Jack Goldsmith

The Internet, Conflicts of Regulation, and International Harmonization

A standard set of assumptions underlies the debate on the jurisdictional difficulties presented by regulation of the Internet. Internet protocol addresses do not do not necessarily correlate with physical location. This means that persons communicating and transacting via the Internet often do not know each other's physical location and usually cannot control the geographical flow of content. In addition, information mediated by many Internet services can appear simultaneously in almost every nation in the world. Finally, information transmitted on the Internet can easily flow across national borders without detection.

These assumptions have led many to conclude that Internet regulation creates a jurisdictional quagmire[1]. It is generally accepted that a nation can regulate a transaction that has local effects. But if Internet transactions have effects in every nation, then every nation can regulate the transaction. Since nations differ in their regulatory commitments, many Internet transactions will be subject to inconsistent regulations. And most unilateral national regulations of the Internet – and especially the most demanding and restrictive ones – will affect the regulatory efforts of other nations and the Internet activities of parties on other jurisdictions.

1 See, for example, *David Post* and *David Johnson*, Law and Borders – The Rise of Law in Cyberspace, 48 *Stan. L. Rev.* 1367 (1996).

To make the problem concrete, consider an example drawn from the Bavarian Justice Ministry's 1995 threat to prosecute CompuServe for carrying on-line discussions involving persons from around the globe that violated German antipornography laws[2]. CompuServe initially blocked access to these discussion groups in Germany. Because CompuServe could not control the geographical flow of the information on the discussion group, its response to the Bavarian regulation had the effect of blocking access to these discussion groups for all CompuServe users worldwide. 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 would presumably have a similar effect.

These types of jurisdictional difficulties appear to be implicated by unilateral national (or regional) regulations of privacy, Internet gambling, data collection, consumer protection, intellectual property, and so on. How are we to think about and resolve the conflicts of laws that arise when nations unilaterally apply regulations embodying "local values" to Internet transactions on global networks? My answer has two parts. I first try to show why the jurisdictional clashes presented by the Internet are not as severe, and certainly not as novel, as the conventional wisdom sketched above would suggest. Once we have a more realistic conception of the nature of the jurisdictional conflicts presented by the Internet, I sketch the possibilities for resolving, or at least minimizing, these conflicts through international harmonization techniques.

I. Understanding the Jurisdictional Quagmire of the Internet

The claim that unilateral national regulation of the Internet invariably leads to multiple and conflicting regulation of the Internet is, for several reasons, exaggerated.

It is true that a nation can, in theory, apply its laws to a transnational transaction that has local effects. It does not follow, however, 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[3]. 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[4]. The true scope and power of a nation's regulation is measured by its enforcement jurisdiction, not its prescriptive jurisdiction.

---

2 The details of the example have been simplified for illustrative purposes.

3 Restatement (Third) of the Foreign Relations Law of the United States, sec. 401 (1987).

4 Id.

For the most part, a nation can exercise enforcement jurisdiction only against persons or entities with a presence or assets within its territory[5]. The vast majority of content providers on the Internet have no presence or assets in the jurisdictions that wish to regulate their information flows. (Here and through this essay, I use the term "content provider" as a generic term to refer all persons transmitting information on the Internet, including e-commerce buyers and sellers, porn purveyors and consumers, chat room participants, web page owners, and the like.) The vast majority of Internet content providers 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 mirrors the multiple regulatory exposure faced by persons and firms in "real space.".

Of course, offshore content providers can still feel the effects of local regulations indirectly. Even though a nation's enforcement jurisdiction does not extend to such offshore content providers, the nation can regulate content from offshore indirectly by regulating local persons and entities. For example, it can penalize in-state end-users who obtain or use the foreign content[6]. Or it can regulate in-state hardware and software through which Internet transmissions are received[7]. Or it can regulate Internet access providers and other local firms that facilitate the local transmission of the digital goods[8]. Or it can regulate local financial intermediaries – banks, credit card companies, and the like – that facilitate Internet transaction[9]. In these and many other ways, unilateral national regulations directed at local persons and firms raise the costs of transmission to the offshore content provider, and thereby regulate the flow of the foreign- provided content.

