# *Internet Regulation: A Case Study in the Problem of Unilateralism*

Yochai Benkler*

## Abstract

*The paper identifies two insights that the problem of Internet regulation provides for understanding the more general problem of unilateralism. First, it suggests the existence of a wide variety of mechanisms for encoding the normative preferences of one nation as behavioural constraints on the citizens of another. In the Internet context in particular, technological and organizational adaptations to law play this role. A broad principle of cooperation among nations, which would require each nation to take account in its public actions of the constraints it would impose on the citizens of other nations, would therefore entail a breathtaking degree of cooperation and consideration among nations, or risk that the very breadth of its ambition will severely limit its domain of operation. Secondly, it suggests that the interplay between unilateral lawmaking on the one hand, and a harmonization ethic implemented by imperfectly articulated multilateral processes on the other hand, creates an institutional environment ripe for the picking by non-representative commercial or other organizations to embed their values in the regulatory system that will ultimately emerge.*

## 1 On the Transmission of Values as Behavioural Constraints

The problem of Internet regulation presents a microcosm of the debates about, and conceptions of, the problem of unilateralism in relations among nations. I will address this paper to two specific insights that the problem of Internet regulation has to offer the more general study of the problem of unilateralism. First, there is the question of the appropriate normative and legal domain of application of the problem. In particular, the question is what mechanisms of transmission of the values of one nation as behavioural constraints in another are within the ambit of concern for international law. Another way of putting this is to think of it as a test case for the proper scope of a 'principle of cooperation' among nations such as the one proposed by

* Associate Professor, New York University School of Law.

*EJIL* (2000), Vol. 11 No. 1, 171–185

Pierre-Marie Dupuy.[1] The second area of concern is emphasized by the (admittedly anecdotal) experience of Internet regulation in particular, and the regulation of digital media in general, with the interplay between unilateral lawmaking and an imperfectly articulated multilateral process and harmonization ethic. Specifically, I raise the concern that a system with imperfectly defined relations between local and global, private and public regulatory processes, and between exceptionalism and harmonization presents an institutional environment ripe for the picking by non-representative commercial or other organizations to embed their values in the regulatory system that will ultimately emerge.

The two Internet regulation papers presented in this symposium represent two radically different conceptions of the domain of application of the concern embodied in the quasi-pejorative term, 'unilateralism'. Jack Goldsmith's paper[2] seeks to diffuse the criticism embedded in the term by at once expanding the range of activities captured within its definition, while limiting the domain he would accept as the appropriate normative concern of an international legal system. 'Unilateralism' in his paper exists whenever nations enact internal law with cross-border effects in other nations. Normatively, he sees nothing improper about one nation embodying its values in the laws it enacts for its own jurisdiction, even if there are some cross-border spillovers, as long as these are not excessive. And, he claims, the spillover effects that are *relevant to the concerns of international law* are no different in the area of Internet regulation than in real space. Franz Mayer's paper takes a very different view.[3] He suggests what is essentially an application of a principle of cooperation, a duty on the part of nations to include in their considerations the effects of their actions on other nations. The premise of his paper is that it is appropriate for Europe to demand a seat at the table of Internet standard setting because the Internet is an important global medium. Though it was created in the United States, funded by the US government, and its standards developed by American engineers, Mayer's paper calls for an internationalization of the standard setting process because this 'American thing', as he calls it, has come to touch the lives of everyone.

At the outset, it is important to understand that both papers share a definition of 'unilateralism' much broader than the minimal concern with action against an established multilateral order that is suggested by Michael Reisman.[4] Unilateralism in this broader conception refers to a concern we might have when one nation acts to encode its values in a manner that transmits them as behavioural constraints on the citizens and residents of another nation that either does not share these values, or at least does not share the determination that they should act as firm behavioural constraints. The two Internet regulation papers differ deeply, however, on what

[1] See Dupuy, 'The Place and Role of Unilateralism in Contemporary International Law', this issue.

[2] Goldsmith, 'Unilateral Regulation of the Internet: A Modest Defence', this issue.

[3] Mayer, 'Regulating the Internet: The European Perspective: the Old World and the New Medium', this issue.

[4] See Reisman, 'Unilateral Action and the Transformations of the World Constitutive Process: The Special Problem of Humanitarian Intervention', this issue.

means of transmission are relevant to considerations of international law, and therefore on how important Internet regulation is.

