Unilateral Regulation of the Internet: A Modest Defence

Jack Goldsmith*

Abstract

This article analyses the conflicts-of-law problems that supposedly arise from the fact that every nation can unilaterally regulate every Internet transaction. It argues that the threat of multiple national regulation of Internet transactions is significantly exaggerated. It then examines a more serious problem: the spillover effects from unilateral national regulation. These spillovers do not affect the legitimacy of unilateral regulation, but they might argue for public and private harmonization strategies to eliminate the spillovers. Unfortunately, the prospects for such harmonization are generally dim in many contexts. This means that unilateral national regulation will continue to be a primary vehicle of Internet regulation — a prospect that is not nearly as destructive of the Internet's future as conventional wisdom suggests.

First-generation Internet scholarship maintained that the Internet undermined the feasibility of unilateral national or regional regulation.[1] As the ubiquitous complaints about unilateral Internet regulation suggest, this view has been overrun by events.[2] Today the problem seems not to be the impossibility of unilateral regulation. The problem seems to be the opposite one of too much unilateral regulation by too many nations. It turns out that nations can do lots of things within their territories to affect the cost of, and thereby regulate, transnational Internet communications. And since Internet communications can appear simultaneously in (and thus do harm in) many nations, many nations might assert unilateral regulatory control over Internet transactions. The result is thought to be a conflicts-of-law nightmare, with potentially every nation regulating potentially every Internet transaction.

This article tries to put this purported conflicts nightmare into proper perspective. The discussion proceeds in four parts. The first part explains how unilateral regulation

* Professor of Law, University of Chicago. This essay draws and builds upon my earlier work on Internet regulation, especially 'Against Cyberanarchy', 65 *Chicago Law Review* (1998) 1199 and 'Regulation of the Internet: Three Persistent Fallacies', 73 *Chic. Kent. L. Rev.* (1999) 1119.

1 See Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors', 66 *University of Cincinatti Law Review* (1997) 177, at 178. The best-known statement of this view in the United States is by David Post and David Johnson. See Johnson and Post, 'Law And Borders — The Rise of Law in Cyberspace', 48 *Stanford Law Review* (1996) 1367.

2 Think, for example, about the complaints over the European Data Protection Directive or US Export Controls on Encryption. Such complaints would be unnecessary if national and regional regulation of the Internet were infeasible.

EJIL (2000), Vol. 11 No. 1, 135–148

of Internet transactions can be both effective and (from the perspective of jurisdiction) legitimate. The second explains why threats of simultaneous multiple national regulation of Internet transactions are significantly exaggerated. The third section addresses a more serious problem: the spillover effects from unilateral national regulation. It explains that these spillovers do not affect the legitimacy of unilateral regulation, but they might argue for public and private harmonization strategies to eliminate the spillovers. The fourth part suggests that the prospects for such harmonization are in many circumstances dim. Unilateral national regulation will continue to be a primary vehicle of Internet regulation, but this fact is not as bad for the success of the Internet as some suggest.

1 The Efficacy and Legitimacy of Unilateral Regulation

A *Efficacy*

First generation Internet thinkers believed that unilateral regulation of Internet communications would be ineffective. They reasoned as follows. The Internet makes it possible for a content provider with a computer in one country to communicate instantaneously and simultaneously with computer users in multiple countries.[3] A territorial government cannot regulate offshore content producers beyond the nation's physical control. Nor can it regulate the flow of digital information packets across its borders. And even if a nation tried to do so, Internet users can route around or otherwise evade such regulation by using re-mailers, mirror sites, and the like. For these reasons, many commentators thought the Internet defied unilateral territorial regulation.

These beliefs turned out to be wrong. They were wrong because they overlooked the abiding significance of territorial sovereignty. A nation can take many steps within its territory to regulate content transmitted from abroad indirectly. It need not inspect every item crossing its borders to regulate effectively the flow of items within its borders. Instead, it can achieve a great deal of regulatory control over illegal imports by imposing costs on persons and property within its territory. In short, a nation has many territorial weapons with which to fight offshore Internet transactions.