---

5 There are exceptions to this point. A nation can enforce its laws against persons abroad over whom it can obtain personal jurisdiction and enforce a default judgment abroad. It can also extradite persons from other countries. For reasons that I have outlined elsewhere, these forms of enforcement jurisdiction are not likely to have relevance when the issue is unilateral regulation of Internet transactions. See *Jack L. Goldsmith*, Against Cyberanarchy, 65 *U. Chic. L. Rev.* 1199, 1216-1222 (1998).

6 As, for example, many consumers of child pornography have discovered.

7 See *James Boyle*, Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors, 66 *U. Cin. L. Rev.* 177 (1998); *Lawrence Lessig*, Reading the Constitution in Cyberspace, 45 *Emory L J* 869 (1996).

8 For example, pending Internet gambling legislation authorizes federal and state officials to order Internet service providers to shut down illegal Internet gambling sites under threat of penalty. See *John T. Fojut*, Legislative Update, Ace in the Hole: Regulation of Internet Service Providers Saves the Internet Gambling Prohibition Act of 1997, 8 *DePaul-LCA J. Art & Ent. L.* 155 (1997).

9 For example, credit card companies have recently been sued in connection with their facilitation of on-line gambling. See *Matt Beer*, Wages of the Web, *San Francisco Examiner*, August 17, 1998.

A clearer picture about the possibility of multiple and conflicting Internet regulations thus looks like this. Most Internet content providers will not be subject to any regulation other than the one in the territory in which they have presence. The Internet-related entities that need be concerned about multiple, potentially-conflicting regulatory requirements are persons and firms with a multi-jurisdictional presence. This is just as it is in "real space." Also as in "real space," local regulation of such persons and firms can indirectly affect the availability and cost of Internet transactions in other countries. Such indirect regulation is the way in which unilateral regulation has extraterritorial consequences.

Three features of this picture should be highlighted before addressing harmonization issues. I will use the simplified CompuServe example to illustrate.

First, unilateral national regulation of the harmful local effects of Internet information flows is, from a jurisdictional perspective[10], perfectly legitimate. It is clearly consistent with international law for Germany to regulate within its borders the local harms caused by offshore Internet activity. It is also fair for Germany to do so. For German citizens such regulation is a cost (or, depending on each citizens' perspective, a benefit) of citizenship. 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 judgment that the benefits of doing business outweigh its costs.

Second, the extraterritorial spillover effects of unilateral national regulation of Internet transactions are both inevitable and legitimate. Anyone familiar with the ancient discipline of conflicts of law (or private international law) realizes that there are *always* spillover effects from unilateral regulation of transnational transactions. For example: When reinsurance agents in England design contracts that are legal in England but that cause anti-competitive effects in the United States, the application of U.S. antitrust laws to the English reinsurers raises the costs of their activities in England and affects the reinsurance market worldwide[11]. If English rather than U.S. regulation governed the situation, U.S. insurance companies and U.S. regulatory interests would be harmed and

---

10 This is an important caveat. I am talking throughout this essay about regulation of the Internet from the perspective of jurisdiction and choice of law. This is an issue wholly distinct from the merits of any particular regulation of the Internet – for example, whether particular national regulations of the Internet promote democracy, or are efficient, or are good or bad for humanity. Resolution of these substantive regulatory issues turn on contested normative judgments and difficult context-specific, cost-benefit analyses that have little to do with jurisdictional issues. 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 my focus here.