Goldsmith tells us more or less the following. Reports (sometimes found in early Internet-related literature) of the death of the nation state are grossly premature. Law matters in cyberspace as much as it does in real space. But the law of one nation does not matter too much for the residents of another, except those residents who would have to worry about the law of another nation anyway — primarily companies that have assets in the regulating state. This is so for two reasons. First, a state cannot enforce its laws against actors who do not have some presence or assets in the jurisdiction. And secondly, technology is developing to allow information providers to control the transmission of information quite tightly, and hence to refrain from sending information into a jurisdiction where sending this information would subject them to liability. His conclusion is that regulatory spillover — the imposition of one nation's values on the nationals of another through law — is no worse in cyberspace than elsewhere. And, he concludes, since some degree of regulatory spillover is an inevitable side effect of states carrying on their legitimate function of encoding their values into law binding on their citizens, Internet regulation poses no new concern for international law.

The core methodological limitation of Goldsmith's paper is its linear conception of the causal link between law and behaviour it regulates. This limitation, in turn, questions his treatment of the role technology plays in relation to law and the regulation of behaviour, and his sanguinity vis à vis the cross-border effects of Internet regulation.

Goldsmith assumes that the only relevant domain of application for international law arises, if at all, when the medium of encoding the values of state *A* as behavioural constraints in state *B* is law directly applicable to the nationals of *B*. For example, if a German anti-pornography law leads to the prosecution of an agent of CompuServe,[5] which in turn leads to the elimination everywhere of material deemed unacceptable in Germany, but perfectly acceptable elsewhere, then we are faced with an instance that *might* be within the ambit of the problem of 'unilateralism'.[6] Goldsmith's discussion of the role of technology, however, suggests that if, in order to avoid liability under German law, CompuServe changes the whole way it interacts with its consumers — requires them, say, to present national identity certification — that is beyond the scope of concern for the international legal order.

I will illustrate in the following section the dynamic account of the causal relationship between law, technology, and behaviour. Here I only note that Goldsmith's limited focus is central to his analysis, because otherwise his assumptions about containment of the effects of unilateral action would need different proof from

[5] Amtsgericht Munchen 8340 Ds 465 Js 173158/95, 28 May 1998, *MMR* (1998) 429 and *NJW-CoR* (1998) 356. For an English description of the case, see Moritz, 'Pornography Prosecution in Germany Battles ISPs', *The National Law Journal*, 4 December 1998, at B7.

[6] Goldsmith similarly discusses, for example, direct legal imposition of the v-chip, and regulatory review of the Boeing–McDonnell merger. Each has a similar structure — they refer to direct effects of a legal imposition.

what he offers. The limited enforcement capacity of countries is very important if what one cares about is the direct effect of law on the behaviour of its express addressees. But if one sees regulatory steps as moves in a dynamic system that eventually structures the very network and the relationships of control over information flows through the network, and sees this structuring as an area of valid normative concern, then unilateralism becomes more important to everyone.

Moreover, within a framework of analysis that sees law and technology constraining behaviour in a dynamic relationship, technology, far from being the fix for unilateral law, as Goldsmith suggests, is precisely the most important and pervasive mechanism for the transmission of regulatory values across jurisdictional boundaries. Goldsmith suggests, for example, that organizations subject to multiple jurisdictions require users to identify their country of origin.[7] But in order to implement this technological solution, a multi-jurisdictional actor must reconfigure its relationships with *all* its users, regardless of national origin, in order to exclude those users from contact with those who would subject it to regulation. Pervasive adoption of such strategies by multi-jurisdictional actors will, in turn, pervasively alter the relationships of users to information they seek.

Now, other nations may well have normative commitments contrary to those imposed by the regulating nation. One might imagine that nation *A* abhors pornography, while nation *B* cherishes privacy and its implementing mode of communication — anonymity. The effect of an information provider's adaptation to the regulation of *A* by seeking identification from all users everywhere is to negate the possibility of the implementation of state *B*'s public policy of facilitating anonymous communication. This quasi-Coasian reciprocity of effect of encoding values as behavioural constraints is unavoidable. The incorporation of the values of one nation into the technology of communication shared by many displaces those of other nations, while a nation that refrains from such incorporation is exposed to communications that implement the values of another. This reciprocity suggests that true commitment to concern whenever a nation encodes its values in a manner that imposes them as behavioural constraints on nationals of a coordinate nation requires cooperation on a much grander scale than usually considered necessary — even if implemented only through consultation or as moral claims within internal political debate on the scope or manner of regulation.[8]

Franz Mayer's paper relies on assumptions opposite to those Goldsmith embraces.

[7] Goldsmith, *supra* note 2.

[8] Within the United States claims have been made, for example in the debate of the Clipper Chip, that enforcing 'law and order' values through forcing weak encryption will expose the nationals of more repressive nations to easier and more effective regulation. See Moglen, 'So Much for Savages', comments at a conference on The Role of Encryption Technology in Business, Law Enforcement, and Constitutional Analysis, New York University School of Law, 19 November 1998, available at *http://old.law.columbia.edu/my_pubs/yu-encrypt.html* (arguing for a pervasively encrypted network by reference to, among other things, its capacity to 'prevent . . . fingernails being ripped out, not to mention worse things being done, by nasty people all over the world who have a tendency to tap telephones and torture people based on what they hear').