Consider how nations have regulated other forms of offshore communication that produce local harms. For example, unwanted radio and television content can be broadcast from one nation into another. The content source is beyond the territorial government's reach, and broadcast signals are difficult to stop at the border. The nation can still control the unwanted content within its borders. It can go after the offshore content provider's local assets. And if there are none, it can punish local consumers of the content, regulate local transmission facilitators, or regulate the

[3] Here and through this essay, I use the term 'content provider' as a generic term to refer to all persons transmitting information on the Internet, including e-commerce buyers and sellers, porn purveyors and consumers, chat room participants, web page operators, and the like.

technical design of local reception devices.[4] These local regulations make the foreign content harder to obtain within the territory, thereby regulating it even though its source is abroad and the broadcast signals cannot be stopped at the border.

Consider the analogous problem of grey-market goods. A grey-market good is one sold lawfully in state *A* but imported into state *B* without the consent of the owner in *B* of the intellectual property rights associated with the good. Grey-market goods are, like Internet information packets, offshore products that are illegal within the regulating country but very hard to intercept at the border. But the officials in state *B* can still effectuate *B*'s intellectual property laws by regulating domestic users and distributors of the grey-market goods. For example, *B* might authorize valid trademark or copyright holders to sue grey-market distributors and users.[5] This regulation of the local demand side of the grey-market goods raises their domestic cost, making them less attractive to import and thereby regulating the foreign provider of the good. Once again, purely local regulation achieves extraterritorial regulatory effect.

Territorial regulation with indirect extraterritorial regulatory effect is how nations regulate the Internet. One way to control Internet information flows is to punish the foreign content provider's local assets or agents.[6] Often, however, the foreign content provider will not have a local presence.[7] But the regulating territorial jurisdiction still has many options. It can penalize in-state end-users who obtain or use illegal foreign content. It can regulate the in-state hardware and software through which Internet transmissions are received.[8] In addition, a nation can regulate Internet access providers and other local firms that facilitate local consumption of Internet transmissions.[9] Finally, a nation can regulate local financial intermediaries — banks, credit card companies, and the like — that facilitate Internet transactions.[10] In these and many other ways, territorial governments make the domestic side of Internet transactions more expensive, thereby indirectly regulating the extraterritorial source

[4] All three strategies have been employed by nations seeking to interrupt cross-border propaganda transmissions. See Krasner, 'Global Communications and National Power: Life on the Pareto Frontier', 43 *World. Pol.* (1991) 336, at 344–349.

[5] See, e.g. *Parfums Givenchy, Inc. v. Drug Emporium, Inc.*, 38 F.2d 477, 481 (9th Cir. 1994).

[6] This is what happened in a recent Internet gambling case, *New York v. Vacco*, No. 404428/98, Supreme Court, 22 July 1999, discussed below.

[7] Note that this is typically the case of small companies with a single-jurisdictional presence; larger firms with a multi-jurisdictional presence thus face a greater threat of multiple regulatory exposure.

[8] For example, some countries have set up proxy servers and software blockades, the FCC recently mandated v-chip blocking technology in computers that receive video broadcasting, and some have proposed mandatory rating and screening technology for web browsers.

[9] This is the strategy of proposed US federal gambling legislation, which would authorize the United States to order Internet service providers to shut down illegal gambling sites.

[10] For example, the FTC has gone after offshore Internet fraud schemes by seizing control of the US financial intermediaries through which the offshore entities were paid. Similarly, an Internet gambling player in the United States recently sued a local credit card company to recover money lost on Internet gambling with an offshore company. See Beer, 'The Wagers of the Web: Lawsuit Could Unravel On-line Gaming Industry', *San Francisco Examiner*, 17 August 1998, at B1.

of the offending content. Sceptics about Internet regulation will respond that these strategies will not *eliminate* offending Internet content from abroad. Not only can hackers and clever Internet users circumvent territorial regulations, but individual Internet users are hard to identify, isolate, and sanction.

