1999

Against Cyberanarchy

Jack L. Goldsmith

OCCASIONAL PAPERS FROM
THE LAW SCHOOL
THE UNIVERSITY OF CHICAGO

NUMBER 40

AGAINST CYBERANARCHY

BY JACK L. GOLDSMITH

THE LAW SCHOOL
THE UNIVERSITY
OF CHICAGO

AGAINST CYBERANARCHY

Jack L. Goldsmith*

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

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."

---

*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. A different version of this paper was originally published as Volume 65, No. 4 of *The University of Chicago Law Review*.

[1] 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.

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 implicated 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. 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 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.

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. They make and breach contracts. They distribute pornography and swap bombmaking tips. They infringe trademarks, violate copyrights, and steal data. They issue fraudulent securities and restrict competition. 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. 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 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. In addition, information mediated by certain cyberspace services appears "simultaneously and equally in all jursidictions" around the world. 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. One reason is that information transmitted via cyberspace can easily flow across national borders without detection. Another reason is that it is senseless to apply geographically configured choice-of-law rules to a-geographical cyberspace activities. A third reason is that regulation of the local effects of cyberspace information flows permits all nations simultaneously to regulate all web-based transactions. The result is multiple and inconsistent regulation of the same activity. A final reason is that the architecture of cyberspace enables its users to route around or otherwise evade territorial regulation.

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. 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. 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. 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, 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 obliga-

tions. 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. This conception was repudiated in the middle of this century. The skeptics' first mistake, therefore, is to measure the feasibility and legitimacy of national regulation of cyberspace against a repudiated yardstick. This Section 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. 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.

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. They also argued that a forum's decision to apply foreign law was always determined by local domestic policies. 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 nations. But positivism's insistence on a sovereign source for every rule of decision undermined judicial reliance on these laws. 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. As different jurisdictions adopted different choice-of-law regimes, the goal of a single governing law for transjurisdictional transactions was further frustrated.

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." In practice, this standard is notoriously easy to satisfy. 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

settled 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. In addition, both the Constitution and international law permit a nation or state to regulate the extraterritorial conduct of a citizen or domiciliary. 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. 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.

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 succes-

sion 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. 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. They can also specify the governing law for matters ranging from intellectual property to trusts and estates to internal corporate affairs.

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. Mandatory laws range from limits on contractual 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. They can, in theory, be resolved by public contract—international agreements that embrace uniform international rules or uniform choice-of-law rules. 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.

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. 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. But regardless of which substantive law the forum applies, the application of that law will frequently create spillover effects on activities in other coun-

tries 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.

Consider, for example, the Supreme Court's decision in Hartford Fire Insurance Co v California. 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. 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. Minnesota applied its pro-plaintiff stacking rules for automobile insurance coverage to an accident in Wisconsin among Wisconsin residents. 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. 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. New York applied its tort law to a car accident in Canada. California taxed a British corporation based on the California portion of its world profits.

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. International harmonization efforts seek to achieve similar aims, often at the expense of national prerogatives.

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 underappreciation 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. 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. 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 enforced 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." 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. Or the governing law could be the contractual terms themselves. 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." 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. 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.

Many have proposed a structure for private legal ordering of cyberspace along the lines just sketched. 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. 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. 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 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. 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.

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. But the effective scope of a nation's law depends on the nation's abili-

ty 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.

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. 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. 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.

Application of this standard to cyberspace activities presents special difficulties. Under standard assumptions about cyberspace 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. 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. 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 multi-jurisdictional 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. 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. As such control becomes more feasible and less costly, personal jurisdiction over cyberspace activities will become 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. However, also in contrast to domestic law, there is no full faith and credit obligation to enforce foreign judgments in the international sphere. If one country exercises personal jurisdiction on an exorbitant basis, the resulting judgment is unlikely to be enforced in another

country. 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. For these reasons, there is little concern that a foreign default judgment 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. 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. A different, but equally forceful, limitation applies to international extradition. International extradition is governed largely by treaty. 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. 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 less

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

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. 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. 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. 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. For example, they can relocate in geographical space, or employ telnet or anonymous remailers to make the geographical source of their content difficult to discern. 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. 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. 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. They also regulate the local means through which foreign content is transmitted. For example, they impose screening obligations on in-state Internet service providers and other entities that supply or transmit information. Or they regulate in-state hardware and software through which such transmissions are received. Or they regulate the local financial intermediaries that make commercial transactions on the Internet possible.