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

the worldwide reinsurance market would be affected[12]. This example shows that spillovers are present whenever one nation regulates transnational conduct differently than another, regardless of which nation's regulation applies. These spillovers are inevitable as long as we wish to maintain both national (as opposed to international) lawmaking and transnational activity. And under current conceptions of international law and territorial sovereignty, such spillovers are perfectly legitimate in the absence of some 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 rational for the regulation is the same in both 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 or moral 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[13]. In the absence of some international law to the contrary, Germany can regulate the local harm of transnational Internet activity even if this regulation produces spillover effects.

Third, the extraterritorial effects caused by a unilateral Internet regulation are premised to a great degree on the architectural assumption that content providers and Internet service providers cannot control the real-space geographical flow of Internet content. This claim is largely false, and increasingly so. Content flow can today be regulated geographically through a variety of means ranging from conditioning access to content on geographical identification, to centralized filtered servers, to mandated end-user filtering, to the imposition of severe penalties for uploading or downloading certain information. The question is not whether the architecture of the Internet permits geographical content discrimination; the question is the cost of geographical content discrimination and the desired degree of effectiveness. The intense demand by Internet users, content providers, service providers, and regulating jurisdictions to reduce such spillovers is driving the development of technologies that lower the costs of discrimination and increase its effectiveness. The adequacy of these developments will

---

12 The same analysis applies to the European Commission's recent imposition of strict conditions on an FTC-approved merger between Boeing and McDonnell Douglas. The application of European competition law raised the cost of the predominantly-U.S. merger, and inevitably had spillover consequences on the aircraft production market in other countries. Similarly, the non- application of European law would have resulted in harm to European interests.

13 These points have special force in the CompuServe case because foreign persons indirectly affected by the German regulation remain free to choose among dozens of Internet access services that are unaffected by the German regulation.

depend on yet-unanswered empirical and technological issues. The point for now is that as content providers and systems operators are increasingly able to control the geographical flow of information, they (like purveyors of information via other communication media) can keep information out of the regulating jurisdiction, thereby reducing regulatory spillover effects and multi-jurisdictional regulatory exposure.

In sum, the unilateral application national regulations to Internet activity can be expected to produce spillover effects and regulatory conflict. The negative spillovers and regulatory conflicts caused by such regulation are narrower than is often claimed. But they are non-trivial; they impose significant costs on Internet activity. How, if at all, should nations think about resolving or minimizing these conflicts?

II. How to think about Resolving or Minimizing Regulatory Conflict

There are three basic responses to the spillovers and conflicts caused by unilateral Internet regulation: (1) private ordering; (2) various harmonization strategies; and (3) muddling through and learning to live with regulatory conflict. Private ordering 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), we will have to learn to live with regulatory conflict, alleviating them on a piecemeal basis and at the margins when possible.

1. Private Ordering

One response to conflicts of national regulations is to let Internet participants regulate their own transactions and communications. This option has intuitive appeal because the conflicts of national regulations often seem to cause severe spillover harms, and because the Internet has been conceptualized as a separate place than can regulate itself.

The problem is that the Internet is not a separate place, and Internet users do not form a self-contained group removed from our world[14]. Internet users are no more removed or self- enclosed than participants in other trans-jurisdictional communication mediums, such as telephone users or postal users or carrier-pigeon users. They are in real space in front of a screen using a keyboard and scanner to communicate with someone else, often in a different territorial jurisdiction. And these real-space communications 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

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

by e-mail; a corporation can issue a fraudulent security; a pornographer can sell kiddie porn; and so on. It is these and many other real-space costs – costs that Internet communities have not effectively internalized – that national regulatory regimes worry about and aim to regulate[15].

Pointing out the harmful real-world effects of Internet transactions is not, by itself, an argument for national (or international) regulation of the Internet in any particular context. It is simply an argument for more realism about the possibility and efficacy and even legitimacy of private ordering of various Internet activities. The best argument for private ordering is an efficiency argument that says the third-party harms of unilateral national regulation are more severe than the third-party harms of private ordering. This calculus requires difficult and controversial valuations that most Internet regulation skeptics have not begun to consider. Such an analysis would also need to focus on particular regulatory contexts rather than on Internet regulation per se. It is very unlikely that such an analysis would lead to the conclusion that self- regulation is cost-effective in all contexts. Indeed, the normative arguments for self-regulation of issues like privacy, consumer protection, gambling, data collection, and pornography are not likely to be any more powerful in the Internet than in the non-Internet contexts.