These points are true, but their relevance is overstated. Regulation is rarely if ever perfect in the sense of eliminating all individual violations. And it need not eliminate all violations to be effective. Governments regulate an activity by raising the activity's costs in a manner that achieves desired ends.[11] The relevant question is whether territorial regulation will heighten the cost of unwanted Internet transmissions sufficiently to achieve acceptable control over them. In this connection, it is a mistake to think that governments regulate the Internet only through direct sanctioning of individuals. Governments can also alter the social meaning of the activity, regulate the hardware and software through which the activity takes place, make individual penalties severe and notorious (thereby deterring individuals not subject to direct enforcement), or impose liability on intermediaries like Internet service providers or credit card companies. Whether these regulatory methods achieve acceptable levels of control depends on the importance the government attaches to achieving control, and the cost the government is willing to pay to achieve it. (Imposing the death penalty for Internet gambling would deter Internet gambling significantly, but no nation is willing to impose such a penalty.) The point for now is simply to understand how unilateral national regulation of the Internet can be efficacious.

B *Legitimacy*

It is well accepted today that international law permits a nation to regulate the harmful local effects of foreign conduct. The effects rationale is what justifies nations in unilaterally regulating the harmful local effects of Internet transactions.[12]

Some commentators challenge this conclusion by arguing that the Internet itself is a separate 'place', and that any regulation of this separate place constitutes impermissible extraterritorial regulation.[13] This is a bad argument. The Internet is not a separate place removed from our world. Like the telegraph and telephone, it is a means of transborder communication in which someone in one jurisdiction communicates with someone in another in ways that can cause real-world harms. For example: Internet gambling can decrease in-state gambling revenues and cause family strife; a book uploaded on the Internet can violate an author's copyright; a chatroom participant can defame someone outside the chatroom; terrorists can promulgate bomb-making or kidnapping tips; merchants can conspire to fix prices by e-mail; a corporation can issue a fraudulent security. The list goes on and on. Just about any real-world transjurisdictional harm can occur on the Internet. And from

[11] See Lessig, 'The Zones of Cyberspace', 48 *Stanford Law Review* (1996) 1403, at 1405.

[12] I assume here that there is no independent substantive international law, such as a human rights treaty, that limits the nation's ability to regulate against local harms as it sees fit. I also assume away for purposes of the discussion substantive challenges to the regulation from other perspectives, such as efficiency.

[13] See Johnson and Post, *supra* note 1.

the perspective of the regulating nation, the justification for regulation is no different: something it deems bad is happening within its territory, and it seeks to stop it.

2 Why Worries about Multiple Regulation Are Exaggerated

Many worry that because Internet transactions can appear simultaneously in every jurisdiction, and because nations can regulate the harmful local effects of offshore activity, unilateral regulation of the Internet will lead to multiple and conflicting regulations. This concern is greatly exaggerated for two reasons. One has to do with the limits of enforcement jurisdiction. The other has to do with technological change.

A *The Limits of Enforcement Jurisdiction*

Although a nation can in theory apply its laws to the local effects of a transborder transaction, it does not follow that every nation where an Internet information flow appears can regulate that information flow. To understand why, it is necessary to distinguish between a nation's prescriptive jurisdiction and its enforcement jurisdiction. Prescriptive jurisdiction is a nation's power to make its laws applicable to particular transactions. A nation can apply its regulations to an Internet communication that produces harmful local effects. This is prescriptive jurisdiction. But the force of this law — whether or not the regulation is effective — depends on the nation's ability to induce or compel compliance with the law. This is enforcement jurisdiction. The true scope and power of a nation's regulation is measured by its enforcement jurisdiction, not its prescriptive jurisdiction.

For the most part, a nation can exercise enforcement jurisdiction only against persons or entities with a presence or assets within its territory.[14] The vast majority of content providers on the Internet have no presence or assets in the jurisdictions that wish to regulate their information flows. They thus need worry only about the regulations of the nation in which they are physically located. Their activities are not subject to multiple regulation, at least not directly so. As a practical matter, the entities potentially subject to multiple Internet regulations are users, systems operators (especially Internet access providers) and transaction facilitators (such as banks and credit card companies) with a presence in more than one regulating jurisdiction. The potential multiple regulatory exposure of these entities is non-trivial; but the scope of this exposure is far narrower than is commonly thought, and it mirrors the multiple regulatory exposure faced by persons and firms in 'real space'.