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. The question is always whether the regulation will heighten the costs of the activity sufficiently to achieve its acceptable control from whatever normative perspective is 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. 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. 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. 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 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. 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. 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. 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.

The subsequent events of the CompuServe controversy, like the response to the Supreme Court's invalidation of the Communications Decency Act in Reno, 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. Cyberspace information can only appear 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. 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 geographi-

cal locations not to view or enter, and disclaim legal liability if they do. Others condition access on proof of age or on membership in one of dozens of private age-verification services. Others require potential end-users to send by fax or telephone information specifying age and geographical location. 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. 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. 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. A government can choose to have no Internet links whatsoever and to regulate telephone and other communication lines to access providers in other countries. 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. 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. The Federal Communications Commission recently required V-chip blocking technology to be placed in computers capable of receiving video broadcasting, and pending anti-spam legislation would impose identification requirements on commercial e-mail senders and filtering requirements on Internet service providers. There are numerous other possibilities.

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. This is one reason why information filtering is an essential component of all communications media. 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 invention of identification and filtering technologies that made it possible to organize and select from the morass of available information.

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 —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." Many jurisdictions have already mandated the use of filtering and identification mechanisms. 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. They argue that content filters invariably both over- and underfilter; 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. 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. Although the ultimate accuracy of cyberspace filtering 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. 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. 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 regula-

tion. These techniques will not resolve all conflict of laws in cyberspace 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. 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. These harmonization efforts grow out of an international copyright regime that is over one hundred years old. 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. 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. Several international organizations have drafted model laws and guidelines to facilitate Internet commerce and related digital certification issues. There are scores of other international efforts in a variety of cyberspace-related contexts.

International harmonization is not always (or even usually) the best response to the spillovers and evasions that result from unilateral regulation. 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. 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. In this light, the enormous increases in the pervasiveness and complexity of conflict of laws in this century can be viewed as 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?" 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?

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.

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

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 built the server and the country of the server whose hyperlink pointed to the server that contained the infringing material. The limits on enforcement jurisdiction may further minimize the scope of the conflict. 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. 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.

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. 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 administered 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. 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 choice-of-law methods that alleviate these problems. A unilateral method considers only whether the dispute at issue has close enough connections to the forum to

justify the application of local law. 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.

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. 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.

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, individuals 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. Internet gambling makes it significantly easi-

er 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.

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 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. In the CompuServe example, Germany regulated transmission flows from other countries. 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.

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 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. 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 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. Without this presence, German enforce-

ment 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. 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. 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 countries 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. 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. 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.

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 uncon-

trollable 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. 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. 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. 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 dynamic 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, 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. 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.

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.

OCCASIONAL PAPERS FROM
THE LAW SCHOOL
THE UNIVERSITY OF CHICAGO
1111 EAST 60TH STREET
CHICAGO, ILLINOIS 60637

No.1. "A Comment on Separation of Power"
Philip B. Kurland, November 1, 1971.

No. 2. "The Shortage of Natural Gas"
Edmund W. Kitch, February 1, 1972.

No. 3. "The Prosaic Sources of Prison Violence"
Hans W. Mattick, March 15, 1972.

No. 4. "Conflicts of Interest in Corporate Law Practice"
Stanley A. Kaplan, January 10, 1973.

No. 5. "Six Man Juries, Majority Verdicts—What Difference Do They Make?"
Hans Zeisel, March 15, 1973.