First, he embraces the proposition that technology is a means of transmitting the values of one nation as behavioural constraints in another as the working assumption of his paper. As he puts it, if one nation builds the roads so that large trucks cannot travel upon them, then the other nation's sovereign power to impose traffic laws no longer includes, as a practical matter, the power to permit trucks to travel on those roads. And secondly, he implicitly assumes that the mere fact that the Internet has become an important presence in European lives, for example, entitles them to a say in how this technological marvel — financed, built, and managed largely in the United States, with government funds, by Americans — will be designed. In other words, he assumes a 'principle of cooperation' of quite significant scope, and requires Americans to yield some of their factual control over the Internet to an international forum where the values and interests of all those affected by the Net will be present. Figure 1 graphically expresses these differences in assumptions between the two papers.

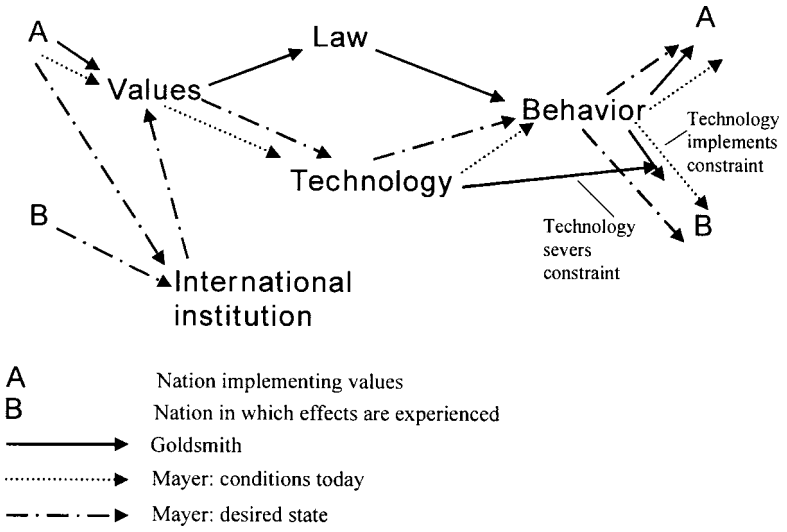


**Figure 1. Law and Technology as Mechanisms of Cross-Border Transmission of Values**

## 2 On the Dynamic Relationship between Law and Technology as Regulators of Behaviour

Law regulates behaviour, and technology regulates behaviour.[9] Law, technology and behavioural adaptations to them interact in a dynamic recursive process to form

[9] The former statement is hardly surprising. The latter is generally identified with Lessig's notion of 'code as code', see Lessig, 'Surveying Law and Borders: The Zones of Cyberspace', 48 *Stanford Law Review* (1996) 1403, at 1408; and Reidenberg's notion of 'lex informatica', Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', 76 *Texas Law Review* (1998) 553.

the parameters of human behaviour that is bound up with the technology.[10] Since I have elsewhere set out the defence of this proposition in great detail, let me explain here by way of illustration.

Once upon a time a single prudish Senator held up the most important overhaul of telecommunications regulation in the United States in over half a century in order to force Congress to pass an ineffective and unconstitutional ban on dirty words and pictures on the Net. Congress passed the law, known as the Communications Decency Act (CDA) in early 1996, and the courts promptly struck it down as unconstitutional.[11] One might think that this was a case of ineffective regulation. But that would be far from true. The introduction of the CDA bills in early 1995 focused the efforts of well-meaning engineers and of commercial software developers and information services on perfecting content 'filtering' mechanisms — ways in which users can get their software to prevent their kids from receiving dirty pictures.[12] Many thought that if they developed an effective filtering technology, the need for speech-restrictive legislation would disappear, and user-controlled information flows would prevail. Indeed, in striking down the CDA the courts mentioned the availability of filters as a less restrictive means of protecting children from pornography. But the consequence of these efforts was the development of sophisticated technological tools that allow anyone who controls a part of the network on the way to the end-user's computer to interject themselves — by setting filtering rules — between an end user (whether child or adult) and information the end-user wants (be it porn, union organizing materials, or political criticism).[13] Nothing limits their utility to parents, as opposed to governments or employers, who can, if they so choose, control what many people can receive. Just as the parent can introduce software at the home computer to prevent kids from accessing materials of which the parents disapprove, so can the public library prevent access from its computers,[14] so can the Internet service provider filter information before it reaches its subscribers,[15] and so can a government willing

[10] Benkler, 'Communications Infrastructure Regulation and the Distribution of Control Over Content', 22 *Telecommunications Policy* (1998) 384; Benkler, 'Overcoming Agoraphobia: Building a Commons for the Digitally Networked Environment', 11 *Harvard Journal of Law and Technology* (1998) 287.