Combining this point with the point of the last section, a clearer picture about the possibility of multiple and conflicting Internet regulations looks like this. Most Internet content providers will not be subject to any regulation other than the one in

[14] There are of course exceptions to this general proposition. A default judgment can sometimes be enforced abroad, and extradition is a possibility. I explain why these enforcement strategies are not likely to be relevant to Internet transactions in Goldsmith, see affiliation above, at 1217–1220.

the territory in which they have presence. As we learned in the above, these Internet users might indirectly suffer consequences from another nation's territorial regulation of the user's Internet transmission. But these offshore users with no local assets are generally beyond the regulating nation's enforcement jurisdiction. The Internet users that need to worry about the liability consequences of multiple, conflicting regulatory requirements are persons and firms with a multi-jurisdictional presence.

B *Technology*

Even for Internet users and firms with a multiple-jurisdictional presence, concerns about multi-jurisdictional regulatory exposure are exaggerated. The concerns are premised on the idea that a content provider or Internet service provider with a multi-jurisdictional presence cannot monitor or control the geographical flow of information on the Internet. This assumption is false. The architecture of the Internet permits geographical content discrimination. The relevant question is the cost of geographical content discrimination and the desired degree of effectiveness.

To understand the point, consider the problems faced by a real-space newspaper company that publishes in many jurisdictions. The newspaper publisher is liable for harms caused wherever the newspaper is published or distributed. A newspaper from state *X* that publishes in state *Y* is not allowed to proclaim ignorance of *Y*'s law as a defence when something in the newspaper violates *Y*'s laws governing, for example, copyright or libel. This seems appropriate because, among other reasons, the publisher can control the geographical locus of publication and distribution. The requirement to keep offending content out of a jurisdiction imposes costs on the publisher, who must, for example, keep abreast of regulatory developments in different jurisdictions and take steps to exclude publication and distribution of offending content in places where liability should be avoided. It is thought to be fair and legitimate for a nation to impose this relatively small cost on offshore content providers in order to exclude unwanted content from the territory.

Now consider a content provider on the Internet, such as a commercial web page operator. Many people think that this web page can be accessed anywhere in the world, and that there is nothing the web page operator can do to control the geographical flow of his/her information on the Internet. But this is untrue. The web page operator can take many steps to ensure that content does not reach an unwanted geographical destination. At the most basic level, she or he can warn users from certain places that access to page's content (be it pornography, a newspaper, a commercial advertisement, a roulette wheel, or whatever) is illegal.[15] Or a multi-state Internet operator can segment web pages geographically and linguistically.[16] Or it can condition access to information on a user's presentation of geographical identification. Many Internet services, for example, require a fax or credit card information to confirm geographical identification. And we are beginning to see tracking software that confirms the user's geographical identification, as well as digital geographical

[15] This is a common strategy among gambling and pornographic web pages.

[16] Both IBM and Amazon.com employ this strategy, in different ways.

identification intermediaries akin to age identification intermediaries that already flourish on the Internet. In short, it is quite possible to 'zone' an Internet transmission flow along geographical dimensions.[17] The only question is the cost of geographical discrimination, and the cost is rapidly falling. (It is falling precisely because the threat of multiple regulatory exposure makes it cost-effective for Internet firms to innovate in favour of geographical discrimination.)

Returning to our Internet web page operator, many commentators believe they should not be liable for harms caused in the many nations where their content appears. The primary basis for this intuition is that the content provider cannot control the geographical and network distribution of its information flows. But this latter point is groundless. We have just seen that 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, Internet content providers will come to occupy the same position as the 'real-space' newspaper publisher. It will thus be appropriate on the Internet, as in 'real space', for national 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.

If this conclusion seems too strict, it is because we are operating on the assumption that an Internet content provider simply places their content on a web page or e-mail list, not knowing where the content may go and thus not responsible for the harm caused by the content when it enters a jurisdiction that forbids it. It seems that the content provider could not have reasonably foreseen that the content was entering a particular jurisdiction, and thus should not be held liable there. But '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, an Internet content provider cannot necessarily claim ignorance about the geographical flow of information as a defence to the application of the law of the place where the information appears. The nature of the Internet makes it foreseeable that the content might appear anywhere.[18] Whether it is fair to hold a content provider liable in a regulating jurisdiction depends on a complex mixture of what the content provider reasonably should have known about the geographical consequences of its acts, the significance of the extra-jurisdictional harms caused by the acts, and the costs of precautions.