No. 6. "On Emergency Powers of the President: Every Inch a King?"
Gerhard Casper, May 31, 1973.

No. 7. "The Anatomy of Justice in Taxation"
Walter J. Blum and Harry Kalven Jr., October 1, 1973.

No. 8. "An Approach to Law"
Edward H. Levi, October 15, 1974.

No. 9. "The New Consumerism and the Law School"
Walter J. Blum, February 15, 1975.

No. 10. "Congress and the Courts"
Carl McGowan, April 17, 1975.

No. 11. "The Uneasy Case for Progressive Taxation in 1976"
Walter J. Blum, November 19, 1976.

No. 12. "Making the Punishment Fit the Crime: A Consumers' Guide to Sentencing Reform"
Franklin E. Zimring, January 24, 1977.

No. 13. "Talk to Entering Students"
James B. White, August 15, 1977.

No. 14. "The Death Penalty and the Insanity Defense"
Hans Zeisel, April 15, 1978.

No. 15. "Group Defamation"
Geoffrey R. Stone, August 10, 1978.

No. 16. "The University Law School and Practical Education"
Carl McGowan, December 20, 1978.

No. 17. "The Sovereignty of the Courts"
Edward H. Levi, July 15, 1981.

No. 18. "The Brothel Boy"
Norval Morris, March 15, 1982.

No. 19. "The Economists and the Problem of Monopoly"
George J. Stigler, July 1, 1983.

No. 20. "The Future of Gold"
Kenneth W. Dam, July 15, 1984.

No. 21. "The Limits of Antitrust"
Frank H. Easterbrook, April 15, 1985.

No. 22 "Constitutionalism"
Gerhard Casper, April 6, 1987.

No. 23. "Reconsidering Miranda"
Stephen J. Schulhofer, December 15, 1987.

No. 24. "Blackmail"
Ronald H. Coase, November 14, 1988.

No. 25. "The Twentieth-Century Revolution in Family Wealth Transmission"
John H. Langbein, December 8, 1989.

No. 26. "The State of the Modern Presidency: Can It Meet Our Expectations?"
Stuart E. Eizenstat, March 10, 1990.

No. 27. "Flag Burning and the Constitution"
Geoffrey R. Stone, May 1, 1990.

No. 28. "The Institutional Structure of Production"
Ronald H. Coase, May 15 , 1992.

No. 29. "The Bill of Rights: A Century of Progress"
John Paul Stevens, December 1, 1992.

No. 30. "Remembering 'TM'"
Elena Kagan and Cass R. Sunstein, June 8, 1993.

No. 31. "Organ Transplantation: Or, Altruism Run Amuck"
Richard A. Epstein, December 1, 1993.

No. 32. "The Constitution in Congress: The First Congress, 1789-1791"
David P. Currie, June 15, 1994.

No. 33. "Law, Diplomacy, and Force: North Korea and the Bomb"
Kenneth W. Dam, December 15, 1994.

No. 34. "Remembering Nuremberg"
Bernard D. Meltzer, December 20, 1995.

No. 35. "Racial Quotas and the Jury"
Albert W. Alschuler, February 20, 1996.

No. 36. "The Restructuring of Corporate America"
Daniel R. Fischel, June 20, 1996.

No. 37. "Constitutional Myth-Making: Lessons from the *Dred Scott* Case"
Cass R. Sunstein, August 26, 1996.

No. 38. "The Role of Private Groups in Public Policy: Cryptography and the National Research Council"
Kenneth W. Dam, January 15, 1997.

No. 39. "Impeachment and Presidential Immunity from Judicial Process"
Joseph Isenbergh, November 11, 1998

No. 40. "Against Cyberanarchy"
Jack L. Goldsmith, August 13, 1999

Copies of *Occasional Papers* from the Law School are available from William S. Hein & Company, Inc., 1285 Main Street, Buffalo, New York 14209, to whom inquiries should be addressed. Current numbers are also available on subscription from William S. Hein & Company, Inc.