[11] *Reno v. ACLU*, 521 US 844 (1997).

[12] See Resnick, 'PICS, Censorship, & Intellectual Freedom FAQ', available at *http://www.w3.org/PICS/PICS-FAQ-980126.html* (Resnick defends filters against claims that they facilitate speech restriction, but accepts that efforts in this area follow attempts in early 1995 to regulate Internet content.)

[13] See Lessig, 'What Things Regulate Speech, CDA 2.0 vs. Filtering', available at *http://cyber.law.harvard.edu/works/lessig/what_things.pdf* For a number of very useful papers on Internet filtering see *Filters & Freedom, Free Speech Perspectives on Internet Content Controls* (1999).

[14] See, e.g., *Mainstream Loudon v. Board of Trustees of the Loudon County Library* (ED Va 7 April 1998), available at *http://www.techlawjournal.com/courts/loudon/80407mem.htm*

[15] The benign version is something like TheKosher.net, an ISP that filters out content inappropriate for orthodox Jews and sells that filtered service. See *http://www.thekosher.net/about.htm* Nothing, however, prevents *any* service from introducing a filter at any layer of the service, and this need not be transparent to users. Even if the effect is nothing more than to alter the default availability of information for browsing, subject to change by the user, this would have a significant effect on what users actually see. Otherwise it is hard to see how Netscape's value is so heavily tied to the fact that its homepage is the default portal for users of its browser.

to enforce its will on service providers filter information that reaches its citizens. This makes the lives of regulators easier, because now they can target regulation to take advantage of the technology. Senator McCain's bill to require all schools and libraries that benefit from federal funding to install filters is a simple illustration.[16]

So, law threatened action, which lead to the rapid development of a technology that, although originally intended to move control over information flows to end users, in fact created a tool that could enable governments to control the flow of information to and from their citizens. Now, this was unilateral legislation that was not necessarily seen as having side effects outside of the United States, but nonetheless has cross-border effects, as the drive to universalize standards for filtering increases.[17]

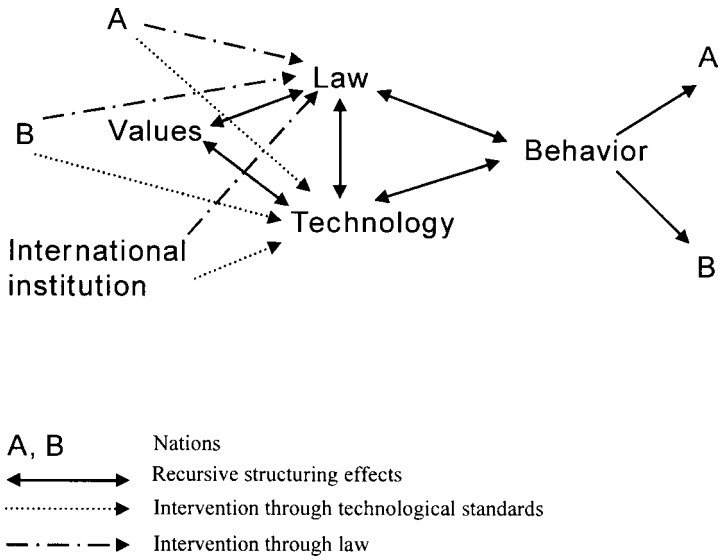


**Figure 2. The Interaction between Law and Technology as Means of Encoding Values as Behavioural Constraints**

Once one perceives the dynamic relationship between law, technology and the regulation of information flows, it becomes more difficult to remain sanguine about the persistence of unilateral regulation. In effect, any state or international body can intervene at any point in the recursive process, constraining the behaviour of individuals far outside its formal jurisdiction.

Consider Goldsmith's discussion of how technology serves as a solvent to prevent even multi-jurisdictional actors from facing liability under extensive unilateral

[16] 105 s. 1619.