This is why in the next few years one of the most important issues concerning transnational liability for Internet transactions will be the specification of what reasonable steps an offshore content provider must take to keep offending content out of a regulating jurisdiction. The tentative claim of US regulators is that a mere disclaimer will not suffice. A recent US decision suggested this in dicta.[19] The US Securities and Exchange Commission (SEC) recently stated that to avoid US securities

[17] Cf. Lessig, 'Reading the Constitution in Cyberspace', 45 *Emory Law Journal* (1995) 869, at 895–899.

[18] In a later draft, I will consider here the distinction between push and pull technology. It seems that the conclusion in the text only applies to push technology, but I shall argue otherwise.

[19] *New York v. Vacco*, *supra* note 5.

liability, an unregistered offshore securities offeror must *both* (a) prominently disclaim that the offer is directed to countries other than the United States, *and* (b) implement procedures that are reasonably designed to guard against sales to US persons, such as ascertaining the purchaser's geographical identification information (address or telephone number) prior to sale.[20] (Note that for Internet commercial transactions that involve delivery of real space, as opposed to digital, goods, the Internet firm knows where in real space the product is going and can take steps to keep it from the regulating jurisdiction; the situation is more complicated for the delivery of digital goods.) The fairness of the requirement to take steps to ascertain geographical identity will depend, as suggested above, on the costs of doing so — costs that are falling every day.

3 The Problem of Regulatory Spillover

A different problem from multi-jurisdictional regulatory exposure is the problem of the spillover effects of unilateral national Internet regulations. The worry is that unilateral national regulations — and especially the most demanding and restrictive ones — will affect the regulatory efforts of other nations and the Internet activities of parties in other jurisdictions. This is the problem of regulatory spillover.

A *The Problem*

To understand the problem, consider three examples involving Internet porn, data protection and Internet gambling. These examples confirm the points made in the first section about the potential efficacy of unilateral regulation. They also demonstrate the problem of regulatory spillover.

First, consider a German official's threat to prosecute CompuServe for carrying online discussions involving persons from around the globe.[21] A local German prosecutor claimed that the appearance of these discussions violated German anti-pornography laws. The German prosecution threat was a real one because CompuServe had equipment and employees in Germany, as well as several hundred German subscribers. CompuServe's initial response was to block access to the discussion groups in Germany. Because CompuServe could not then control the geographical flow of the information on the discussion group in a cost-effective manner, its response to the Bavarian regulation had the effect of blocking access to these discussion groups for all CompuServe users around the world. Faced with multiple regulatory regimes in the many places where it did business, CompuServe bowed to the most restrictive. The consequence was that the Bavarian regulation interrupted the flow and availability of the discussion groups for CompuServe clients everywhere in the world. Any other nation attempting to enforce restrictive anti-pornography laws against CompuServe could have a similar effect.[22]

[20] Statement of the Commission Regarding Use of Internet Web Sites to Offer Securities, Solicit Securities Transactions or Advertise Investment Services Offshore, 23 March 1998.

[21] The facts presented here are incomplete and simplified; I use the example for illustrative purposes only.

[22] Or at least any other nation in a market CompuServe cared about.

Consider next the European Data Protection Directive, which prohibits transfer of personal information from the European Union to countries that lack 'adequate' privacy protection.[23] Europe can enforce this law against non-European companies with a presence in Europe. From the perspective of the United States, where privacy law is less restrictive, the directive constitutes impermissible extraterritorial regulation because it threatens to cut off US computers from European data.[24] Relatedly, if a non-European company wants to mingle European and non-European data, the directive encourages it to move its data processing operations to Europe.[25] In this way, the Internet will often encourage firms to comply with the most restrictive regulatory regime.