2. 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.

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[16]. These harmonization efforts

---

15 Critics of Internet regulation tend to ignore or attenuate the real-world harms of Internet activity. They do not consider these effects because they take it as an article of faith that Internet participants form a self-contained group that can internalize the costs of its activity. But this assumption is simply false. Internet 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.

16 In December 1996, the World Intellectual Property Organization ("WIPO") reached agreement on a treaty that significantly extended international copyright protection for digital property. WIPO Copyright Treaty, adopted Dec 20, 1996, WIPO Pub No 226(E) (WIPO 1997). Within a year, the European Commission issued a draft directive to bring European law into line with these international obligations. See Draft EC Directive Provides Strong Online Copyright Protection. The United States has enacted similar legislation. See WIPO Copyright Treaties Implementation Act; Digital Millennium Copyright Act of 1998. (May 6, 1998).

grow out of an international copyright regime that is over one hundred years old[17]. The G8 economic powers have recently begun to coordinate regulatory efforts concerning Internet-related crimes in five areas: pedophilia and sexual exploitation; drug-trafficking; money-laundering; electronic fraud, such as theft of credit-card numbers, and computerized piracy; and industrial and state espionage[18]. 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[19]. Several international organizations have drafted model laws and guidelines to facilitate Internet commerce and related digital certification issues[20]. 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[21]. If successful, these strategies can reduce or even eliminate the costs of regulatory conflict. But harmonization is not a panacea. Harmonization usually comes at the cost of local values and national difference, and whether the gains from harmonization outweigh these costs is usually difficult to determine. Moreover, harmonization is often not easy to achieve. And many harmonizations efforts reflect coercion by powerful nations rather than truly fair or efficient regulatory improvements. It is very difficult to generalize about when harmonization is appropriate and what form harmonization should take. Here are some notes that may help us to understand the problem:

---

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

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

19 See *Anne-Marie Slaughter*, The Real New World Order, *Foreign Affairs* 183, 18992 (Sep/Oct 1997).

20 For example, in February 1997, the United Nations Commission on International Trade Law ("UNCITRAL") began to draft model international digital signature legislation. See Report of the Working Group on Electronic Commerce, Thirty-First Session (New York, Feb 12-28, 1997). See also UNCITRAL Working Group on Electronic Commerce, Planning Of Future Work on Electronic Commerce: Digital Signatures, Certification Authorities and Related Legal Issues A/CN.9/WG.IV/WP.71 (Dec 31, 1996). Similarly, in November 1997, the International Chamber of Commerce issued the General Usage for International Digitally Ensured Commerce ("GUIDEC"), a set of guidelines for ensuring trustworthy digital transactions over the Internet. And the Organisation for Economic Co-operation and Development ("OECD") recently adopted principles to guide countries in formulating their own policies and legislation relating to the use of cryptography. See OECD Cryptography Policy: The Guidelines and the Issues, Unclassified OCDE/GD(97)204 (1997).

21 They are also important for resolving the related problem — hinted at above but not developed in this draft — of regulation evasion. Regulation evasion appears to be a particular problem posed by the Internet, for nations cannot enforce regulations directly against offshore content providers, and because the Internet makes it relatively easy for content providers to shift the source (or apparent source) of content offshore. A good example is on-line gambling. The regulation evasion problem, like the problem of regulatory conflict and the problem of spillovers from unilateral regulation, is real but usually exaggerated. Harmonization strategies can help to eliminate or minimize regulation evasion by ensuring that the same regulatory standards apply everywhere.