[17] For example, see report on efforts organized by the Bertelsmann Foundation to foster development of a globally available, polycultural filtering standard. Mendels, 'Plan Calls for Self-Policing of the Internet', *New York Times*, 20 September 1999, *http://www.nytimes.com/library/tech/99/09/biztech/articles/20rate.html*

regulation. These actors, traditionally exposed to varying laws in different jurisdictions, can turn to technology to prevent this exposure for online activities. Technology, he says, enables these actors to segregate their services by user's country of origin.[18] Goldsmith starts by using a non-Internet example of a newspaper distributor refraining from sending copies into a jurisdiction as his example for how a multi-jurisdictional actor can comply with conflicting regulatory regimes by refraining from providing some services to a given jurisdiction. As a technical matter, however, this is a weak example. Refraining from posting copies of a newspaper to Alabama has no effect on readers outside of that state. The baseline condition of a newspaper is that it lies quietly in a pile and waits for someone to move it. It cannot get to Alabama unless the sender specifically sends it to that jurisdiction. The same is not the case with the baseline architecture of the Web. Here, in the absence of some specific action to prevent it, information once posted is available everywhere and to everyone. And what that preventive or containing action is, is not so easy to define, as Goldsmith's efforts show.

Goldsmith suggests three actions a content provider can take to prevent its materials from being accessed in jurisdictions where its information is illegal. None of these responses, however, is *both* effective *and* without consequence for users outside the jurisdiction. First, he says, the information provider can warn users. If effective, Goldsmith is correct that this technique in fact creates relatively minor spillover effects. But it is an effective technique if, and only if, the jurisdiction treats 'warnings' without more, as exculpatory. Imagine: Warning, the following political criticism is banned in China (or Singapore, or Germany); if you are a resident of China (or Singapore, or Germany) do not access this information. One might imagine governments less than enthusiastic to exculpate the provider. Secondly, he suggests geographic or linguistic segmentation of the web service. All this means is that the German-language website will not be in violation of German law. It is unclear, however, why German law would care whether the Nazi propaganda available in Germany is in English or French, rather than German. Presumably, in order to avoid German law a website operator will have to affirmatively block access to the illegal propaganda, in whatever language it is presented.

And here enters Goldsmith's third proposal, his first actually effective technological means of preventing materials from entering a jurisdiction where they are considered harmful. And here, too, is the rub. For to do as Goldsmith suggests — require extensive self-identification of users before they receive access to information — is to change how the server interacts with all users, from all jurisdictions, in order to keep the server safe from liability in a single jurisdiction. This is where regulatory spillover occurs, and occurs at the level of the basic structure of the relationship that everyone, everywhere, has with the information. Rather than being a solvent of the relationship between the law of one nation and the behaviour of those outside it, technology becomes the means of transmitting and implementing the values of the regulating nation.

[18] Goldsmith, *supra* note 2.

By affecting network design, one nation's law can affect how everyone in the world interacts with information that is deemed offensive in that jurisdiction. In our example, it makes access to such information more difficult for everyone. It may trade off privacy or anonymity, for example, for access to the information, and may do so for users around the world. It may simply raise the costs of access to information the regulating nation deems offensive, which, on the view of many including Goldsmith, is what, as a functional matter, regulation always does when it seeks to affect behaviour. The magnitude of the cost increase outside of the jurisdiction may be lower than in it, but the qualitative effect is the same — the costs of engaging in behaviour deemed harmful in the jurisdiction is raised for users both inside and outside the jurisdiction. And this, in turn, undermines Goldsmith's first point, about the limited jurisdictional reach of states. If states can affect how all multi-jurisdictional players in the Internet service market structure their relationships to their users everywhere, then the practical reach of each state's jurisdiction to increase the costs of, and shape the way people in other jurisdictions interact with, information it deems harmful — say, Nazi propaganda or pornography — is in fact quite extensive.

## 3 On the Dangers of Imperfect Multilateralism and the Ethic of Harmonization

As I noted before, Mayer bases his discussion on the assumption that technology is not only an effective medium for transmitting the values of one nation as behavioural constraints in another, but also that this form of transmission is one that is properly the concern of the international order. To quote the Reply of the European Commission and the Council to the US Green Paper,[19] 'the future management of the Internet should reflect the fact that it is already a global communications medium and the subject of valid international interest'.[20] Note that this statement seems to assume that 'a valid international interest' arises from the importance of something to many nations, even, as is the case with the standards and approaches to connecting computers that make up the Internet, if that something was developed with a quarter century of US government funding, mostly by American engineers, and is heavily based on the facilities of American universities and companies under contract with the US government.[21] While the European response could have cited the threat that a failure to include Europeans in the design would result in the emergence of a separate, and incompatible European design, that was not the argument made. (This may partly be due to the fact that such a threat is highly improbable. Although standards can easily diverge if they compete before adoption, where a standard is so widely adopted as are the Internet standards, in an economic good like communication that

[19] The Green Paper, entitled 'A Proposal to Improve Technical Management of Internet Names and Addresses' can be found at *http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm*

[20] Brussels, 16 March 1998, available at *http://www.ispo.cec.be/eif/policy/govreply.html*

[21] See Leiner *et al.*, 'A Brief History of the Internet', *http://www.isoc.org/Internet-history/brief.html*

has such overwhelming network effects, the probability of emerging European incompatibility is not too high.) The argument sounds much more in a moral claim for participation and cooperation than in a claim about efficiency of a common standard facing the threat of forking standards. It is important to face this structure of the claim, because it presents at least one radically broad interpretation of the principle of cooperation — that is, that even a country that beneficially affects lives in other countries is then bound to consider how changes to its beneficial policy implicate the values and interests of these other countries.