Finally, consider a recent Internet gambling case from the United States. Golden Chips Casino, a subsidiary of a New York corporation, is an Antiguan corporation licensed to operate gambling facilities in Antigua. Golden Chips operated an Internet gambling website from Antigua that was available to Internet users in New York. A New York Supreme Court judge ruled that Golden Chips violated New York's anti-gambling laws, and enjoined its operations.[26] The injunction was successful because Golden Chip's directors and employees were in the United States. The injunction had the effect of shutting down Golden Chip's Internet gambling operations worldwide.

All three examples have a similar form. A content provider communicates over the Internet in a way that has multi-jurisdictional consequences. A national or regional government regulates the local effects of the communication, enforcing the regulation by punishing both local and (indirectly) foreign entities. Because Internet transactions are inherently multi-jurisdictional, and because the content provider must take affirmative and sometimes costly steps to keep its Internet out of some territorial jurisdictions and in others, a content provider will sometimes have an incentive to conform its activities to the most restrictive national regulation. Sometimes this means eliminating the content worldwide; other times it means raising the cost for the content worldwide. The bottom line is that unilateral regulation of Internet communications can be effective and might cause worldwide spillover effects.

B *Analysis*

Unilateral national regulation of the harmful local effects of Internet information flows is, from a jurisdictional perspective, perfectly legitimate. This conclusion is not affected by the presence of spillover effects.

Consider first an analogous 'real-space' example, the recent Boeing–McDonnell

[23] Directive 95/46/EC of the European Parliament and the Council, 24 October 1995. The Directive contains many exceptions. For a general discussion from a distinctly American perspective, see P. Swire and R. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (1998).

[24] Swire and Litan, *ibid.* at 3.

[25] *Ibid.* at 4.

[26] *New York v. Vacco, supra* note 5.

merger.[27] These two American companies do business worldwide but have all of their productive resources in the United States. The US Federal Trade Commission investigated and approved the merger. But the European Commission threatened to enjoin the merger (on punishment of severe fines) on the ground that Boeing's exclusive contracts with other airlines — contracts presumably entered into in the United States — were harmful to European competition. Ultimately Boeing acceded to the Commission's demands to (among other things) eliminate exclusive contracting. I am not interested here in the merits of the FTC and Commission actions. The pertinent point is that whichever unilateral regulation prevailed, there would have been spillover effects on to other countries. If the merger went through on FTC-approved terms, Airbus and/or consumers in Europe would have been harmed, and European regulatory interests would have been ignored. And as things turned out, the Commission's conditions on the deal raised the costs in the United States of a merger among two American companies, and superseded the regulatory efforts of the FTC.

Assuming for now that the Commission's regulation responded to a legitimate local competition concern and was not motivated by protectionism, there is nothing illegitimate — at least from a jurisdictional perspective — about its actions. It acted to protect Europeans from the harmful local effects of offshore activity. It had leverage over the two American companies because they did significant business in Europe. The two companies could have stopped doing business in Europe; they decided instead that it was better for them to continue to do business in Europe and comply with the European regulation. It is true that the European regulation causes spillover effects on to the United States. But if Europe did not enforce its regulation, the more permissive American regulation would have caused harmful spillover effects on Europe. In the absence of an international agreement harmonizing competition law, such spillovers are the inevitable consequence of unilateral regulation.

This example reminds us that spillovers are present whenever one nation regulates transnational conduct differently than another, regardless of which nation's regulation applies. The point generalizes. There are *always* spillover effects from unilateral regulation of transnational transactions. These spillovers are inevitable as long as we wish to maintain both national (as opposed to international) lawmaking and transnational activity. Under current conceptions of international law and territorial sovereignty, such spillovers are perfectly legitimate in the absence of some independent international law to the contrary.

These points apply with equal force to unilateral regulation of the Internet. Consider again the CompuServe example. Germany bans certain forms of pornography within its borders. If the medium of the porn were paper, there could be no jurisdictional objection to a German prohibition on the porn's entry at the border or to German punishment of those later discovered to have smuggled it in. From the German perspective it makes no difference whether the porn enters the nation via the Internet or the postal service. The rationale for the regulation is the same in both

[27] See Fox, 'Lessons from Boeing: A Modest Proposal to Keep Antitrust out of Politics', *Antitrust Bulletin*, November 1997, at 19.

contexts: preventing local harms. The German regulation of the Internet affects the cost and availability of pornography in other countries. But if Germany did not regulate the transnational Internet activity, *it* would suffer local harms from extraterritorial conduct. There is no legal principle that requires Germany to yield local control over its territory in order to accommodate the users of the Internet in other countries. Nor does any such principle require Germany to absorb the local costs of foreign Internet activity because of the costs that German regulation might have on such activity. In the absence of some substantive international law to the contrary, Germany can regulate the local harm of transnational Internet activity even if this regulation produces spillover effects. The same analysis applies to the privacy and gambling examples above.