First, we should keep in mind 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[22]. 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, and the American conception of federalism. In addition to these "substantive" differences among nations, there is "procedural" value in having decisions made at the smallest possible political unit[23]. 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.

Second, when regulatory difference reflects important local values, harmonization is very difficult to achieve because of (among other things) domestic political opposition. This is why almost all international regulatory regimes are littered with (usually ill-defined) mandatory or local public policy exceptions[24]. This fact should give harmonization's champions pause when addressing national differences concerning privacy, free speech, consumer protection, competition policy, and the like.

Third, the WTO – at least as currently conceived – is probably not the ideal forum for resolving conflicts of regulatory difference implicated by the Internet. The WTO and its predecessors have largely succeeded in lowering express trade barriers because the first generation of anti-discrimination principles they have employed – national treatment and most- favored nation – rest on well accepted economic theory and are relatively easy to enforce. As the WTO has moved into the more contested non-tariff trade barrier contexts (such as health and environmental regulation), its work has become much more controversial. It is likely to become more and more difficult to harmonize social regulations through the rubric of free trade. Many provisions of the WTO scheme recognize this point explicitly[25].

Fourth, harmonization of Internet-related regulations will likely to be easiest to achieve in two contexts. First, we can expect relatively robust harmonization in those contexts—like many aspects of criminal law enforcement—where nations'

---

22 See *David Leebron*, Lying Down With Procrustes: An Analysis of Harmonization Claims, in 1 Bhagwati and Hudec, Fair Trade and Harmonization: Prerequisites for Free Trade? 67-70 (1996). I am indebted to Leebron's excellent analysis of the virtues and vices of harmonization.

23 Id. at 71-75.

24 This is true, to give but a few examples, of the Rome Convention on the Law Applicable to Contractual Relations, all of the Hague Conference treaties, and the New York Convention on the Enforcement of Arbitral Awards.

25 To take one example, the General Agreement on Trade Services creates an exception for national regulations designed to prevent deceptive practices and protect privacy in data collection and dissemination. See GATS, Article XIV.

interests converge and the gains from cooperation are high. Second, harmonization is easiest to enforce in coordination situations — such as the communication protocols that define the Internet – where every nation has an incentive to adhere the adopted standard. The particular standards adopted of course have distributional consequences, which usually mean that powerful nations determine their content[26]; but after the standard is adopted, all nations have incentives to adhere to it. This type of coordination situations, it must be admitted, is not likely to be present when contested social values are in issue.

Fifth, 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.

Sixth, 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 much more costly to control information flows geographically over the Internet. Firms in real space minimize multiple regulatory exposure by directing business away from in restrictive jurisdictions. As discussed above, this is relatively costly to do under the current architectural structure of the Internet. This appears to be changing; conditioned access to content, geographical identification, and more sophisticated filtering devices permit much greater geographical discrimination today than a few years ago. Technological predictions are precarious (especially by me); the only point here is that as Internet content providers can discriminate the flow of their content with greater precision and at less cost, their regulatory exposure, and thus the nature of regulatory conflict, will come to look just as it does in real space.

Seventh, beyond these relatively banal thoughts, it is difficult to make generalizations about the likelihood and desirability of harmonizing regulations pertaining to the Internet. Global arguments for and against regulatory harmonization will not do. In each regulatory context, the costs and benefits of harmonization must be carefully considered, and if harmonization is normatively desirable, the best and most feasible form for achieving harmonization must be chosen. All of these issues are contested. Progress is likely to be achieved slowly and in narrow rather than broad contexts.

---

26 On this problem see *Stephen Krasner*, Global Communications and National Power: Life on the Pareto Frontier, 43 *World Pol.* 336 (1991).

3. Learning to live with Conflict

Scholars who study conflicts of law are used to regulatory conflict. They do not see it as the unalloyed evil that other scholars do 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 remember that unilateral national regulations of Internet activity will not, as many once feared, destroy the Internet. They will raise 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.