The relatively limited experience of Internet regulation with the interaction between unilateral and multilateral regulatory efforts, however, cautions against too easy an adoption of an ethic of harmonization, or a principle of cooperation. Mayer's proposal provides a good basis for evaluating these risks. He suggests that ICANN — the Internet Corporation for Assigned Names and Numbers — be recreated under a multilateral treaty, with some special relationship to WIPO, which would result in what he admits would be 'an interesting animal in the zoo of public international law'.[22] But it is precisely the domain name controversy that led to the creation of ICANN that advises a skeptical stance towards the regulatory prowess of interesting animals.

The history of ICANN, and the role that private interests, the US government, and international organizations — namely, the ITU and WIPO — played in its formation and are playing in its operation provide an important lesson about how the drive to international cooperation can be hijacked to impose values that cannot legitimately be claimed to belong to any state or international assembly.[23] It represents a story of how commercial interests bent on extending the hold that their trademark gives them on trade in real space found a way to privatize a public resource while retaining enough public power to enforce their trademarks when necessary. The story, and its implications for thinking about the dangers of imperfect multilateralism, are set out plainly by Michael Froomkin, a law professor who was the public interest representative on the panel of experts advising WIPO as it formulated its recommendation to ICANN for resolving the domain name trademark issue.[24]

The story that ends up with the WIPO recommendation to ICANN revolves around the management of a public good — the Internet's equivalent to our real world system of street addresses and post office boxes. Each computer that is 'connected to the Internet' has a unique number that identifies it to all other computers called an IP (Internet Protocol) number. These numbers are mapped to correspond to alphanumeric strings such as *law.nyu.edu*, called domain names. Because the IP numbers are

[22] Mayer, *supra*, note 3.

[23] Sources for this history are Froomkin, 'Semi-Private International Rulemaking: Lessons Learned from the WIPO Domain Name Process', *http://www.law.miami.edu/~froomkin/articles/tprc99.htm*; Simon, 'Overview of the DNS Controversy', *http://www.flywheel.com/ircw/overview.html*; Post, 'Governing Cyberspace', *http://www.icannwatch.org/archives/essays/930604982.shtml*; Dawson, 'A History of Developments in the Assigning of Domain Names', *http://www.tbtf.com/resource/domain-name-hist.html*

[24] Froomkin, 'Of Governments and Governance', 14 *Berkeley Technology Law Review* (1999) 617.

hard to remember, domain names have become the common human interface to IP addresses — whether in sending emails or accessing web pages. Throughout most of the Internet's life, these addresses were managed by a group of volunteer computer engineers organized as the Internet Assigned Numbering Authority (IANA), headed by one of the original developers of the Internet Jon Postel, in cooperation with, and funding from the United States Department of Defense. In 1992, the US government contracted with a private firm, Network Solutions, Inc. (NSI), to take the increasing burden off the hands of the volunteers and the government. In 1995, a budget-conscious administration decided to fund this operation with user fees, and permitted NSI to charge for domain name registration. At about the same time, widespread adoption of graphical interfaces called browsers made using the World Wide Web — a new way of using the Net developed in 1993 — radically simpler and more intuitive to the uninitiated. These two developments brought together two forces to bear on the domain name issue — two forces of very different origin and intent. The first force consisted of the engineers who had created and developed the Internet, who understood the domain name space to be a public trust, and were resisting its commercialization by NSI. The second force were the owners of trademarks and their lawyers, who suddenly realized the potential for using control over domain names to extend the value of their brand names to a new domain of trade — e-commerce. These two forces placed the US government under pressure to do two things: release the monopoly that NSI — a for-profit corporation — had on the domain name space, and find an efficient means of allowing trademark owners to control the use of alphanumeric strings used in their trademarks as domain names.