Note that the German regulation is not unfair to CompuServe or to CompuServe users in other countries. For foreign companies like CompuServe that engage in local business, the German regulation is a cost of doing business in Germany. CompuServe reaps financial and other benefits from its presence in Germany. Without this presence German enforcement threats would be empty. CompuServe need not remain in Germany; it can close its shop there if German regulations are too burdensome. Its decision to stay in Germany and comply with German regulations reflects the company's judgement that the benefits of doing business outweigh its costs. As for the CompuServe users outside of Germany: they remain free to choose among dozens of local Internet access services that are not affected by the German regulation. They have no legitimate expectation of access to a worldwide communications network that enables them to cause harms in other countries.

4 On the Likely Persistence of Unilateral Internet Regulation

There are two basic responses to the conflicts and spillovers caused by unilateral Internet regulation: (i) private ordering; and (ii) various harmonization strategies. It is far beyond the scope of this article to assess the likely success for these two strategies. Indeed, the appropriate level of Internet regulation will differ sharply from issue to issue. For example, there is no reason to think that regulation of Internet pornography, intellectual property and privacy will take the same form.

The modest goal of this section is to suggest why private and public harmonization strategies will be inadequate. Private ordering necessarily plays an important role in Internet communities but cannot come close to an adequate response to the many Internet regulation difficulties. Harmonization comes in many stripes and can, in some contexts, alleviate regulatory conflicts. But harmonization is rarely an effective or comprehensive response to conflicts among regulations that reflect important local values. This means that in many Internet contexts (as in many real-space contexts) unilateral regulation will persist. This is not nearly as bad for the future of the Internet as some suggest.

A *Private Ordering*

Private regulation will play a special role on the Internet for two reasons. First, Internet users can by contract choose a single, certain governing law for the particular transactions or networks in question. This alleviates conflicts-of-law difficulties. Second, the value of many Internet transactions is so low that in most circumstances recourse to real-space courts will not be cost-justified. It simply will not be worthwhile for a US citizen who is libelled in a chatroom by a Dane, or who purchases a defective $100 product from a Spanish Internet company, to seek relief in a national court. Private regulators can provide dispute resolution mechanisms that are much cheaper and less formal than national courts. We already see various Internet service companies ranging from E-Bay to Amazon.com to Visa offering informal, effective dispute resolution programmes for multi-jurisdictional consumer Internet purchases. These programmes are likely to be especially robust in the Internet context, where the establishment of trust is so crucial.

Nonetheless, private ordering will not be a panacea. Private regulation takes place in the shadow of public regulation. The desire for trust might well lead large firms to establish effective and dependable private legal regimes. But it is still doubtful whether these private regimes will accord with the mandatory laws of territorial governments. And more importantly, many, perhaps most, Internet content providers care little about a reputation for reliability. These content providers cannot be expected to worry about the harms flowing from their transactions, or to establish fair and effective private legal and dispute resolution mechanisms. In short, private regulation will be a crucial aspect of Internet regulation, but Internet transactions will still cause many local harms that national regulators will worry about and try to regulate.

B *Public Harmonization Strategies*

When regulatory conflict and regulatory spillover occur with respect to 'real-space' transnational transactions, nations have responded with a variety of international harmonization strategies. Sometimes harmonization takes the 'hard' form of treaties that either establish a uniform international standard, or an international anti-discrimination regime, or an international choice-of-law regime. Other times harmonization takes 'softer' forms like information sharing among enforcement agencies or informally agreed-upon regulatory targets.[28]

Various harmonization strategies are being employed to address the challenges of regulating the Internet. Consider a few examples. Several recent treaties and related multinational edicts that have strengthened digital content owners' right to control the distribution and presentation of their property online. These harmonization efforts

[28] Once again, it is hard to overstate the extent to which regulatory conflict related to the Internet might be reduced through technological innovation. The central difference between transnational transactions via the Internet and transnational transactions through other means is that it is, at present, more costly to control information flows geographically over the Internet. Firms in real space minimize conflicting or multiple regulatory exposure by directing business away from restrictive jurisdictions. As discussed above, Internet users increasingly have this capability.

