ironic and damning that my description of a legal regime that supposedly promotes private ordering focuses so much on the role of national courts and national laws. This focus is misleading. Much of the regulation of these private matters is and will continue to be governed by a variety of privately enforceable rules, norms, and enforcement mechanisms. Yet the overarching national and international legal regimes remain necessary for two reasons. First, they provide a ready-made coordination and enforcement regime that transnational parties can invoke in the many situations in which information-gathering and related costs of purely private enforcement are prohibitively high. Second, they give private parties enormous flexibility in creating a private regime in a fashion that can accommodate and minimize the intrusion of oft-conflicting mandatory laws. In this connection, it should be emphasized that the international commercial arbitration model is not as litigious, and would not be as intrusive on private cyberspace orders, as it might at first glance appear. If real-space commercial arbitrations are any guide, recourse to national courts will be relatively infrequent as the background public enforcement patterns become relatively clear.

I do not mean to suggest that international commercial arbitration is a comprehensive panacea for the jurisdictional challenges of cyberspace. It is not. Many, probably most, cyberspace transactions will have such a low value that affected parties will not bother to enter into contractual relations, much less contract for governing law and private enforcement. In addition, cyberspace transactions that adversely affect third parties are beyond the ken of international commercial arbitration, which depends upon *ex ante* consent for its effectiveness and legitimacy. Relatedly, although the international arbitration regime has taken steps to privatize the enforcement of mandatory laws, many mandatory laws—most prominently traditional criminal laws and certain limits on contractual capacity—are not subject to enforceable international arbitration. Indeed, some might object that cyberspace-related choice-of-law and private arbitration agreements that are not dickered should be viewed as unenforceable contracts of adhesion.[190]

---

[189] See Born, *International Commercial Arbitration* at 147-52 (cited in note 179).

[190] I have tried to avoid analysis of the merits of particular regulatory regimes in this article, but it is perhaps worth noting that this adhesion contracts concern has relatively little force in the cyberspace context, where users have an array of options for the large majority of functions and services.

These limitations on the international commercial law regime are not, of course, unique to cyberspace transactions. These same limitations characterize real-space transnational transactions. Such limitations are inevitable when it is difficult for parties to transnational transactions to craft private legal regimes *ex ante*, or when these transactions harm third parties or implicate the paternalistic interests of affected nations. The important point is that these limitations are difficult to overcome in "real space" and cyberspace alike. My modest aim has been to show that the governing law challenges presented by cyberspace are not significantly different from the ones presented by other transnational transactions.

CONCLUSION

Cyberspace transactions are no different from "real-space" transnational transactions. They involve people in real space in one jurisdiction communicating with people in real space in other jurisdictions in a way that often does good but sometimes causes harm. There is no general normative argument that supports the immunization of cyberspace activities from territorial regulation. And there is every reason to believe that nations can exercise territorial authority to achieve significant regulatory control over cyberspace transactions. Resolution of the choice-of-law problems presented by cyberspace transactions will be challenging, but no more challenging than similar problems raised in other transnational contexts.