By late 1996 the International Ad Hoc Committee (IAHC) was formed, with the blessing of the Internet Society (ISOC), the major professional membership society for individuals and organizations involved in Internet planning. The membership of IAHC is indicative of the interests it represents.[25] Of the ten-member committee, three were intellectual property lawyers, one of them senior legal counsel at WIPO; five were engineers from the US, Australia, Japan, and Israel; one represented the US government's National Science Foundation, and one was from the International Telecommunications Union (ITU). In February of 1997, IAHC came out with a document called the gTLD-MoU.[26] Although the product of a small group, the document claimed to speak for 'the Internet Community', and although involving no governments, was deposited 'for signature' with the ITU. And, dutifully, some 226 organizations — Internet services companies, telecommunications providers, consulting firms, and a few chapters of the ISOC signed on.[27] Section 2 of the gTLD-MoU, announcing its principles, reveals the driving forces of the project. While it begins with the announcement that the top level domain space 'is a public resource and is subject to the public trust', it quickly commits to the principle that 'the current and future

[25] Available at *http://www.isoc.org/whatsnew/iahcmembers.html*

[26] Available at *http://www.itu.int/net-itu/gltd-mou/gTLD-Mou.htm* gTLD stands for generic top level domains, the '.com', '.edu' '.org' parts of the domain name, which do not have a country-based modifier like .fr (France). These country-based top level domain names are denoted ccTLD. MoU stands for Memorandum of Understanding.

[27] Available at *http://www.itu.int/net-itu/gtld-mou/signat.htm*

Internet name space stakeholders can benefit most from a self-regulatory and market-oriented approach to Internet domain name registration services'. This results in two policy principles — commercial competition in domain name registration, i.e., releasing the monopoly NSI had; and protecting intellectual property in the alphanumeric strings that make up the second level domain names. The final, internationalizing component of the effort — represented by the interests of the WIPO and ITU bureaucracies — was attained by creating a Council of Registrars as a Swiss corporation, and creating special relationships with the ITU and WIPO.

But none of this institutional edifice could be built without the US government. In early 1998 the administration responded to this ferment with a Green Paper, seeking the creation of a private non-profit corporation registered in the United States to take on management of the domain name issue.[28] By its own terms, the Green Paper responded to concerns of the domain name registration monopoly and of trademark issues in domain names, first and foremost, and to some extent to increasing clamour from abroad for a voice in Internet governance. Despite a cool response from the EU,[29] the US government proceeded to finalize a White Paper and authorize the creation of its preferred model — the private non-profit corporation. Thus was born ICANN, whose coordination with WIPO to resolve the trademark/domain name controversy completes this morality tale, and adds a very concrete example of what Laurence Boisson de Chazournes identifies as the 'unilateralism' of international organizations[30] — in this case, the WIPO Secretariat.

Following an invitation in the US government's White Paper to study the proper approach to trademark enforcement in the domain name space, WIPO initiated a process that began in July 1998,[31] and ended in April 1999.[32] As Froomkin describes his experience as a public interest expert in this process, however, there was much appearance of transparency and open discourse in this process, but an actuality of opaque staff-driven drafting.[33] The result was a very strong property right available to trademark owners in the alphanumeric strings that make up domain names, supported by binding arbitration, capable of worldwide enforcement through ICANN's control over access to addresses, and hence power to prevent access to those not in compliance with the arbitration awards. This result was attained without ever being subject to negotiation among nations. It was a product of the WIPO staff; could not be subject to judicial review, for no such review is available of either the WIPO staff or of ICANN, a private actor; and did not require ratification by elected legislatures —

[28] 'A Proposal to Improve Technical Management of Internet Names and Addresses', *http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm* (January 1998).

[29] See Mayer, *supra* note 3.

[30] L.B. Chazournes, 'Unilateralism and Environmental Considerations, Issues of Perception', *EJIL*, forthcoming.

[31] RFC 1, 'Request for Comments on Terms of Reference, Procedures, and Timetable for the WIPO Internet Domain Name Process', 8 July 1998, *http://wipo2.wipo.int/process/eng/timetable.html*

[32] World Intellectual Property Organization, 'The Management of Internet Names and Addresses: Intellectual Property Issues', *http://wipo2.wipo.int/process/eng/FinalReport.html*

[33] Froomkin, 'Semi-Private International Rulemaking: Lessons Learned from the WIPO Domain Name Process', *http://www.law.miami.edu/~froomkin/articles/tprc99.htm*

for its implementation is a recommendation to the private corporation that acts as gatekeeper to the Internet.