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 Internet-related crimes in five areas: paedophilia and sexual exploitation; drug-trafficking; money laundering; electronic fraud, such as theft of credit-card numbers, and computerized piracy; 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 Internet-related contexts.

Harmonization strategies such as these are clearly an important response to the jurisdictional difficulties of Internet regulation. If successful, these strategies can reduce or even eliminate the costs of regulatory conflict. But public harmonization is not a panacea. It is useful to recall, in this regard, that there are good reasons for regulatory difference among nations. Nations have different regulatory commitments because of, among other things, differences in endowment, technological capacities, and preferences. A primary virtue of decentralized lawmaking by nation states (as opposed to uniform international rules) is that it allows populations to implement policies that reflect these differences. This in a nutshell is the theory that informs, among other things, the concept of national sovereignty, the European principle of subsidiarity, the American conception of federalism, and the economic concept of comparative advantage. In addition to these 'substantive' differences among nations, there is 'procedural' value in having decisions made at the smallest possible political unit.

These substantive and procedural values are diminished by international harmonization. They are costs to be weighed in the balance when considering the virtues of harmonization, especially since some harmonization efforts reflect coercion by powerful nations rather than truly fair or efficient regulatory improvements. In addition, these considerations suggest why harmonization is often not easy to achieve. When regulatory difference reflects important local values, harmonization is hard because of (among other things) domestic political opposition. This is why so many international regulatory regimes are littered with (usually ill-defined) mandatory or local public policy exceptions.[29] This fact should give harmonization's champions pause when addressing national differences in the Internet context concerning privacy, free speech, consumer protection, competition policy and the like.

It is difficult to generalize about when harmonization of Internet-related regulations will be successful, for the Internet covers a broad range of regulatory concerns. We can probably expect relatively robust harmonization in those contexts — like criminal law enforcement and perhaps consumer fraud — where nations' interests converge

[29] For example, the New York Convention, the Convention on the International Sale of Goods, the Rome Convention, and so on.

and the gains from cooperation are high.[30] Harmonization is also likely in coordination situations — such as the communication protocols that define the Internet — where every nation has an incentive to adhere to the adopted standard. The particular standards adopted of course have distributional consequences, which usually mean that powerful nations determine their content; but after the standard is adopted, all nations have incentives to adhere to it. This type of coordination situation, it must be admitted, is not likely to be present when contested social values are in issue.

In many other situations, harmonization will either be undesirable or impossible to achieve. In these situations unilateral regulation will remain the primary method of public regulation.

C *Learning to Live with Unilateralism*

Scholars who study conflicts of law are used to regulatory conflict. They are less likely to see it as the unalloyed evil that other scholars see because they realize that it is often normatively preferable to harmonization and that it is in any event often inevitable. With this thought in mind, it is important to see that the threat of multiple regulatory exposure will not, as many once histrionically claimed, destroy the Internet. The threat of multiple regulatory exposure is simply a cost of doing business on the Internet, a cost that has not prevented enormous Internet growth in recent years. Unilateral regulations affect the cost of Internet transactions and lower their speed, at least until technology eliminates or changes the nature of the problem. But there is nothing sacrosanct about Internet speed or expense. Increasing Internet speed and lowering the costs of Internet transactions are values to be weighed in the mix.

[30] We are likely to see soft harmonization of contested national regulatory regimes before we see hard harmonization. With issues like privacy, consumer protection, and free speech, the most feasible approach for harmonization in the short run is through informal means such as informal enforcement agreements, targeted goals, a softening of unilateral extraterritorial enforcement on a case-by-case basis, and information sharing. These soft strategies can help to reduce regulatory difference, and can lead to harder harmonization agreements.