The value of extending strong property rights in the alphanumeric strings that make up trademarks so as to apply them to domain names is at least controversial. The underlying assumption of the value of trademarked alphanumeric strings as second level domain names is that users will approach electronic commerce by typing in *www.[brandname].com* as their standard way of relating to information on the Net. But this, at the very least, is a narrow-minded and near sighted assumption. In physical space, where collecting comparative information on price and quality etc. is very costly, brand names serve an important informational role. In cyberspace, where software can compare prices, and product review services that link to vendors are easy to set up and cheap to implement, the brand name becomes an encumbrance on good information, not its facilitator. If users are limited to hunting around as to whether information they seek is on *www.brandname.com* or *www.brand-name.com* or *www.brand.net* etc., name recognition from the real world becomes a bottleneck to e-commerce. And this is precisely the reason why owners of established marks sought to assure early adoption of trademarks in domain names — it assures users that they can in fact find their accustomed products on the Web without having to go through search algorithms that might expose them to comparison with pesky startup competitors.[34]

The point here, though, is not to re-argue whether strong trademarks in domain names are a good idea or a bad idea. That question will probably fall by the historical wayside, as newer interfaces to accessing information on the Web will develop to make the whole domain name guesswork approach to looking for information seem silly. The point is to observe how commercial interests embedded their values in the regulatory framework by manipulating pressures for an internationalized, mixed public–private solution to a problem with perceived cross-border effects. In this process, internationalization served to exclude, as a practical matter, the values that might have been adopted by *any* nation that would have had a legitimate public debate on the matter. Moreover, the complex interaction between law and technology and between various national and international legal and standard-setting processes described in Figure 2 permits such organizations to intervene in whatever forum would most effectively move the process to embed values dear to them as behavioural constraints on all users of the Net. Such a process occurred when the US administration — largely driven by Hollywood — tried to pass expansive prohibitions on circumventing technological locks that prevent access to information goods. It first failed in the US, then tried to reintroduce these prohibitions as treaty provisions in the negotiation of the WIPO treaties, failed there, and eventually persuaded Congress to pass the law, The Digital Millennium Copyright Act of 1998,[35] on the unfounded

[34] See Y. Benkler, *Electronic Communications and the Law* (1996, 1997 Supp.) §33A.2; Litman, 'Electronic Commerce and Free Speech', available at *http://www.law.wayne.edu/litman/papers/freespeech.pdf*

[35] Pub. Law 105–304 (1998).

claim that it must be passed to keep the US in compliance with the WIPO treaties.[36] Similarly, the drive to harmonization with the EU was also central to the lobbying efforts of some in the database industry to persuade Congress to pass a *sui generis* right in facts contained in databases[37] equivalent to that recognized in the EU.[38]

## 4 Conclusion

Internet regulation presents a fascinating case study for the question of unilateralism, because the Internet is at once recognized as immensely important everywhere and at the same time is subject to no recognized international legal order.

The first insight to be drawn from the question of Internet regulation is that a broad understanding of the problem of unilateralism, one that would recognize a general 'principle of cooperation' whenever one nation encodes its values in a manner that imposes behavioural constraints on nationals of another, would implicate a tremendously large number of policy decisions taken in various countries. Both law and technology can act as means of embedding values of one nation as behavioural constraints in another. Moreover, the dynamic causal relationship between law and technology means that many more decisions about local law are translated, in a digitally networked globe, into behavioural constraints in other nations. Anyone who embraces a principle of cooperation must take into account, on the one hand, how extensive a set of requirements such a principle imposes if it applies whenever one nation imposes its values on the nationals of others, and on the other hand, how ineffective the principle would be if it were to limit itself solely to behavioural constraints imposed directly by law.

The second insight to draw from the experience of Internet regulation is that internationalization of policy questions is itself a medium for encoding and imposing values as behavioural constraints in many countries. This experience suggests, however, that the mechanism of internationalization profoundly affects the source and legitimacy of the constraints imposed. In particular, the experience of the domain name trademark issue suggests that imperfect multilateralism can result in the imposition of values that belong to no nation. Through combinations of public and private, national and international, unilateral and multilateral rulemaking mechanisms, powerful commercial interests, professional bureaucrats, both national and international, and other highly committed individuals and organizations interested in

[36] Samuelson, 'Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised', 14 *Berkeley Technology Law Journal* (1999) 519. See also Litman, 'The Tales that Article 2B Tells', 13 *Berkeley Technology Law Journal* (1998) 931, at 932–933.

[37] See, e.g., Hearing on HR 2652, Collections of Information Antipiracy Act, Before the Subcommittee on Courts and Intellectual Property of the House Committee on the Judiciary, 105th Cong. (statement of Robert E. Aber, on behalf of the Information Industry Association). On the effects of the combined European–American drive to extend protection see Reichman and Samuelson, 'Intellectual Property Rights in Data?' 50 *Vanderbilt Law Review* (1997) 51.

[38] Commission Directive 96/9/EC OJ 1996 L 77/20, on the Legal Protection of Databases.

a policy question can define the regulatory universe according to their interests, free of scrutiny and effective control by any body that can plausibly claim democratic legitimacy.